澳 門 金 融 管 理 局
AUTORIDADE MONETÁRIA DE MACAU

Circular no. 021/B/2016-DSB/AMCM of 15 June 2016
Circular no. 030/B/2016-DSB/AMCM of 2 December 2016
Circular no. 006/B/2019-DSB/AMCM of 30 January 2019

ANTI-MONEY LAUNDERING (AML) AND COMBATING THE FINANCING OF TERRORISM (CFT) GUIDELINE

Table of Content

ANTI-MONEY LAUNDERING (AML) AND COMBATING THE FINANCING OF TERRORISM (CFT) GUIDELINE

1. INTRODUCTION

1.1 This "Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) Guideline" (hereinafter referred to as "AML/CFT Guideline" or "Guideline") is to supersede the two guidelines promulgated by the Monetary Authority of Macao (AMCM) under Notice no. 010/2009-AMCM of 24th July.

1.2 The Guideline has incorporated the requirements of the AML/CFT laws and regulations enacted in Macao, the requirements of the Financial Action Task Force (FATF) Recommendations as well as the relevant best practices released by the FATF. The Guideline has also taken into consideration the opinions from the relevant sector on the implementation of the AML/CFT measures, and the findings of AMCM's ongoing supervision related to AML/CFT compliance.

2. SCOPE OF APPLICATION

2.1 The Guideline sets out the key requirements for credit institutions and other financial institutions to fulfil the relevant AML/CFT statutory and regulatory obligations.

2.2 The Guideline is applicable to the following financial institutions (hereinafter referred to as "institutions") authorized under the provisions of the Financial System Act (FSA) approved by Decree-Law no. 32/93/M of 5th July:

2.2.1 Credit institutions, financial intermediaries, or other financial institutions incorporated in Macao;

2.2.2 Macao establishments (e.g. majority-owned subsidiaries, branches, sub-branches, representative offices, etc.) of credit institutions, financial intermediaries, or other financial institutions incorporated abroad; and

2.2.3 Overseas establishments (e.g. majority-owned subsidiaries, branches, sub-branches, representative offices, etc.) of credit institutions, financial intermediaries, or other financial institutions incorporated in Macao.

2.3 The Guideline is also applicable to the following financial institutions (hereinafter referred to as "institutions") authorized under the provisions of specific laws and regulations other than the FSA:

2.3.1 Finance companies authorized under Decree-Law no. 15/83/M of 26th February;

2.3.2 Institutions authorized under Decree-Law no. 51/93/M of 20th September to carry out financial leasing activities in Macao;

2.3.3 Institutions authorized under Decree-Law no. 54/95/M of 16th October to carry out venture capital activities in Macao;

2.3.4 Institutions authorized under Decree-Law no. 25/99/M of 28th June to carry out assets management activities in Macao; and

2.3.5 Investment funds and investment fund management companies domiciled in Macao authorized under Decree-Law no. 83/99/M of 22nd November.

2.4 The following financial institutions (hereinafter referred to as "institutions") should establish and implement adequate and appropriate AML/CFT system, including AML/CFT policies, procedures and controls by observance of the requirements of the Guideline with necessary adaptation in conformity with the nature, size and risk profile of their respective business:

2.4.1 Institutions authorized under Decree-Law no. 38/97/M and 39/97/M of 15th September or other laws to carry out money changing activities in Macao; and

2.4.2 Institutions authorized under Decree-Law no. 15/97/M of 5th May to carry out cash remittance activities in Macao.

3. RISK OF MONEY LAUNDERING & TERRORIST FINANCING

3.1 Money laundering is defined by Article 3 of Law no. 2/2006 as a crime that includes conversion, transfer or dissimulation of properties or proceeds from illicit activities punishable with a maximum penalty of imprisonment over 3 years, or assistance or facilitation in such operations.

3.2 The process of money laundering has three stages:

3.2.1 Stage one (placement): To introduce the money into the financial system without causing suspicion, the money tends to be either broken up into smaller, less conspicuous amounts, or used to buy other financial instruments or commodities. These are then collected and deposited at another location.

3.2.2 Stage two (layering): The funds or assets, in their various forms, are then "layered", that is, moved around the world, from institution to institution, and sometimes may be disguised as payments for goods and services.

3.2.3 Stage three (integration): The funds, assets or commodities are reintroduced into the legitimate economy, as apparently *bona fide* financial instruments.

3.3 Terrorist Financing is defined by Article 7 of Law no. 3/2006 as a crime that includes the provision or collection, by any means directly or indirectly, of any property with the intention that the property be used, or knowing that the property will be used, in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used).

3.4 Money laundering and terrorist financing pose a serious risk for financial institutions. The inadequacy or absence of AML/CFT policies can subject institutions to serious customer and counter-party risks, especially **reputational, operational and legal risks.** All of these risks are interrelated and can interact upon each other. The possible adverse effects of money laundering include:

3.4.1 Reputational damage, which can harm a company's business and shareholder value, and its relationship with other relevant entities;

3.4.2 Criminal and regulatory sanctions resulting from non-compliance with laws and regulations; and

3.4.3 Civil litigation in connection with laundered money and related crimes.

4. APPLICABLE LEGISLATION

4.1 The FSA imposes the following control on money laundering and terrorist financing:

4.1.1 Compulsory identification of all customers (Article 106);

4.1.2 Personal identification of founding shareholders of institutions and their respective shareholdings (Paragraph 1 d) of Article 22);

4.1.3 Suitability of qualifying shareholders and managers (Articles 40, 41, 47 and 48);

4.1.4 Financial statements of institutions audited by independent external auditors (Article 53);

4.1.5 Consolidated supervision of the activity of institutions (Article 9);

4.1.6 Exchange of information between the AMCM and other supervisory authorities (Paragraph 1 b) of Article 79); and

4.1.7 Banking secrecy duty exempted by judicial order in case of criminal proceedings (Article 80).

4.2 Under Articles 7 to 9 and 29 of Law no. 17/2009 on prohibition of production, trafficking and illicit consumption of stupefying and psychotropic substances, any public or private entities can be requested for information or seizure of documents in respect of the assets, deposits or any other valuables belonging to the defendants or individuals strongly suspected of practice of the prescribed crimes, with a view to forfeiture. Such request of information or seizure of documents cannot be refused by any public or private entities, namely banking or financial institutions, partners or companies as well as registration and tax departments, provided that the request is detailed, sufficiently concretized and with indication of reference of the respective proceeding.

