ANTI-MONEY LAUNDERING AND
TERRORISM FINANCING COMPLIANCE PROGRAM

Company: DM GLOBAL FINANCE LIMITED

Date: 19.02.2025

Valid until: 19.02.2026

Update due to: 19.02.2026

Approved and reviewed by: MANUILA DUMITRU

TABLE OF CONTENTS

GENERAL

DM GLOBAL FINANCE LIMITED (the "Company") is committed to full compliance with applicable anti-money laundering (AML) laws and regulations, including Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). This policy forms an essential part of the Company's broader AML framework, outlining the procedures and responsibilities necessary to uphold regulatory requirements.

Purpose of This Policy

The primary objective of this policy is to ensure the Company meets its legal obligations in preventing money laundering and terrorist financing. It aims to support law enforcement efforts in detecting illicit activities while safeguarding the Company's resources from potential misuse. Non-compliance with AML regulations could lead to legal, financial, and reputational consequences for both the Company and its personnel.

Who Must Adhere to This Policy

This policy applies to all employees, management, and directors of the Company. Specifically, the designated AML Compliance Officer is responsible for overseeing its implementation and ensuring adherence to regulatory standards.

AML Compliance Officer: Manuila Dumitru (dmglobalex@gmail.com)

AML Procedures and Compliance Measures

Money laundering involves concealing the origin, ownership, or destination of funds obtained through illegal activities. The Company is committed to identifying, preventing, and reporting any suspicious activities in line with FINTRAC's guidelines. A risk-based approach will be used to assess transactions and mitigate exposure to illicit financial activities. All measures and controls are further detailed in the Company's AML Compliance Program.

Client Identification and Verification Procedures

To comply with AML requirements, the Company has implemented a customer due diligence (CDD) process that verifies the identity of all clients before account activation.

For individual clients, the Company requires valid identification, which may include but is not limited to:

1. A government-issued passport
2. A valid driver's license
3. Screening against compliance databases (e.g., FINTRAC, OSFI, or international watchlists)

For corporate or legal entities, the Company requires formal documentation verifying the entity's existence, address, and the authorization of its representatives. The AML Compliance Officer will maintain records of all collected documentation in accordance with legal retention requirements.

Prohibited Clients

The Company will not establish accounts, accept funds, or process transactions for individuals or entities that present a high risk of money laundering or terrorist financing unless enhanced due diligence (EDD) measures have been thoroughly conducted and properly documented.

Introduction

The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) establishes specific requirements to prevent financial institutions from being used for illicit activities. Compliance with this legislation ensures that the Company, along with the broader Canadian financial system, remains safeguarded from illicit funds.

Under the Act, the Company must maintain detailed records of business transactions, which include:

1. The identification of all parties involved in a transaction, documented through activity reviews.
2. A description of the transaction, including its purpose and method of execution.
3. Account details associated with the transaction, including the institution, branch, and relevant identifiers.
4. The total value of the transaction.

To comply with these requirements, the Company commits to maintaining all client transaction records for a minimum of five years following the termination of the business relationship. Failure to properly retain financial records as mandated by the Act constitutes a legal offense.

Regulatory Oversight & Monitoring

Regulatory authorities, including FINTRAC, have the right to inspect financial records if there is reasonable suspicion of a money laundering or terrorist financing offense. These inspections may be conducted during normal business hours, and institutions must fully cooperate by providing relevant transaction data. Additionally, the Company is required to exercise heightened scrutiny over complex, large, or irregular transactions—whether completed or not—as well as recurring transactions that lack a clear economic or lawful purpose.

Reporting Obligations

Management is responsible for reviewing large transaction reports and monitoring all incoming and outgoing wire transfers. Failure to report suspicious activities, or intentionally filing false reports, constitutes a criminal offense. Furthermore, employees and management are strictly prohibited from informing or "tipping off" clients about any ongoing investigations or regulatory inquiries.

Commitment to Due Diligence

The Company is committed to implementing rigorous due diligence procedures to verify the true identity of all customers and prospective clients. This ensures that no funds are deposited or invested under false, assumed, or fictitious identities.

Enhanced Due Diligence (EDD) Measures

The Company implements enhanced due diligence (EDD) procedures for clients who pose a higher risk of money laundering or terrorist financing. These include, but are not limited to:

- Politically Exposed Persons (PEPs);

• Clients operating in high-risk industries, such as online commerce or money services businesses;

• Clients conducting business in jurisdictions with active military conflicts, significant drug production, or known terrorist activities;

• Clients engaging in frequent high-value transactions or large, unexpected one-time transactions.

