Unofficial English Translation

Guidelines for the prevention and suppression of money laundering and financing of terrorism for auditors, accountants and tax advisers

1. Preface

1.1 With the purpose of preventing and suppressing money laundering and terrorist financing, Law No. 2/2006– Prevention and Suppression of the Crimes of Money Laundering and Law No. 3/2006 – Prevention and Suppression of the Crimes of Terrorism, amended by Law No. 3/2017, and Administrative Regulation No. 7/2006– Preventative Measures for the Crimes of Money Laundering and Financing of Terrorism, amended by Administrative Regulation No. 17/2017, are promulgated.

1.2 When participating or assisting, in the exercise of their professional activities, in the operations listed in paragraph 5) of Article 6 of Law No. 2/2006, amended by Law No. 3/2017, or preparing or performing operations for a client within the scope of the activities listed in paragraph 6) of the same article, auditors, accountants and tax advisers are obliged to carry out preventive obligations. These guidelines aim to implement the prerequisites referred to in paragraph 1) of Article 3 and Article 7 of Administrative Regulation No. 7/2006, amended by Administrative Regulation No. 17/2017, as well as to systematize the procedures for compliance with the duties specified in Article 7 of Law No. 2/2006, in Article 11 of Law No. 3/2006, amended by Law No. 3/2017, and in Article 3 to Article 8 of Administrative Regulation No.7/2006, amended by Administrative Regulation No. 17/2017,.

2. General provisions

2.1 Auditors, accountants and tax advisers are obligated to comply with the duties provided for in paragraph 2.3, when participating or assisting, in the exercise of their professional activities, the operations of:

2.1.1 buying and selling of real property;

2.1.2 management of client funds, securities or other assets;

2.1.3 management of banks, savings or securities accounts;

2.1.4 organization of contributions for the creation, operation or management of companies;

2.1.5 creation, operation or management of legal persons or entities without legal personality, and buying and selling of business entities.

2.2 When auditors, accountants and tax advisers prepare or perform operations for a client, within the scope of the following operations, they also have to comply with the duties in paragraph 2.3:

2.2.1 acting as a formation agent of legal persons;

2.2.2 acting as a director or secretary of a company, a partner, or a similar position in relation to other legal persons;

2.2.3 providing a registered office, business address, correspondence or administrative address for a company, or any other legal person or entities with legal personality;

2.2.4 acting as a trustee;

2.2.5 acting as a partner of a company on behalf of another person;

2.2.6 carrying out the measures necessary for a third party to act in the manner prescribed in paragraphs 2.2.2, 2.2.4 and 2.2.5.

2.3 Auditors, accountants and tax advisers are required to perform the following duties:

2.3.1 adopt customer due diligence measures, including the duty of identification and verification of the identity concerning the contracting parties and clients;

2.3.2 adopt adequate measures to detect operations suspected of money laundering and terrorism financing;

2.3.3 refuse to perform operations, when the necessary information is not provided for the compliance with the duties established in paragraphs 2.3.1 and 2.3.2;

2.3.4 keep records, for a reasonable period of time, relative to the compliance with the duties established in paragraphs 2.3.1 and 2.3.2;

2.3.5 report operations, or attempted operations, regardless of their amounts, when they indicate the commission of the criminal offence of money laundering or terrorism financing;

2.3.6 collaborate with all the authorities with competence in the prevention and suppression of the criminal offence of money laundering and terrorism financing.

3. Assessing risks and applying a risk-based approach

3.1 Auditors, accountants and tax advisers should be required to take appropriate steps to identify and assess their money laundering and terrorist financing (ML/TF) risks (for customers, countries or jurisdictions; and products, services, transactions or delivery channels). This includes being required to:

3.1.1 document risk assessments;

3.1.2 consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation measures to be applied;

3.1.3 keep these assessments up to date;

3.1.4 have effective mechanisms to provide risk assessment information to competent authorities.

3.2 Auditors, accountants and tax advisers should be required to:

3.2.1 have policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified;

3.2.2 monitor the implementation of those controls and to enhance them if necessary; and

3.2.3 take enhanced measures to manage and mitigate the risks where higher risks are identified.