4.3 Under Paragraph 2 of Article 103 of the Criminal Code, approved by Decree-Law no. 58/95/M of 14th November, all assets or gains through criminal activities shall be confiscated. If the assets were substituted by other assets, the latter will be confiscated; if this is not possible, an equivalent amount of money has to be paid to the Government.

4.4 In 1998, Decree-Law no. 24/98/M of 1st June was passed to impose mandatory requirements for reporting suspicious transactions. This Decree-Law has been replaced by Administrative Regulation no. 7/2006 enacted under the provisions of Article 8 of Law no. 2/2006 and Article 11 of Law no. 3/2006.

4.5 On 15th April 2002, Law no. 4/2002 was promulgated to implement the measures of the international conventions signed and ratified by the Central Government that are applicable to Macao Special Administrative Region

(Macao SAR). Under the Law, the anti-terrorism measures under Resolution no. 1373 and other relevant resolutions of the United Nations Security Council become applicable in Macao SAR.

4.6 As mentioned in 3.1, Article 3 of Law no. 2/2006 on prevention and suppression of money laundering crime has established a clear definition of money laundering crime. Apart from strengthening the relevant sanction measures, Article 5 of the Law stipulates that legal entities committing money laundering crime are also criminally liable. Articles 6 and 7 of the Law define more entities that have obligation for taking customer due diligence measures and reporting suspicious transactions. At the same time, Paragraph 3 of Article 7 of the Law protects the reporting entities from any responsibility and they are not considered to have committed violation of secrecy, when providing information in good faith. Paragraph 4 of the same Article also prohibits reporting entities from disclosing to any customers or third parties any information in relation to fulfilment of the reporting obligation.

4.7 Articles 4, 5, 6 and 6-A of Law no. 3/2006 on prevention and suppression of terrorism crime define what terrorist organizations, other terrorist organizations, terrorism and other means of terrorism are. Article 7 of the Law stipulates that any person that provides or collects funds for the purpose to finance, totally or partially, terrorist activities shall be punished with a penalty of imprisonment from 1 to 8 years or a more severe penalty. As required by Article 11 of the same Law, the provisions in Articles 6, 7, 7-A, 7-B, 7-C, 7-D, 7-E and 8 of Law no. 2/2006 are applicable to prevention and suppression of terrorist financing after adaptation.

4.8 As required by Article 7 of Administrative Regulation no. 7/2006 on preventive measures against money laundering and terrorist financing crimes, the entities subject to the supervision of the AMCM should report, within the prescribed time limit, to the Financial Intelligence Office (GIF) any transactions which indicate money laundering and/or financing of terrorism. In addition to the reporting obligation, Articles 3 and 4 of the same Administrative Regulation also establish obligations for taking customer due diligence measures, identifying suspicious transactions and recording relevant information of such transactions. If obligations laid down in Articles 3 and 4 to obtain the relevant information cannot be carried out, Article 5 stipulates that such transactions should be refused. In accordance with Article 6, all relevant records should be retained for at least 5 years. As stipulated in Article 9, non-compliance with the relevant provisions of the Administrative Regulation constitutes an administrative offence, punishable by a fine from ten thousand (MOP 10,000) to five hundred thousand Macao patacas (MOP 500,000) for a natural person

and from one hundred thousand (MOP 100,000) to five million Macao patacas (MOP 5,000,000) for a legal entity, or, when the economic benefit obtained from the money laundering activity exceeds a value more than half the maximum limit (i.e. MOP 250,000 for natural persons or MOP 2,500,000 for legal entities), such limit will be double of the economic benefit.

5. AML/CFT SYSTEM

5.1 General

Institutions should establish and implement an adequate and appropriate AML/CFT system, including AML/CFT policies, procedures and controls to mitigate the risks of money laundering and terrorist financing (ML/TF).

5.2 Risk factors

To ensure that appropriate measures and controls are implemented to mitigate and manage the associated ML/TF risks, institutions should consider and assess the following risk factors:

5.2.1 Country/jurisdiction or geographic location;

5.2.2 Customer[1];

5.2.3 Product/service; and

5.2.4 Delivery/distribution channel.

5.3 Senior management responsibility and oversight

The board of directors or senior management of institutions should ensure that:

5.3.1 An effective AML/CFT system is established and implemented; and

5.3.2 The statutory and regulatory AML/CFT requirements are complied with.

5.4 Compliance and audit function

5.4.1 There should be an independent and adequately resourced compliance and audit function in place to:

[1] "Customer" refers to those natural or legal persons with whom business relationship is established or for whom transaction is carried out by the institutions.

a) Have regular assessment and/or review of the AML/CFT system to ensure compliance with institutions' AML/CFT policies and procedures as well as statutory and regulatory requirements and obligations; and

b) Communicate key AML/CFT issues and compliance deficiencies with the board of director or senior management.