In addition to standard account verification and ongoing monitoring, any client or transaction requiring enhanced due diligence must be reviewed by the Chief Compliance Officer (CCO). The CCO will assess whether the transaction warrants the filing of a Suspicious Transaction Report (STR) with FINTRAC.

Verification of Asset Legitimacy

The Company is committed to verifying that all funds deposited originate from lawful sources. This measure ensures that proceeds of crime are neither introduced into nor processed through the Company's financial system.

Record-Keeping and Compliance

To adhere to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), the Company ensures that all financial transaction records are accurately maintained. Employees are required to uphold strict documentation standards in compliance with legal and regulatory obligations.

Reporting Suspicious Transactions

All personnel are trained to identify unusual or potentially suspicious transactions. If there is reasonable suspicion of money laundering, an STR must be submitted to FINTRAC immediately, as required by law.

Regulatory Compliance and Training

The Company strictly follows FINTRAC's AML guidelines and training protocols to support Canada's reputation as a jurisdiction committed to combating financial crime. Employees receive ongoing training to ensure they remain vigilant in detecting and preventing illicit activities.

Customer Due Diligence (CDD) and KYC Standards

The Company maintains a comprehensive client information system to properly identify both individual and corporate customers. This system includes detailed records of business activities, as well as verification of the client's source of funds and wealth.

• At the time of account opening, all clients undergo Know Your Customer (KYC) verification.

• Clients are screened against international sanctions lists, including the Office of Foreign Assets Control (OFAC) database, at least annually.

• Clients classified as high-risk or subject to enhanced due diligence undergo quarterly re-screening against sanctions lists.

• Where feasible, the Company will use automated software solutions to perform sanctions list screening.

Additionally, each client profile includes expected transaction patterns, allowing the Company to detect anomalies. Any unexpected transactions will automatically trigger enhanced due diligence procedures and review by the Compliance Officer.

Beneficial Ownership Verification

The Company will not establish payment accounts unless it has taken all reasonable steps to verify the identity of the beneficial owner of the funds being deposited or invested.

Scope of Application

Company personnel are required to verify the identity of all prospective clients—both individuals and corporate entities—prior to account opening. This obligation applies regardless of whether the account is registered under a personal or business name. For cash-equivalent transactions, including currency exchanges, the purchase or sale of precious metals, or cash-based subscriptions to financial instruments, employees must verify the identity of the customer and confirm the source of funds for any transaction exceeding $10,000 USD (or equivalent).

Client Identification Procedures

Individuals

For individuals without a fixed address or residing outside of Canada, identity verification must be conducted using an official government-issued document, such as:

• Passport

• National identification card

• Driver's license

Corporate Entities and Legal Persons

For businesses and legal entities, verification requires:

• Confirmation of the company's registered address through postal verification or another reliable method.

• Examination of official corporate documentation, such as:

• Certificate of incorporation

• Articles of association

• Extract from the commercial register or an equivalent authoritative source

These measures ensure compliance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and support the Company's commitment to preventing illicit financial activities.

Verification of Account Signatories

All individuals authorized to sign on behalf of a company must provide valid credentials confirming their authority. For organizations such as clubs, societies, and charitable entities, the Company will take reasonable steps to verify the legitimacy of the organization's purpose—such as requesting a copy of its constitution.

If an account requires multiple signatories, the Company will verify the identity of at least two signatories at the time of account opening. When signatories change, due diligence will be conducted to ensure that at least two active signatories have been properly verified.

Identification of the Beneficial Owner

The Company will ascertain the identity of the ultimate beneficial owner (UBO) of any assets deposited at the time of account opening.

Reasonable due diligence must be applied to determine the true ownership of funds. While the Company may initially assume that the individual or entity opening the account is the beneficial owner, this assumption will not apply in cases where unusual circumstances or red flags arise. If a corporate entity is acting as the account holder, the Company must document the entity's legal name, registered address, and country of incorporation.

Handling Cases of Uncertainty

If there is any doubt about the legitimacy of a client's identity or the source of funds, the following procedures must be followed:

1. Enhanced Verification – The Company's internal compliance team and external auditors will conduct additional checks to validate client information. Clients will be screened against databases such as:

• World Compliance

• The U.S. Department of the Treasury - Office of Foreign Assets Control (OFAC)

2. Record-Keeping – The Company must maintain detailed records of:

• Client names and registered business names (if applicable)

• Address and country of residence/incorporation

• Methods used to verify identity

• Supporting corporate documentation for legal entities

3. Ultimate Beneficial Owner (UBO) Disclosure – If there is doubt regarding beneficial ownership, the Company will require a written declaration from the client stating whether they are acting on their own behalf or for a third party. If acting on behalf of another party, they must disclose the identity of that third party.

