ANTIMONEY LAUNDERING POLICY

Mega Fusion Group (Pty) Ltd
Company Number 2024 / 073707 / 07, Financial Services Provider ('FSP') Number 54221
Authorized and regulated by The Financial Sector Conduct Authority, South Africa (the 'FSCA')

Table of contents

This Policy has been in accordance with the provisions of the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001), as amended by the following legislation:

- Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004)
- Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008)
- General Intelligence Laws Amendment Act, 2013 (Act No. 11 of 2013)
- Financial Intelligence Centre Amendment Act, 2017 (Act No. 1 of 2017)

This Policy manual sets out the procedures required to ensure compliance with the aforementioned legislation and any related regulatory obligations.

1. Purpose

The purpose of this Anti-Money Laundering (AML) Policy is to establish the measures, procedures, and responsibilities necessary to prevent and detect money laundering and the financing of terrorism within Mega Fusion Group (Pty) Ltd ("the Company"). This policy is designed to ensure compliance with all applicable Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) laws and regulations.

Furthermore, this policy sets out the procedures for conducting customer identification and verification in accordance with Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements.

2. Policy Statement

Mega Fusion Group (Pty) Ltd is committed to upholding the highest standards of integrity and full compliance with all relevant AML and CTF laws and regulations. The Company strictly prohibits any engagement, whether direct or indirect, in activities that may facilitate money laundering, terrorist financing, or any other form of financial crime.

All employees, contractors, agents, and third-party service providers associated with the Company are required to adhere to the provisions of this policy and ensure strict compliance with AML obligations.

This policy applies to all customers of the Company, including natural persons, legal entities, and other organizations, irrespective of their jurisdiction or nature of business.

3. Definitions

Accountable Institutions (AI)

According to the provisions of the "2001 Financial Intelligence Center Act," entities or individuals that are obligated to comply with anti-money laundering (AML) and counter-terrorism financing (CTF) obligations are generally referred to as "responsible institutions." These institutions include, but are not limited to, publicly listed companies, lawyers, real estate agents, insurance companies and intermediaries, as well as mutual fund management companies.

These institutions are considered particularly vulnerable to infiltration by money laundering activities, and therefore must adhere to specific legal and regulatory requirements, as well as strengthen internal controls and risk management to ensure compliance with AML and CTF regulations, thereby preventing the occurrence of financial crimes.

Within the financial services industry, the definition of a "responsible institution" applies equally to any entity or individual providing financial services, particularly those engaged in foreign exchange transactions, investment services, or other activities related to the movement of funds. These institutions and individuals are required to comply with the relevant regulations to safeguard the transparency and stability of the financial system.

Beneficial Owner

In relation to a legal entity, a "Beneficial Owner" refers to a natural person who, whether independently or jointly with another person, directly or indirectly:

(a) Holds a majority ownership interest in the legal entity; or

(b) Having substantial control over the legal entity, including but not limited to holding positions such as Chief Executive Officer, Non-Executive Director, Independent Non-Executive Director, Director, Manager, or Trustee, etc. (such individuals may also be referred to as "controllers").

The determination of a beneficial owner is not solely based on formal ownership or managerial records. For instance, where a company is owned by another company or a trust, the true beneficial owners are the natural persons who ultimately control or benefit from that secondary entity or trust.

Cash / Cash Transaction

"Cash" or a "Cash Transaction" refers to coins and banknotes (paper money) of the Republic of South Africa or any other sovereign state, which are legally designated as tender and customarily used as a medium of exchange within the issuing country. This definition also includes travelers' cheques.

However, "Cash" excludes the following:

(a) Negotiable instruments, such as promissory notes or bills of exchange;

(b) Non-physical fund transfers, including transactions conducted via bank cheques, bank drafts, electronic funds transfers (EFTs), wire transfers, or any other form of written payment order that does not involve the direct exchange of physical currency.

CDD Procedures

Customer Due Diligence (CDD) procedures refer to the processes undertaken to identify and verify the identities of clients in accordance with applicable Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations.

Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) refers to the implementation of additional investigative and verification measures when a client or transaction is classified as high-risk for Money Laundering (ML) or Terrorist Financing (TF). This includes obtaining supplementary information, conducting heightened monitoring, and implementing enhanced scrutiny of business relationships.

Money Laundering

Refers to any act intended to conceal, disguise, or obscure the nature, source, location, disposition, or transfer of illicit proceeds. These acts include, but are not limited to: facilitating the entry of illegal funds into the legitimate financial system through transactions or other means; as well as any criminal acts specified under Article 64 of the Financial Intelligence Center Act, or Articles 4, 5, and 6 of the Organized Crime Prevention Act.

Politically Exposed Persons (PEPs)

Refers to individuals who, due to holding prominent public positions, may be exposed to higher risks of bribery, corruption, or money laundering. Due to their roles and influence, these politically exposed persons (PEPs) have a higher likelihood of encountering assets obtained through illicit means. They can be categorized into the following risk categories: domestic politically exposed persons, foreign politically exposed persons, and politically exposed persons related to international organizations. When conducting business with such individuals, enhanced due diligence measures should be adopted to mitigate the risk of financial crimes.

Prevention of Organised Crime Act (POCA)

The Prevention of Organised Crime Act, 121 of 1998 establishes the primary legal framework for combating money laundering, organised crime, and related offences. It provides for the prosecution of money laundering offences and the confiscation or forfeiture of proceeds derived from criminal activities.

Proceeds of Crime

Any financial gain, monetary benefit, or asset obtained directly or indirectly as a result of criminal conduct.

Proceeds of Unlawful Activities

Any property, service, advantage, benefit, or reward acquired, received, or retained whether directly or indirectly, within the Republic of South Africa or elsewhere, at any time before or after the enactment of POCA, as a result of unlawful activity. This includes any property that represents or is derived from such unlawfully acquired assets.

Single Transaction

A transaction that is not conducted within the context of an ongoing business relationship and where the transaction value meets or exceeds ZAR 5,000.00 (Five Thousand South African Rand), except as otherwise stipulated under Section 20A of FICA.

Smurfing, Splitting, Structuring

Techniques used in Money Laundering that involve breaking down large sums of illicit funds into smaller amounts through multiple transactions to evade detection by financial authorities.

Suspicious Activity Reporting (SAR)

Pursuant to Section 29(1) of the Financial Intelligence Centre Act, a responsible institution is required to submit a Suspicious Activity Report (SAR) when there are reasonable grounds to suspect that a particular activity involves proceeds of unlawful conduct or money laundering. The reporting obligation applies not only to transactions between two or more parties but also extends to activities that, despite not resulting in a transaction, still raise suspicion. Furthermore, pursuant to Section 29(2) of the Financial Intelligence Centre Act, the reporting requirement also encompasses reports concerning transactions that have not yet been completed but have raised suspicion, including transaction inquiries that may indicate potential illicit activity.

Suspicious or Unusual Transaction Report (STR)

Pursuant to Section 29(1) of the Financial Intelligence Centre Act, a responsible institution is required to submit a Suspicious or Unusual Transaction Report (STR) when there is suspicion that a particular transaction or a series of transactions involves proceeds of unlawful conduct or money laundering. Unlike a Suspicious Activity Report (SAR), an STR primarily pertains to transactions involving two or more parties.

Transaction

Refers to any agreement or arrangement established between a client and a responsible institution, conducted within the scope of the institution's business operations. Such transactions are not limited to financial transactions involving the movement of funds.

Unlawful Activity

Any act, omission, or conduct that constitutes an offence or violates any law, regardless of whether the act took place before or after the enactment of POCA (The Prevention of Organised Crime Act) and irrespective of whether it occurred within South Africa or in another jurisdiction.

Verification

The process by which an Accountable Institution (AI) is required to authenticate the identity and information provided by a client. This involves obtaining, reviewing, and comparing relevant documentation or data to ensure the accuracy and legitimacy of the information supplied.