5.4.2 The frequency and extent of assessment and/or review should be commensurate with the ML/TF risks.

5.4.3 The internal audit should evaluate independently and regularly the effectiveness of institutions' AML/CFT policies and procedures, including the compliance function, staff awareness and reporting of suspicious transactions.

5.5 AML/CFT Compliance Officer

Institutions should designate at least one compliance officer responsible for AML/CFT compliance, co-ordination and follow-up of related activities as well as reviewing and determining whether or not to file a suspicious transaction report with the GIF. The AML/CFT Compliance Officer should also coordinate the risk assessment as required in 6.2 and submit the updated risk assessment report to the AMCM in December of each year. The designation of the AML/CFT Compliance Officer(s) or any subsequent replacement requires prior consent from the AMCM [2]. In addition to appropriate competence and experience, the following criteria should also be observed:

5.5.1 The AML/CFT Compliance Officer should have an appropriate management or senior position within the institution's organizational structure;

5.5.2 The reporting lines should be such that the AML/CFT Compliance Officer's role will not be compromised by undue influence from line management; and

[2] The application for designation of AML/CFT Compliance Officer should be at least accompanied by the following documents of the designated person:

1. Curriculum vitae detailing academic qualifications and working experience;
2. Certificate of criminal record or equivalent document;
3. Organization chart showing the designated position and the relevant job description; and
4. If the designated person holding concurrent jobs in the institution, description of current jobs and measures to avoid job conflict.

5.5.3 The AML/CFT Compliance Officer should have timely access to all customer files, transaction records and other relevant information.

5.6 Staff screening and training

5.6.1 Institutions should have proper screening procedures in place to ensure hiring of employees with high standards and integrity.

5.6.2 Institutions should have an ongoing employee training programme so that staff members are adequately trained in understanding the AML/CFT laws and regulations, relevant policies and procedures, ML/TF risks, updated ML/TF techniques, methods and trends.

5.6.3 The training programme should be designed according to different staff needs, in particular, new staff (irrespective of seniority), front-line staff, supervisory staff and staff with compliance and audit functions. For instance, new staff members should be educated of the importance of AML/CFT measures, the related policies and other relevant basic requirements of the institutions. Front-line staff members who deal directly with the public should be trained to use reasonable means to verify the identity of customers, to exercise ongoing due diligence measures in handling accounts of existing customers, and to detect patterns of suspicious transactions. Back-end staff members should be trained to perform effective verification of customer records and detection of patterns of suspicious transactions. Supervisory staff members should be trained in skills for monitoring proper execution of the policies and procedures. AML/CFT Compliance Officer(s) should be trained in skills for assessing suspicious transaction reports and for carrying out reporting of suspicious transactions. The training for staff members with compliance and audit functions should be focused on the corresponding functions, while managerial staff should be given higher-level training covering various aspects of the institutions' AML/CFT system as well as their responsibilities.

5.6.4 Regular and timely refresher training should be provided to ensure that all staff members are reminded of their responsibilities and kept informed of new developments.

5.6.5 Institutions should monitor the effectiveness of the training so that further training needs can be identified for appropriate follow-up action.

5.7 Financial groups and overseas establishments

5.7.1 Financial groups should require all branches and majority-owned subsidiaries of the group to implement consistent group-wide policies and procedures to tackle ML/TF risks and to share the related information when necessary for AML/CFT purposes[3]. Proper measures should be established to ensure the compliance of any other legal obligations when sharing information. Adequate safeguards on the confidentiality and use of information exchanged should be in place, including to prevent tipping-off.

5.7.2 Institutions should ensure that their overseas branches and majority-owned subsidiaries comply with the Guideline to the extent that the laws and regulations of the host jurisdictions permit, and should pay special attention to whether the AML/CFT measures similar to those outlined in the Guideline are sufficiently applied in the host jurisdictions.

5.7.3 In the event that there are differences in such measures, institutions should apply the ones of higher standard. If any such overseas establishments could not comply with the Guideline because this is prohibited by the laws and regulations of the host jurisdictions, institutions should advise the AMCM in writing and take appropriate measures to mitigate the ML/TF risks effectively.

5.8 Third-party reliance

5.8.1 Institutions may rely upon some third parties, e.g. introducers, intermediaries or other members of the same financial group to perform the following customer due diligence measures:

a) Identification of customers and the related beneficial owners by verifying the relevant identity using reliable and independent source documents, data or information;

[3] This should include information and analysis of transactions or activities which appear unusual (if such analysis was done); and could include an STR, its underlying information, or the fact that an STR has been submitted. Similarly, branches and subsidiaries should receive such information from group-level functions when relevant and appropriate to risk management.

b) For customers being legal persons and legal arrangements, the measures should also cover understanding of the relevant ownership and control structure; and

c) Understanding and obtaining information on the purpose and intended nature of the business relationship.

5.8.2 The reliance is subject to the following criteria:

a) Institutions should satisfy themselves that the third parties are not located in the countries identified by the FATF or other similar bodies as having strategic AML/CFT deficiencies but are properly regulated, supervised and/or monitored to have implemented adequate measures in compliance with the customer due diligence and record-keeping requirements in line with the Guideline;

b) Institutions relying upon third parties should immediately obtain the necessary information concerning the elements of the customer due diligence set out in 8.4;

c) Institutions should satisfy themselves that copies of identification data and other relevant documentation relating to customer due diligence requirements will be made available from the third parties upon request without delay; and

d) Institutions should also satisfy themselves that the systems of the third parties to verify the identity of their customers are reliable.

5.8.3 Institutions relying on customer due diligence performed by third parties should still assume ultimate responsibility in this regard.