3.3 When assessing risk, all the relevant risk factors should be considered before determining what are the level of overall risk and the appropriate level of mitigation measures to be applied. Auditors, accountants and tax advisers may differentiate the extent of measures, depending on the type and level of risk element for the various risk factors (e.g. in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa).

3.4 Auditors, accountants and tax advisers should identify and assess the money laundering and terrorist financing risks that may arise in relation to:

3.4.1 the development of new products, new services and new delivery mechanisms;

3.4.2 the use of new or developing technologies for both new and pre-existing products.

4. Internal controls

4.1 Auditors, accountants and tax advisers should implement programs against ML/TF, which have regard to the ML/TF risks and the size of the business, and which include the following internal policies, procedures and controls:

4.1.1 compliance management arrangements, including the appointment of a compliance officer at the management level;

4.1.2 screening procedures to ensure high standards when hiring employees;

4.1.3 an ongoing employee training program; and

4.1.4 an independent audit function to test the system.

4.2 If the auditor, accountant and tax adviser is part of a group, the group should be able to implement group-wide programs against ML/TF, including policies and procedures for sharing ML/TF information[1]. In case of foreign branches or subsidiaries of the group, they should ensure that the branches or subsidiaries apply AML/CFT measures consistent with the home country requirements if the minimum AML/CFT requirements of the host country are less strict than those of the home country.

4.3 The compliance officer referred in paragraph 4.1.1 should have a senior management position within the organization structure, and is responsible to execute, co-ordinate and follow-up of activities against ML/TF, including:

4.3.1 handling of internal reporting, and when necessary, submission of reports to the Financial Intelligence Office;

4.3.2 ongoing monitoring of the adequacy of internal policies and procedures to ensure they comply with the requirements by relevant regulations and guidelines.

4.4 When a sole practitioner has no other employees, it is deemed that the sole practitioner fulfills the role of the compliance officer.

5. Customer due diligence and measures to detect suspicious operations

5.1 Auditors, accountants and tax advisers should not have business relationship with clients who is anonymous or provides a fictitious name.

5.2 Auditors, accountants and tax advisers should undertake CDD measures for the identity of clients and beneficial owners. The measures to be taken are as follows:

5.2.1 identifying the client and verifying that client's identity using reliable, independent source documents, data or information;

5.2.2 identifying the beneficial owner, and taking reasonable measure to verify the identity of the beneficial owner, such that the auditor, accountant and tax adviser are satisfied that they know who the beneficial owner is. For legal persons and arrangements this should include understanding of the ownership and control structure of the client.

[1] Whenever in the context of a risk analysis exercise of financial transactions or the underlying economic activity, a new method or typology of money laundering or financing of terrorism is identified and determined as relevant in the context of the risk management of the economic group and even on the cases where such transaction has been reported as suspect, the underlying information may be shared within entities of the same group, safeguarding the compliance of any other legal obligations.

5.2.3 understanding and obtaining information on the purpose and intended nature of the business relationship.

5.2.4 conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the auditor/accountant/tax adviser's knowledge of the clients, their business and risk profile, including, where necessary, the source of funds.

5.3 When performing the CDD measures specified under paragraphs 5.2.1 and 5.2.2, auditors, accountants and tax advisers should also be required to verify that any person purporting to act on behalf of the client is so authorized, and should identify and verify the identity of that person.

Individual clients

5.4 Auditors, accountants and tax advisers should institute effective procedures for obtaining reliable evidence of the identity of individual clients and/or beneficial owners including obtaining information about the name, type and number of identification document and the date of issuance, permanent residential address, contact numbers, date of birth, nationality, and profession and professional domicile.

CDD measures required for legal persons and legal arrangements

5.5 When performing CDD measures in relation to clients that are legal persons or legal arrangements, auditors, accountants and tax advisers should be required to identify and verify the client and understand the nature of its business and its ownership and control structure.

5.6 For clients that are legal persons or legal arrangements, the auditors, accountants and tax advisers should identify the client and verify its identity through the following information:

5.6.1 name, legal form and proof of existence;

5.6.2 the powers that regulate and bind the legal person or arrangement (e.g. articles of association of a company), as well as the names of the relevant persons having a senior management position in the legal person or arrangement;

5.6.3 the address of the registered office and, if different, a principal place of business.