Indicators Requiring Additional Scrutiny

The Company will subject an account to further review if any of the following red flags arise:

• The account is opened with an associated power of attorney granted to an unrelated third party, particularly a foreign national.

• A client's known financial situation does not align with the assets being deposited or transferred.

• An account is requested by a foreign individual or entity introduced by a third party, with no clear business justification.

• A foreign client is opening an account remotely via correspondence, without any prior personal engagement with the Company.

• The client exhibits unusual behavior during the account opening process, raising concerns about their intentions.

If reasonable doubt remains after further review and cannot be resolved through additional due diligence, the Company must decline the account opening request.

Independent Audits and Regulatory Inspections

The Company's AML policies and procedures will be subject to an annual independent audit to ensure ongoing compliance. Furthermore, the Company remains prepared for both scheduled and unscheduled regulatory audits by FINTRAC and other relevant authorities.

Prohibited Activities

All Company personnel are strictly prohibited from engaging in the following activities:

1. Opening or maintaining accounts without verifying the identity of the account's ultimate beneficial owner (UBO).
2. Providing services to any customer without conducting thorough due diligence to ensure that the assets or funds involved originate from legitimate sources.
3. Offering services to individuals or entities engaged in online gambling, including internet-based casinos.
4. Disclosing client information to third parties except as permitted by this policy or as required by law.

Suspicious Transaction Reporting (STR)

The Company follows a strict policy of reporting all suspected money laundering or suspicious transactions to the appropriate regulatory body, as required under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). Suspicious Transaction Reports (STRs) will be submitted to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) when:

- Transactions appear unusually complex, large, or lack an obvious lawful purpose.
- There are repetitive small transactions with no apparent business justification.
- A client exhibits unusual financial behavior inconsistent with their stated income or business operations.

Common Indicators of Suspicious Activity

The Company will evaluate the following risk factors when determining whether to file an STR:

1. The client's financial lifestyle appears inconsistent with their stated income.
2. Business transactions do not align with industry standards or expected financial ratios.
3. The client frequently changes accountants or bookkeepers without explanation.
4. The client is unable to provide basic corporate records upon request.
5. The client's company operates at a loss for an extended period without a clear reason.
6. The company has unusual shareholder loan activity unrelated to business operations.
7. The company makes excessive payments to subsidiaries or controlled entities in ways that deviate from normal business practices.
8. Transactions involve jurisdictions with weak anti-money laundering (AML) regulations.
9. The client openly discusses involvement in illegal activities.
10. The client is frequently accompanied or monitored by a third party during financial transactions.
11. Does the client exhibit unusual interest in internal systems, controls, or policies, or have uncommon knowledge of laws regarding suspicious transaction reporting or anti-money laundering regulations?

12. Is the client trying to persuade an employee to avoid completing the necessary documentation for the transaction?

13. Does the client provide unclear information about a transaction or attempt to excessively justify or elaborate on it?

14. Does the client appear secretive or anxious regarding the transaction?

15. Was the client's home or business phone number disconnected soon after an account was established?

16. Does the client utilize aliases or multiple similar but distinct addresses?

17. Does the client provide company employees with money, gifts, or unusual favors in exchange for services that may seem suspicious or out of the ordinary?

18. Does the client give unclear or ambiguous information?

19. Does the client present identification that appears to be false, counterfeit, altered, or inaccurate?

20. Does the client decline to provide personal identification documents?

21. Does the client try to verify their identity using means other than their personal identification documents, or attempt to open accounts under a false name?

22. Is the client's supporting documentation missing critical information, such as a telephone number, or is it otherwise difficult to verify?

23. Do the identification documents presented appear to be in pristine condition?

24. Does the client's transaction exhibit any inconsistencies or lack a legitimate economic purpose?

25. Is there a sudden emergence of significant activity on an account that has been inactive or dormant?

26. Does the transaction pertain to a country where the production or export of illicit drugs may be common, or where an effective anti-money laundering framework is lacking?

27. Does the transaction involve a country recognized or suspected of facilitating money laundering activities?

28. Does the client present multimillion-dollar deposits originating from "confidential sources"?

29. Does the client engage in transactions with an offshore "shell" company whose name bears resemblance to that of a prominent legitimate institution?