6. RISK-BASED APPROACH & RISK ASSESSMENT

6.1 Risk-based approach

6.1.1 Institutions should take a risk-based approach (RBA) to combat ML/TF.

6.1.2 The general principle of RBA is that, where there are higher risks, institutions should take enhanced measures to manage and mitigate the risks, and correspondingly, where the risks are lower, simplified measures may be applied. By adopting RBA, institutions should be able to allocate their resources in the most effective way and to ensure that

measures to prevent or mitigate ML/TF are commensurate with the risks identified.

6.1.3 In implementing RBA, institutions should take appropriate steps to identify, assess and categorize their ML/TF risks, have proper policies and procedures in place to monitor, manage and mitigate the risks, and take enhanced measures to manage and mitigate the risks where higher risks are identified. If lower risks are identified, institutions may take simplified measures. However, simplified measures should not be permitted whenever there is a suspicion of ML/TF.

6.2 Risk assessment

To form the basis for RBA, institutions are required to carry out risk assessments to identify, assess and understand their ML/TF risks (for customers, countries/jurisdictions or geographic areas; and products, services, transactions or delivery channels). The nature and extent of the risk assessments should be appropriate to the nature, complexity and size of institutions' business. Institutions should:

6.2.1 Document their risk assessments and keep them up to date;

6.2.2 Consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;

6.2.3 Obtain the approval of senior management on the assessment results;

6.2.4 Have policies, controls and procedures approved and reviewed by the board of directors or senior management to enable them to manage and mitigate the risks that have been identified; and

6.2.5 Monitor the implementation of those policies and controls, and enhance them if necessary.

6.3 Customer acceptance policy

6.3.1 For effectively implementing the AML/CFT measures, institutions should first develop clear customer acceptance policies and procedures to assess the ML/TF risks and acceptability of customers.

6.3.2 Institutions' customer acceptance policies should determine proper procedures to prevent from establishing business relationship or

conducting transactions with those entities designated as terrorists by the United Nations Security Council (www.un.org/Docs/sc/), Macao SAR Government[4] and other organizations or entities under interregional and international legal instruments, or those who are subject to sanctions announced locally or abroad, and to avoid establishing business relationship or conducting transactions with those from countries/jurisdictions covered in the list or statement published by the FATF (www.fatf-gafi.org) or in other sanction lists with international implications.

6.3.3 The policies should set up basic due diligence requirements for those customers of low risk and stringent requirements with enhanced due diligence for those of high risk.

6.3.4 The policies should also establish that, if it is unable to obtain the required customer information on timely basis, accounts should not be opened, business relations should not be commenced, and transactions should not be performed.

6.4 Risk assessment of customers

6.4.1 Institutions should consider, but not limited to, the following factors for risk assessment of customers and for the relevant ML/TF rating:

a) Country risk

Customers are living in, originating from or having connection with high-risk jurisdictions, such as:

i) Countries/jurisdictions identified by the FATF or other similar international organizations as having strategic AML/CFT deficiencies;

ii) Countries/jurisdictions subject to sanctions, embargos or similar measures issued by the United Nations or similar bodies;

iii) Countries/jurisdictions identified by credible sources as having significant levels of corruption or other criminal activity; and

[4] By announcement published in the Official Gazette of Macao SAR Government from time to time.

iv) Countries/jurisdictions or geographic areas identified by credible sources as having strong links to terrorist activities or providing funding or support for terrorist activities, or that have designated terrorist organizations operating within them.

In assessing country risk associated with a customer, institutions should refer to those publicly available reliable sources, in particular information related to those jurisdictions subject to the ongoing process of FATF or information released by other international bodies[5].

b) Customer risk

The following customers, by nature or behaviour, might present higher ML/TF risks:

i) Non-resident customers;

ii) The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the institution and the customer);

iii) Customers identified as or having close connection with domestic/foreign politically exposed persons (PEPs);

iv) Customers involved in high cash-intensive business, or business activities of which its nature, scope and/or location are more vulnerable to ML/TF risks;

v) Customers with complex relationships or corporate structures, or with use of trusts, nominee and/or bearer shares, particularly without legitimate commercial rationale, or ownership not easily verified.

c) Product/service/transaction risks

Product/service/transaction examples presenting higher ML/TF risks are as follows:

[5] For instance: www.un.org; www.imf.org; www.worldbank.org; www.oecd.org; www.fatf-gafi.org; www.apgml.org; www.bis.org/fsi; www.iosco.org; www.iaisweb.org; www.wolfsberg-principles.com; www.gifcs.org; www.egmontgroup.org; www.transparency.org.

i) Those inherently providing more anonymous transactions (e.g. cash transactions or undue secrecy transactions);

ii) Those with ability to pool underlying customers/funds (e.g. private banking);

iii) Those receiving payments from unknown or un-associated third parties.

d) Delivery/distribution channel risks

The distribution channels for products, e.g. online sales, postal or telephone sales where non-face-to-face business relationships are established or the delivery of products/services through intermediaries may increase ML/TF risks as the business relationship between the customer and the institution becomes indirect.

6.4.2 Institutions should adjust the risk rating of customers from time to time based on the information from reliable sources, and review the relevant customer due diligence performed. In principle, high-risk customers should be subject to periodic review on priority basis, while review of low-risk customers should be triggered by some pre-established criteria (e.g. unusual transactions, transactions in large amount or transaction patterns not commensurate with customer background).

6.5 Anonymous accounts

6.5.1 Institutions should never establish business relationship with a customer who provides a fictitious name or insists on anonymity.