4. AML Compliance Officer

The Company shall appoint an Anti-Money Laundering Compliance Officer ("AML Compliance Officer") responsible for establishing, implementing, and continuously overseeing the Company's anti-money laundering ("AML") program. The AML Compliance Officer shall ensure that the Company does not become a vehicle for money laundering activities and is safeguarded against legal and financial risks. The responsibilities of the AML Compliance Officer include:

4.1 Develop and Maintain AML Policies and Procedures

Ensuring the development, review, and periodic update of comprehensive Anti-Money Laundering ("AML") policies and procedures in compliance with applicable laws and regulations. Such policies must align with AML best practices to effectively prevent money laundering and terrorist financing activities while providing clear guidance for the Company's daily operations.

4.2 Ensure Employee Training on AML Requirements

Ensuring that all employees, agents, and relevant personnel regularly participate in comprehensive and detailed Anti-Money Laundering ("AML") compliance training. Such training shall cover legal and regulatory requirements, internal policies and procedures, methods for identifying suspicious activities, and guidance on taking appropriate actions in accordance with applicable laws and the Company's internal processes.

4.3 Monitor and Report Suspicious Activities

The AML Compliance Officer shall implement robust systems and controls to monitor transactions and business activities for suspicious behavior, and where necessary, report such activities to the relevant authorities in accordance with statutory reporting requirements under the applicable anti-money laundering laws and regulations.

4.4 Conduct Periodic Risk Assessments

Conducting regular comprehensive risk assessments to identify, analyze, and evaluate potential risks related to money laundering or terrorist financing. The scope of such risk assessments shall include, but not be limited to, the following areas: customer relationship reviews, business model and operational processes, and the monitoring and evaluation of emerging risks. The assessment results shall be utilized to optimize internal controls and ensure the effectiveness of risk management measures.

4.5 Stay Informed on Legal and Regulatory Developments

The AML Compliance Officer shall continuously monitor and keep abreast of changes in AML laws, regulations, and guidelines issued by relevant regulatory bodies. This includes updating internal policies and practices to reflect new legal developments, ensuring ongoing compliance with domestic and international AML requirements.

5. Customer Due Diligence (CDD) – Identification and Verification

5.1 The Company shall ensure the implementation of comprehensive customer due diligence procedures, which shall, at a minimum, include the identification and verification of customer identities, in compliance with applicable anti-money laundering and counter-terrorist financing laws and regulations.

5.2 This procedure shall involve the collection, verification, and retention of accurate and complete information to ensure the proper identification of each customer. The specific requirements shall include, but are not limited to, the following key personal information:

(a) Full Name

The legal name as stated on official documents

(b) Date of Birth

The customer's date of birth to establish their legal age and identity

(c) Identity Number or Passport Number

A government-issued identification number that uniquely identifies the individual within their jurisdiction

(d) Residential Address

The customer's current residential address to ensure they are a legal resident or have a valid connection to the address provided.

(e) Email Address

An effective and contactable email address, used for subsequent communication and confirmation.

(f) Telephone Number

A valid contact phone number, for verifying communication information and for further contact with the customer when necessary.

(g) Source of Funds

For transactions involving funds, the company must thoroughly understand and record the source of the funds, including detailed payment methods, the origin of the funds, and the party responsible for the payment. The company must ensure complete understanding of these details and maintain accurate records.

5.3 Record-Keeping of Customer Information

The company shall properly retain and securely store all customer information collected during the customer due diligence process. These records should include detailed data used to verify the customer's identity and must be readily available to meet legal and regulatory requirements. These records should be managed in accordance with the retention periods specified by applicable laws.

5.4 Ongoing Monitoring of Customer Transactions

The company shall establish and implement procedures for the continuous monitoring of customer transactions. This monitoring is designed to detect and assess any abnormal or suspicious activities that may involve money laundering, terrorist financing, or other illegal activities. The company will regularly review customer transactions to ensure they are consistent with the customer's business profile and financial activities.