5.7 Auditors, accountants and tax advisers should identify and take reasonable measures to verify the identity of beneficial owners through the following information:

5.7.1 For legal persons:

5.7.1.1 The identity of the natural persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership) who ultimately have a controlling ownership interest in a legal person;

5.7.1.2 to the extent that there is doubt under paragraph 5.7.1.1 as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means.

5.7.1.3 Where no natural person is identified under paragraph 5.7.1.1 or 5.7.1.2, auditors, accountants and tax advisers should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.

5.7.2 For legal arrangements:

5.7.2.1 Trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust;

5.7.2.2 Other types of legal arrangements – the identity of persons in equivalent or similar positions.

5.8 Where the client or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements which impose requirements to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

Timing of verification

5.9 Auditors, accountants and tax advisers are required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers; or (if permitted) may complete verification after the establishment of the business relationship, provided that:

5.9.1 this occurs as soon as reasonably practicable;

5.9.2 this is essential not to interrupt the normal conduct of business; and

5.9.3 the ML/TF risks are effectively managed.

5.10 Auditors, accountants and tax advisers are required to adopt risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification.

Existing customers

5.11 Auditors, accountants and tax advisers are required to apply CDD requirements to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

Enhanced CDD measures

5.12 There are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced CDD measures have to be taken. Examples of potentially higher-risk situations include:

5.12.1 Non face-to-face clients;

5.12.2 Non-resident clients;

5.12.3 Large cash transactions;

5.12.4 Legal persons and legal arrangements with complex structure;

5.12.5 The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance with the client);

5.12.6 Clients from high risk countries.

5.13 Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

5.13.1 obtaining additional information on the client, including the identity and business background of the client, the intended nature of the business relationship, the source of funds or source of wealth, etc.;

5.13.2 updating more regularly the information of the client and beneficial owner;

5.13.3 obtaining the approval of senior management to commence or continue the business relationship;

5.13.4 conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

5.13.5 requiring the first payment to be carried out through an account opened with a bank subject to similar CDD standards.

Politically exposed persons

5.14 Foreign politically exposed persons (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country or jurisdiction other than Macao[2], for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.

5.15 In relation to foreign politically exposed persons (PEPs) (whether as client or beneficial owner), in addition to performing normal customer due diligence measures, auditors, accountants and tax advisers are required to:

5.15.1 have appropriate risk-management systems to determine whether the client or the beneficial owner is a politically exposed person;

5.15.2 obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;

5.15.3 take reasonable measures to establish the source of wealth and source of funds;

5.15.4 conduct enhanced ongoing monitoring of the business relationship.

5.16 Auditors, accountants and tax advisers should be required to take reasonable measures to determine whether a client or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization (for example, directors, deputy directors and members of the board). In cases of a higher risk business relationship with such persons, auditors, accountants and tax advisers should be required to apply the measures referred to in paragraphs 5.15.2, 5.15.3 and 5.15.4.

5.17 The requirements for all types of PEP should also apply to family members or close associates of such PEPs

[2] For the application of paragraphs 5.14 to 5.17, only PEPs of Macao are classified as domestic PEPs. All PEPs originated from other regions of China are classified as foreign PEPs.

Higher risk countries or jurisdictions

5.18 The Financial Action Task Force (FATF, http://www.fatf-gafi.org) and the Asia/Pacific Group on Money Laundering (APG, http://www.apgml.org) have named those countries and jurisdictions with inadequate rules and practices to fight against money laundering and terrorist financing in a "public statement", which is published on their websites. The FATF and APG also review periodically the progress of these jurisdictions in addressing their situation.

5.19 Auditors, accountants and tax advisers shall perform enhanced CDD measures for those clients, business relations or transactions from these countries or jurisdictions as they present a higher risk for money laundering and terrorist financing.

5.20 Auditors, accountants and tax advisers should consider applying countermeasures to those clients, business relations or transactions from these countries or jurisdictions when called upon by international, national or domestic competent authorities. Examples of countermeasures include ongoing due diligence, close monitoring and limiting business relationship or transactions, etc.

5.21 In addition to the "public statement" referred in paragraph 5.18, auditors, accountants and tax advisers should exercise enhanced measures in respect of clients (including beneficial owners) from countries and jurisdictions named in other international sanction lists.