6.5.2 When a numbered account is requested to offer additional protection for the identity of the account holder, the identity should be known to a sufficient number of staff to exercise proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from an institution's compliance function or from the regulators.

6.6 New technologies

6.6.1 Institutions should identify and assess the ML/TF risks that may arise from:

a) The development of new products and new business practices, including new delivery mechanisms; and

b) The use of new or developing technologies for both new and pre-existing products.

6.6.2 Such risk assessment should take place prior to the launch or use of such new products, business practices and technologies. Institutions should take appropriate measures to monitor, manage and mitigate those risks.

7. FINANCIAL SANCTIONS

7.1 Sanctions against terrorist and proliferation financing

7.1.1 Under Law no. 4/2002, the sanction measures on terrorist and proliferation financing contained in the relevant United Nations Security Council (UNSC) Resolutions are applicable in Macao SAR.

7.1.2 Institutions should freeze without delay and prior notice, the funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by any persons or entities that are:

a) Designated by the UNSC for freezing purpose through Resolutions 1267 (1999), 1718 (2006), 1737 (2006), 1988 (2011) or other subsequent Resolutions; and/or

b) Designated by Macao SAR Government pursuant to UNSC Resolution 1373 (2001).

7.1.3 Institutions are prohibited from making available any funds or other assets, economic resources, or financial or other related services, directly or indirectly, wholly or jointly, for the benefit of the persons and entities designated by UNSC Resolutions as indicated above.

7.2 Database and screening

7.2.1 Institutions should effectively prevent any terrorist suspects and designated parties from trying to enter into business relationship or to initiate transactions.

7.2.2 For such purpose, institutions should maintain a consolidated database of various lists of terrorist suspects and designated parties for screening of customers. Alternatively, institutions may choose to have access to such database provided by some well-known service providers for performing the screening.

7.2.3 Institutions should ensure that the database for screening is up-to-date and covers at least those persons and entities subject to local, UNSC or other international sanctions.

7.2.4 Institutions should conduct:

a) Screening of customers and the related parties (including the beneficial owner and any other natural persons having the power to direct the activities of the customer) before establishing business relationship or conducting occasional transactions exceeding the thresholds laid down in 11.2;

b) Timely screening of all existing customers and the related parties upon awareness of any sanction updates/changes; and

c) Screening of payment instructions, in particular made through wire transfers, in order to ensure that no payments will be made to any persons and entities designated in all the sanction lists.

7.2.5 Institutions, if suspecting any customers or transactions of being terrorist-related, should file a suspicious transaction report to the GIF as soon as possible.

8. CUSTOMER DUE DILIGENCE

8.1 Customer identification and verification

8.1.1 General

Institutions are required to:

a) Identify, verify and record the identity of customers and the related beneficial owners as defined in 8.2 using reliable and independent source documents, data or information;

b) Understand and obtain information on the business nature, ownership and control structure of those legal persons and legal arrangements;

c) Understand and obtain information on the purpose and intended nature of the business relationship;

d) Conduct ongoing due diligence on the business relationship and scrutiny of transactions to ensure consistency with customers' background throughout the course of the relationship;

e) Take particular care in conducting reasonable due diligence measures for the following persons and entities who:

i) Maintain accounts or business relationships, or ask for opening accounts or making transactions, but do not appear to act on their own behalf;

ii) Are the beneficiaries of the transactions conducted by professional intermediaries (e.g. lawyers, accountants, etc.) or by any other similar persons or entities;

iii) Are acting on behalf of existing customers and/or connected with any transactions, posing ML/FT or other risks to the institutions; and

iv) Have access to safe deposit boxes not leased by them.

8.1.2 Account opening procedures

a) Institutions are required to set up account opening procedures for different types of accounts including accounts in name of individual person, commercial business, trust, intermediary or offshore company, etc. There should be proper segregation of duties to perform the procedures and all new customers and new accounts should be approved by the officers with appropriate authority.

b) Institutions should not open accounts, establish business relationship or carry out any transactions with customers unless the customer due diligence process is completed and the customer identity is satisfactorily established.

c) If it is not practicable to do so, institutions should complete the verification procedures as soon as possible after establishment of the relationships, while adopting risk management procedures concerning the conditions, for instance, at least setting limitations on number, types and/or amount of transactions that can be performed by such customers and closely monitoring such relationships pending completion of the identity verification.

d) Once having opened an account or established a business relationship, if customer due diligence cannot be completed within a reasonable period of time and with no reasonable explanation for the delay, or if institutions have subsequent doubts about the customer's true identity which cannot be resolved satisfactorily, the institutions should suspend or terminate the business relationship and consider making a suspicious transaction report to the GIF.

8.1.3 Ongoing review of customer information

Institutions are required to carry out regular and ongoing review of existing records (documents and information collected under the customer due diligence process) to ensure that these records remain up-to-date and relevant on the basis of materiality and risk, particularly when:

a) Suspicion is noted, such as appearance of unusual transactions or transactions not in line with the nature of business or profession stated by the customers or where there are doubts about the veracity or adequacy of previously obtained customer identification data;

b) There is material change, e.g. significant change in business or profession, or in other information, or in the way that the account is operated;

c) Significant amount of transactions takes place;

d) Records are obsolete or insufficient, or information is irrelevant or outdated.