5.5 Verification Methods

(a) Individual Identity Verification

The company shall utilize government-issued original identification documents for the verification of individual customer identities. These documents may include, but are not limited to, South African driver's licenses, passports, or identity cards for South African nationals. For non-South African clients, the company will verify their passport or other valid government-issued identification documents from their country of origin. All documents will be reviewed to ensure the provided information matches the identity, and any discrepancies or inconsistencies will be promptly addressed and investigated.

(b) Business Identity Verification

The company shall review and verify the original registration documents, including but not limited to the certificate of incorporation, business registration certificate, and other official documents issued by government authorities. These documents should include accurate and up-to-date information regarding the company's legal name, registration number, and the jurisdiction of registration. If necessary, the company may request additional supporting documents, such as partnership agreements or articles of association, to verify the company's legal structure and ownership.

(c) Beneficial Owner Identification and Verification

The company shall conduct comprehensive beneficial owner identification and review, regardless of whether the client is an individual or a business. A beneficial owner is an individual who ultimately owns or controls the client entity, or a person who has significant influence over the client through holding shares, voting rights, or control. The company will ensure the accurate identification of beneficial owners and collect sufficient information to confirm the ownership structure of corporate clients. If a beneficial owner holds more than 25% of shares, voting rights, or control, such ownership will be identified and verified. In cases where the ownership structure is complex or the beneficial owner is difficult to identify, the company will conduct enhanced due diligence.

(d) Politically Exposed Person (PEP) Screening

As part of the company's due diligence process, all clients and their beneficial owners will undergo screening against politically exposed persons (PEP) lists. A politically exposed person is an individual who holds or has held a prominent public position or function in a government, international organization, or political party. Such positions include heads of state, senior politicians, judicial officials, senior military officers, or top management in state-owned enterprises, among others. Additionally, the company will screen relatives or business partners closely associated with these politically exposed persons, as these relationships may present risks related to money laundering or terrorist financing. The screening process will be conducted using both internal systems and external, updated politically exposed person databases, ensuring a thorough examination of any client or partner potentially involving high risk.

(e) Use of Third-Party Data Sources for Verification

To assist in identifying and verifying beneficial owners, the company will utilize trusted third-party data sources, including but not limited to government registries, business databases, and commercial information providers. These external data sources provide essential information about the legal status, ownership structure, and financial background of entities and individuals, which will be cross-checked with the documentation provided by clients. This process will help ensure the accuracy, timeliness, and compliance of all verification information with applicable anti-money laundering and counter-terrorism financing regulatory requirements.

6. Undertaken AML Measures

6.1 Reporting Suspicious Activities

All employees of the Company are mandated to promptly report any suspicious activity or transaction that may be indicative of money laundering, terrorist financing, or any other illicit financial conduct. Such reports must be made to the AML Compliance Officer without undue delay. The Company is obligated to submit Suspicious Activity Reports (SARs) to the appropriate regulatory authorities, law enforcement agencies, or other relevant bodies, in compliance with applicable laws, regulations, and reporting obligations under Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) legislation.

6.2 Record-Keeping

The Company is required to maintain comprehensive and accurate records of customer identification, due diligence documentation, and transaction history. These records shall be retained for a minimum period as mandated by relevant statutory and regulatory provisions, including but not limited to the Financial Intelligence Centre Act (FICA) and other applicable national and international laws. All records shall be readily available for review by regulatory authorities upon request, and must be securely stored to prevent unauthorized access or data breaches.

6.3 Employee Training

The company shall provide ongoing and comprehensive anti-money laundering training to all employees, agents, and relevant parties, ensuring they fully understand their responsibilities under the company's anti-money laundering policies and procedures. The training will cover how to identify suspicious activities, reporting processes, employees' legal obligations, and potential penalties for non-compliance. Training shall be conducted regularly and updated whenever there are significant changes in laws or internal procedures. All training activities must be documented and tracked to comply with regulatory requirements.

6.4 Sanctions Screening

The Company shall implement a robust sanctions screening process to ensure compliance with applicable international and domestic sanctions regimes. Customers and their transactions shall be screened against relevant sanctions lists, including those maintained by national and international regulatory bodies such as the United Nations, the European Union, and the Office of Foreign Assets Control (OFAC). The Company shall take all necessary steps to prevent engaging in any business relationships or transactions with prohibited individuals, entities, or jurisdictions subject to sanctions.