Financial institutions are obligated to maintain comprehensive internal reporting procedures and accurate records to support the creation of an audit trail during investigations and prosecutions related to money laundering. These records must encompass customer identification and associated transactions, clearly detailing the identity of all customers and the specifics of each transaction conducted on their behalf. Such records should be securely stored for a minimum of five years following the last relevant financial activity conducted by the institution. This retention period aims to ensure that authorities can access pertinent information without unnecessary delay. In cases where an investigation is ongoing at the conclusion of the five-year period, the records must be preserved until the authorities have resolved the matter. Customer identification records must explicitly indicate the type of identification evidence obtained from the customer, providing sufficient details to verify the customer's identity. A copy of this identification evidence must be retained as part of the customer's record. Transaction records must be admissible in court and should include all necessary information related to the execution of the transactions. This encompasses any records or information that contribute to entries in the financial institution's accounts or the specific account of the customer.

For instance, this includes properly executed cheques, telegraphic transfers, credit or debit slips, among others. In the case of wire transfers, it is essential that all relevant information regarding both senders and beneficiaries is included in the payment messages. When maintaining customer identification and transaction records, it is important to remember that these may serve as a basis for an audit trail. The records should contain sufficient information to enable authorities to identify:

1. the beneficial owner of an account
2. the amounts deposited and withdrawn from an account
3. the source of the funds
4. the manner in which funds were deposited and withdrawn
5. the destination of the funds
6. the identity of the individual executing the transaction
7. the method of instruction for the transaction.

Suspicious Activity Reports (SAR) File

The Compliance Officer, under the oversight of the Director, will keep a comprehensive file that includes any follow-up SARs, along with all reports and documents pertinent to the Company's investigation of the activities referenced in these reports. Furthermore, the Company is required to maintain records of any activities that were investigated but did not result in a SAR filing, including the justification for such decisions. Records of Incoming and Outgoing Wire Transfers The Compliance Officer, under the supervision of the Director, will evaluate and assess whether the observed patterns of substantial incoming wire transfers followed by outgoing transfers from the same client are warranted based on the nature of the business or customer involved. Additionally, an analysis of the types and volumes of wire transfer activities conducted by the Company will be performed. This will also encompass the methods of payment accepted for these transfers and the categories of remitters permitted, such as account holders versus non-account holders.

AML IMPROVEMENT PROCESS

The Compliance Officer of the Company, under the guidance of its Director, is tasked with understanding the relationship between those responsible for monitoring anti-money laundering (AML) efforts and the management of the Company. The Compliance Officer or the Director must ensure that the individuals overseeing AML do not possess excessive authority (both real and perceived) or influence within the Company. Conduct a management-led AML risk assessment across all significant business lines, products, and services. The Compliance Officer, under the supervision of the Director, will carry out an annual assessment, which will be managed by our Compliance Officer. The Company will evaluate risk as a function of volume, regulatory requirements, staff turnover, and regulatory scrutiny. Additionally, the Company will analyze more than just cash transactions; each line of business will be examined to assess potential vulnerabilities to money laundering activities. Please provide a copy of the most recently approved AML policies and procedures.

The Compliance Officer, under the guidance of the Director, will keep detailed records of the last review conducted by the Board of Directors concerning the Company's policies and procedures. The Board of Directors endorses the Company's Anti-Money Laundering (AML) initiatives and is dedicated to providing the necessary personnel and resources to implement this policy effectively. The Company will ensure that the AML policy is aligned with the current regulatory landscape and will conduct an annual review. The most recent Board-approved Know Your Customer (KYC) Policy will be properly maintained. The Compliance Officer, under the supervision of the Director, will implement any future amendments and ensure adherence to the policy by staff through semi-annual training sessions. The Company will consult with FINTRAC's Financial Intelligence to stay updated on AML developments and will incorporate necessary changes into the Company Policy and Procedure Manual. The policy and procedures related to Suspicious Activity Report (SAR) reporting and monitoring requirements will be properly maintained.

The Compliance Officer, under the Director's supervision, will assess how the Company manages its SAR obligations, ensuring that all departments comprehend their responsibilities in reporting suspicions for centralized evaluation and filing. Lessons learned, particularly regarding the reporting of illegal or suspicious activities that may impact the Company, will be documented. The most recent independent audit results concerning compliance, along with management's responses, will be reviewed. The Compliance Officer, under the Director's supervision, will evaluate the latest audit to ascertain whether the Company is performing adequately in this regard. The Company will maintain comprehensive AML training records, including schedules with dates, attendees, and topics covered. These records will be managed by the Compliance Officer or Director, and meetings discussing these subjects will be documented as part of the records. Additionally, it will be ensured that employees who require initial or further training are identified.

Training materials utilized for educational purposes will be maintained by the Compliance Officer, who operates under the guidance of the Director. This documentation will encompass information disseminated to educate Company employees regarding Anti-Money Laundering (AML) obligations.