8.1.4 Enhanced customer due diligence measures

a) Special attention should be exercised in relation to those customers rated as high-risk to safeguard the institution from being used for

money laundering or terrorist financing. Institutions should also examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the ML/TF risks are higher, institutions should conduct enhanced customer due diligence measures consistent with the risks identified. Enhanced customer due diligence measures that could be applied for higher-risk business relationships include:

i) Obtaining independent and reliable sources to verify habitual residential address;

ii) Obtaining additional information on the customer (e.g. occupation, volume of assets, etc.) by referring to publicly available information, making additional data searches, and/or seeking third party verification like reference from other regulated financial institutions;

iii) Obtaining additional information on the corporate customer, its operation and the individuals behind it;

iv) Updating more regularly the identification document of the customer and the beneficial owner(s);

v) Obtaining additional information on the nature of the business relationship;

vi) Obtaining additional information on the source of funds[6] and source of wealth[7] of the customer;

vii) Obtaining information on the reasons for intended and/or performed transactions;

viii) Obtaining the approval of senior management to commence or continue the business relationship;

ix) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and

[6] "Source of funds" refers to the funds for the business relationship originated.
[7] "Source of wealth" refers to the major economic activities that have generated or given rise to the net worth or properties of a person.

selecting patterns of transactions that need further examination;

x) Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar customer due diligence standards.

b) In addition to the enhanced customer due diligence, institutions should take other counter measures, e.g. increasing intensity of monitoring, adoption of specific reporting mechanisms, limiting certain transactions, etc. against those high-risk customers.

c) All high-risk customers (excluding dormant accounts) should be subject to more frequent review to ensure that the respective customer due diligence information remains up-to-date and relevant.

8.1.5 Simplified customer due diligence (SDD)

a) With justification through an adequate analysis of risks, institutions may apply SDD measures, where identification and verification of beneficial owners and/or persons authorized to act on behalf of the customers are not required. The simplified measures should be commensurate with the lower risk identified. In particular, SDD can be applied for those customers, namely government and public bodies, state-owned enterprises, listed companies, and regulated financial institutions, which are established or incorporated in jurisdictions where AML/CFT measures similar to those outlined in the Guideline are adequately adopted.

b) However, SDD should not be permitted whenever there is ML/TF suspicion, or where specific higher-risk scenarios apply.

8.1.6 Customer due diligence and tipping-off

If institutions form a suspicion of ML/TF and reasonably believe that performing the customer due diligence process will tip off the customer, then the process should be discontinued and the case should be reported to the GIF.

8.2 Beneficial owner

8.2.1 Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

8.2.2 Institutions should be satisfied that a customer (natural person) is acting on own behalf or who the relevant beneficial owner is, or require such customers to disclose the identity of the beneficial owners if any.

8.2.3 Institutions should identify the beneficial owners of the customer (legal person or arrangement) and take reasonable measures as mentioned in 8.4.1 to verify the identification of such persons. Beneficial owners may be identified through the following information:

a) For legal persons:

i) The identity of the natural person(s), if any, who ultimately has a controlling ownership interest[8] in the legal person;

ii) If there is doubt under i) above whether the person(s) with the controlling ownership interest is the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural person(s), if any, exercising control of the legal person through other means;

iii) If no natural person is identified under i) or ii) above, the identity of the relevant natural person who holds the senior management position in the legal person;

iv) Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to the disclosure requirements (either by stock exchange rules or through laws or other enforceable means) which 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.

[8] A controlling ownership interest depends on the ownership structure of the company. It may be based on a threshold, e.g. 25% of ownership interest, or lower if higher risk scenarios apply.

b) For legal arrangements:

i) Trusts – the identity of the settlors[9], the trustees[10], the beneficiaries[11] or any other natural persons (e.g. protector) exercising ultimate effective control over the trust (including through a chain of control/ownership);

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

8.3 Person purporting to act on behalf of the customer

Institutions should identify, verify and record the identity of those persons authorized to act on behalf of the customer (e.g. authorized signers or others) by:

8.3.1 Carrying out the same identification and verification measures as mentioned in 8.4.1 c) to d); and

8.3.2 Obtaining the relevant written authority to verify that the persons purporting to represent the customer is properly authorized to do so.

8.4 Minimum requirements for establishing business relationship

8.4.1 Personal customers

a) The following information should be obtained and recorded at the time of establishing a business relationship:

i) Identification information, including name(s), date of birth, and identity document type and number;

ii) Habitual residential address;

iii) Nationality and place of birth;

[9] "Settlor" is a person or company who transfers ownership of its assets to trustee by means of a trust deed.
[10] "Trustee" refers to a person who may be paid professional or company or unpaid person, holds and manages the assets in a trust fund separate from his/her own assets in accordance with the settlor's trust deed, taking account of any letter of wishes.
[11] "Beneficiary" refers to a person whose property is administered by a trustee; in a trust, although the trustee is the legal owner of the property, the beneficiary is the equitable owner who receives the real benefit of the trust.

iv) Name of employer and nature of profession or name and nature of business;

v) Source of funds, wealth or income; and

vi) Purpose and intended nature of the business relationship.

b) Institutions should verify, at least, the identification specified in 8.4.1 a).

c) For the identity, the customer information and personal appearance should be verified against valid original documents of identity issued by governmental authorities (e.g. identity cards, passports or other official documents with photograph). Such documents should be those that are most difficult to obtain illicitly.

d) For Macao residents, the proper identification documents are the "*Bilhete de Identidade de Residente Permanente*" (Permanent Resident Identity Card) and "*Bilhete de Identidade de Residente Não Permanente*" (Non-permanent Resident Identity Card) issued by the "*Direcção dos Serviços de Identificacão*" (Identification Bureau) of Macao or other equivalent identification documents.

e) Special care should be taken in accepting documents that are easily forged or can be easily obtained by false identities in case of foreign customers.