6.5 Independent Review

The AML program shall undergo periodic independent reviews, audits, or assessments conducted by qualified, external parties to evaluate its effectiveness, efficiency, and compliance with applicable laws, regulations, and internal policies. The reviews will assess whether the Company's AML procedures are being implemented appropriately and whether they effectively mitigate risks associated with money laundering and terrorist financing. The findings from such reviews shall be used to enhance the program and ensure it remains fit for purpose.

6.6 Non-Retaliation

The Company expressly prohibits any form of retaliation, discrimination, or adverse action against employees who report suspected violations of AML laws or Company policies in good faith. Employees are encouraged to report any concerns or suspicions without fear of retaliation or reprisal. The Company shall ensure that all reports made in good faith are handled confidentially and investigated thoroughly, with appropriate protection for whistleblowers.

6.7 Penalties for Non-Compliance

Failure to comply with the company's anti-money laundering policies and procedures may result in disciplinary action, including but not limited to suspension, termination of employment, or termination of contractual relationships with the company. The specificity and severity of the penalties will be determined based on the nature of the violation and the risks it poses to the company, stakeholders, or the financial system. The company reserves the right to take legal action when necessary to protect its interests and comply with applicable laws.

6.8 Reporting Violations

Any violations of the AML policy, or any suspicions of money laundering, terrorist financing, or other illicit financial activities, must be reported immediately to the AML Compliance Officer. Prompt reporting is essential for the Company to address and mitigate potential risks, ensure compliance with the law, and take appropriate remedial actions. Employees are reminded of their duty to report all such concerns without delay, and to cooperate fully with any investigations initiated by the Company or regulatory authorities.

7. Obligations of the Company

The company is fully committed to complying with all relevant regulatory requirements and taking proactive measures to prevent money laundering and the financing of terrorism. We will diligently implement, enforce, and continually review our anti-money laundering and anti-terrorism financing policies and procedures to ensure that our products and services are not misused or employed for illegal activities. To this end, we will implement effective control mechanisms, promptly detect and report suspicious transactions, and conduct thorough due diligence to ensure the legality of our clients and their financial transactions.

The Company is also dedicated to adhering to all applicable Know Your Customer (KYC) requirements as mandated by the relevant regulatory authorities. We will ensure that our KYC procedures remain comprehensive, effective, and aligned with the latest regulatory updates and industry best practices. To this end, the Company will conduct periodic reviews and updates of our KYC policies to ensure they reflect current legal standards and effectively mitigate risks associated with money laundering and terrorist financing.

Further, the Company undertakes to maintain a robust internal framework for monitoring and assessing the risk of money laundering and terrorist financing within its operations. This includes providing regular training to employees, conducting internal audits, and ensuring that any changes in the regulatory landscape are swiftly incorporated into our practices. The Company will take all necessary steps to ensure full compliance with Anti-Money Laundering and Counter-Terrorist Financing laws, thereby safeguarding the integrity of our operations and the financial system.

8. Amendments

The company will, as necessary, revise, update, or modify its anti-money laundering and customer identification policies to ensure ongoing compliance with applicable laws, regulations, and industry standards. These revisions may arise from new legislative requirements, regulatory guidelines, or changes in best practices related to the prevention of money laundering, the financing of terrorism, and other financial crimes.

The Company commits to monitoring and reviewing relevant legislative and regulatory developments to ensure that this policy remains aligned with current legal obligations. Any changes or updates to the policy will be communicated to employees, customers, and stakeholders, as appropriate, and will be implemented promptly to maintain the Company's compliance framework.

Where necessary, the Company will also consult with legal and regulatory experts to ensure that all amendments are fully compliant with national and international requirements. These amendments may include, but are not limited to, adjustments in Customer Due Diligence (CDD) procedures, risk assessment methodologies, reporting obligations, and any other aspect of the AML and KYC processes.