Reliance on third parties for CDD measures

5.22 If auditors, accountants and tax advisers rely on third-party to perform the CDD measures set out in paragraphs 5.2.1 to 5.2.3, the ultimate responsibility for CDD measures should remain with the auditors, accountants and tax advisers relying on the third party, which should be required to:

5.22.1 obtain immediately the necessary information concerning the CDD measures set out in paragraphs 5.2.1 to 5.2.3;

5.22.2 take steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;

5.22.3 satisfy themselves that the third-party is regulated, and supervised or monitored for, and has CDD measures and record-keeping requirements in place;

5.22.4 have regard to information available on the level of country risk, when determining in which countries the third party that meets the conditions can be based.

5.23 In case the third party is part of a group, auditors, accountants and tax advisers should ensure that the group apply adequate CDD measures, record-keeping requirements and programs against money laundering and terrorist financing, of which implementation is supervised at a group level by a competent authority. Any higher country or jurisdiction risk is mitigated by the group's AML/CFT policies.

6. Refuse to perform specific operations

6.1 Auditors, accountants and tax advisers should refuse the performance of any operations in the event that they are denied access to necessary information to adopt CDD measures to detect suspicious transactions.

7. Record keeping

7.1 Auditors, accountants and tax advisers are required to maintain all necessary records on transactions for at least five years following completion of the transaction. Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

7.2 Auditors, accountants and tax advisers should keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence, and results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years following the termination of the business relationship.

7.3 Retention may be by way of original documents, stored on microfiche, or in computerized form provided that such forms are accepted as evidence. In situation where the records relate to ongoing investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed.

8. Report suspicious operations

8.1 If auditors, accountants and tax advisers have reasonable justifications to suspect any person of committing crimes of money laundering or financing of terrorism discovered during their course of analysis of the nature, complexity, amount involved and frequency of transactions or unusual circumstances arisen thereof, they should report these activities to the "Financial Intelligence Office", established by Order of

the Chief Executive No.227/2006, within two working days from which the performance of such activities have been detected.

8.2 If auditors, accountants and tax advisers refuse to perform corresponding operations due to the occurrence of conditions referred in 6.1, or were not successful in performing operations for other reasons, they should also report to the Financial Intelligence Office within two working days from the day of refusing such operations.

8.3 Reporting of suspicious transactions should be made in the standard form prescribed by the Financial Intelligence Office.

8.4 Auditors, accountants and tax advisers are prohibited from disclosing, to contract parties, clients or third parties, the fact of their report to the Financial Intelligence Office regarding suspicious transactions or corresponding information[3].

9. Duties to collaborate

9.1 Auditors, accountants and tax advisers should cooperate with all the competent authorities for the prevention and suppression of the crimes of money laundering and terrorist financing (namely the Court, Public Prosecutions Office, Judiciary Police, Financial Intelligence Office and Financial Services Bureau), disclosing all the information and documents requested by such authorities.

10. Penalties

10.1 In accordance with Article 7-B of Law 2/2006 as amended by Law 3/2017, non-compliance (even by negligence) with the duties established in Article 5-A, Article 5-B and Article 7 thereof constitutes an administrative offence, and is subject to the punishment below:

10.1.1 For natural person committing the offence, a fine of $10,000 (ten thousand patacas) to $500,000 (five-hundred thousand patacas);

10.1.2 For legal person committing the offence, a fine of $100,000 (one-hundred thousand patacas) to $5,000,000 (five million patacas).

[3] These provisions do not inhibit the information sharing requirements in paragraph 4.2.

10.2 If the economic benefit obtained by the offender from the commission of the infraction exceeds half of the maximum limit, the maximum limit shall be raised to the double of such benefit.

11. Final provisions

11.1 For the purpose of compliance with the duties described in these guidelines, standard forms shall be used, which can be downloaded from the website of DSF (www.dsf.gov.mo), under the CRAC section; or can be obtained from DSF, located at Rua da Sé, No. 30, Centro de Recursos da Direcção dos Serviços de Finanças, 1st Floor, during office hours.

11.2 These guidelines enter into force on 31st January 2019.