8.4.2 Corporate customers including legal persons/arrangements

a) Institutions should obtain and record the following information:

i) Full commercial denomination;

ii) Date and place of incorporation;

iii) Registration or incorporation number;

iv) Registered office address in the place of incorporation, and, if different, address of principal place of business;

v) Name and habitual residential address of beneficial owners, persons authorized to act on behalf of the corporate customer, persons that regulate and bind the legal person or arrangement, as well as persons having a senior management position in the legal person or arrangement;

vi) Name of shareholders and members of board of directors;

vii) Details of ownership and structure of control;

viii) Nature of business/activities; and

ix) Purpose and intended nature of the business relationship.

b) Institutions should verify customer information specified in 8.4.2 a) i) to vi):

i) For verification of company information, institutions should obtain certificate of incorporation or equivalent documents issued by the relevant government agencies. For locally incorporated companies, business registration certificate and/or company search report from the "*Conservatória dos Registos Comercial e de Bens Móveis*" (Businesses and Vehicles Registry), tax declaration required by "*Direcção dos Serviços de Finanças*" (Finance Services Bureau), deed of incorporation, memorandum and articles of association, etc. For companies incorporated abroad, apart from the equivalent documents mentioned for the local ones, certificate of good standing or other relevant documents;

ii) For verification of identification of beneficial owners, persons authorized to act on behalf of the corporate customer and executive or key members of board of directors[12], institutions should refer to 8.4.1 c) to d).

c) For large corporate customers, financial statements of the business or a description of the customers' principal lines of business should also be obtained. In addition, if significant changes to the company

[12] If any of the executive or key members of board of directors are legal persons, the verification of identification should focus on the relevant natural persons who represent and/or control the aforesaid legal persons.

structure or ownership occur subsequently, further checks should be made.

d) If possible, institutions should take reasonable measures to verify whether the corporate customer operates its stated business at the stated address.

e) If original documents could not be obtained, copies of the documents should be properly certified [13]. Where certified documents are accepted, it is the responsibility of the institutions to satisfy themselves that the certifier is appropriate and reliable.

f) The anticipated level and nature of transactions to be carried out by the customers, and the source and origin of the funds, wealth and income of the customers should be recorded by adopting a risk-based approach.

9. BUSINESS RELATIONSHIPS REQUIRING ADDITIONAL DUE DILIGENCE MEASURES

9.1 Trusts

9.1.1 Institutions should establish whether or not the customers are acting on behalf of other persons as trustees.

9.1.2 Institutions should identify, verify and record details of the nature of the trust, including:

a) Name of the trust;

b) Date of establishment/settlement;

c) Jurisdiction whose laws govern the arrangement as set out in the trust instrument;

[13] Copies of the documents should be certified by a suitable person, such as a lawyer, accountant, director or manager of a regulated institution, a notary public, a member of the judiciary, a senior civil servant, a consular official or a servicing police officer. The certifier should sign and date the copy document (printing his name clearly in capitals below), state that it is a true copy of the original, and clearly indicate his position or capacity on it. If a covering letter is used, it is important to establish the document to which the letter refers.

d) Identification number, if any, granted by any competent authorities (e.g. tax identification number, registered charity or non-profit organization number); and

e) Identity of the trustee(s), settlor(s), beneficiaries and any other persons involved in the structuring of the arrangement (e.g. a protector).

9.1.3 The beneficiaries mentioned above should be identified as far as possible. If the beneficiaries are yet to be determined, institutions should concentrate on the identification of the settlor and/or the persons in whose interest the trust is set up. For beneficiary(ies) of trusts that are designated by characteristics or by class, institutions should obtain sufficient information concerning the beneficiary to satisfy the institutions that they will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.

9.1.4 To verify the details of the trust or other similar arrangements, institutions should review the trust deed, trust instrument or refer to the relevant registration records if available.

9.2 Nominee and fiduciary accounts or client accounts opened by professional intermediaries

9.2.1 Institutions should obtain satisfactory evidence of the identity of the nominees or the intermediaries (e.g. lawyers, accountants, etc.) and the persons on whose behalf they are acting, as well as the details of the arrangements in place.

9.2.2 Special care should also be exercised in initiating business transactions with "shell companies[14]". Satisfactory evidence of the identity of their beneficiary owners should be obtained.

9.2.3 In case the institutions are unable to establish the identity of the persons for whom the intermediaries are acting, or verify the identity of the beneficial owners of the accounts, the institutions should refuse to open the accounts or refuse to establish any business relationships.

[14] "Shell company" refers to a company that exists in name only, or that there may be no employees, physical office and operations / business activity.

9.3 Non-face-to-face relationships

For non-face-to-face business relationships, institutions should apply equally effective customer identification procedures and ongoing monitoring standards as for those face-to-face relationships plus any of the following measures to mitigate the relevant higher risks:

9.3.1 Certification of documents, e.g. the relevant documents should be certified and/or verified by a respondent institution or a reliable third party;

9.3.2 Requisition of additional documents to complement those required for face-to-face relationships, e.g. information provided by another institution subject to similar customer due diligence standards;

9.3.3 Written referral by an introducer who is subject to the same identification procedures as required by the Guideline;

9.3.4 Requiring the first payment to be carried out through an account in the customer's name with another institution subject to the customer due diligence standards similar to the Guideline;

9.3.5 Other similar reasonable measures.

9.4 Politically exposed persons

9.4.1 General

a) Politically exposed persons (PEPs) refer to those persons who are or have been entrusted with prominent public or political functions, either by local government (as domestic PEPs) [15] or by overseas governments or international organizations (as foreign PEPs), or holding senior public office, or entrusted with prominent functions by international organizations, as well as their family members[16] and/or close associates[17].

[15] "Domestic PEPs" refer to those originated from Macao SAR and should be classified in line with the "Legal Regime of Declaration of Assets and Interests" enacted by the Macao SAR government in 2013.
[16] "Family members" refer to those persons who are related to a PEP either directly (consanguinity) or through marriage or similar forms of partnership (civil), e.g. a spouse, a partner, a child, or a parent of a PEP, or a spouse or a partner of a child of a PEP.
[17] "Close associates" refer to those persons who are closely connected with a PEP, either socially or professionally, e.g. persons having close business relation with a PEP.

b) Although PEP status itself does not automatically mean that the PEPs are corrupt or have been incriminated in any corruption cases, their office and position may render PEPs vulnerable to corruption. The risks increase when the PEPs concerned are from foreign countries/jurisdictions with widely-known problems of bribery, corruption and financial irregularity within their governments and societies.

c) PEPs should include heads of state or of government, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned corporations, important political party officials, or members of senior management of international organization, i.e. directors, deputy directors and members of the board or equivalent functions.

9.4.2 Business relationship with PEPs and connected parties

a) Business relationship with PEPs may expose an institution to significant reputational and/or legal risks.

b) Accepting and managing funds from corrupt PEPs will severely damage institutions' own reputation and can undermine public confidence in the ethical standards of the financial system, since such cases usually receive extensive media attention and strong political reaction, even if the illegal origin of the assets is often difficult to prove.

c) Institutions should put in place risk management systems to determine if a customer or beneficial owner is a PEP. To do this, institutions should gather sufficient information from new and existing customers and review the information data in due care and check publicly available information or commercial electronic databases, in order to establish whether or not the customer or beneficial owner is a PEP.

d) Before accepting a PEP as customer, institutions should take reasonable measures to establish the source of funds and wealth of the PEP.

e) The decision to establish and maintain business relationship with a PEP should be made by senior management of the institutions. Where a customer has been accepted and the customer or beneficial

owner is subsequently found to be, or subsequently becomes a PEP or a party connected with PEPs, senior management approval is required for continuing the business relationship.

f) In handling the business relationship with PEPs, institutions should conduct enhanced ongoing monitoring on the relationship and consider the following risk factors:

i) Concerns on the jurisdiction where the PEPs are or have been entrusted with prominent public functions;

ii) Unexplained sources of wealth or income, or funds from governmental bodies or state-owned entities or from the commission earned on government contracts;

iii) Request to put any transactions under secrecy coverage;

iv) Use of accounts at government-owned banks or of government accounts as the source of funds for any transaction.

g) While enhanced due diligence and monitoring measures are required for the business relationship with foreign PEPs, institutions should perform a risk assessment to determine whether a domestic PEP poses a higher risk of ML/TF. Domestic PEP status itself does not automatically confer higher risk. In cases when it poses higher risk, institutions should adopt the same enhanced measures as required for foreign PEPs.

h) The enhanced measures should also be applicable to the business relationships with those parties connected with PEPs by adopting the risk-based approach.

9.5 Non-profit organization (NPO)

9.5.1 NPO refers to a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".

9.5.2 NPOs may be vulnerable to abuse by terrorists as NPOs enjoy the public trust, have access to considerable sources of funds, and are often cash-intensive. Furthermore, some NPOs have a global presence that provides

a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity.

9.5.3 Therefore, institutions need to be vigilant when establishing business relationship with NPOs and the decision for such business relationship should be subject to proper approval. In addition to the customer due diligence measures mentioned in 8, institutions should:

a) Be satisfied that the NPOs intend to enter into business relationships or make transactions are not connected with any known terrorists/terrorist organizations by searching the relevant databases and publicly available information;

b) Take special care for dealing with any NPOs originating from those countries/jurisdictions or areas exposed to terrorist activities;

c) Monitor closely any existing NPO customers rated as high risk and report to the GIF in respect of any suspicious transactions with source from and/or destination to countries/jurisdictions or areas exposed to terrorist activities;

d) Conduct ongoing review and risk assessment of NPO customers by referring to the relevant databases and publicly available information.

9.6 Wire transfers

9.6.1 Definition and scope

a) A wire transfer refers to any domestic/cross-border transaction carried out on behalf of an originator through an ordering financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person. Such wire transfer may include any intermediary financial institution(s) to enable disbursement of the funds to the beneficiary.

b) The requirements specified in this section are not applicable to financial institution-to-financial institution transfers and settlements,

where both the originator and the beneficiary are financial institutions acting on their own behalf.

9.6.2 Ordering institutions

a) Ordering institutions should ensure that wire transfers are always accompanied by the following information:

i) Name and address of the originator;

ii) Number of the originator's account where the transaction is processed or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction;

iii) Beneficiary information, including name of the beneficiary and the beneficiary account number or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and

iv) Instruction details, including name and address [18] of the beneficiary institution, and originator's message to the beneficiary, if any.

b) For wire transfers conducted by account holders, the relevant originator information should correspond to the account holders. Ordering institutions should not entertain any request to override such information or should ask the account holders to provide further explanation for the transactions. If suspicion arises, a report should be filed with the GIF.

c) Institutions should maintain all originator and beneficiary information collected for wire transfers.

d) Ordering institutions should not conduct any wire transfer if the specified information cannot be obtained.

[18] Address of beneficiary institution can be office address or swift, telex, telegram address code or other standard code that is identifiable.

9.6.3 Beneficiary institutions

a) Beneficiary institutions should verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in compliance with 12.

b) Beneficiary institutions should take reasonable measures to identify wire transfers that lack the required originator or beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible.

c) Beneficiary institutions should have effective risk-based policies and procedures for determining: i) when to execute, reject or suspend a wire transfer lacking the required originator or beneficiary information, and ii) the appropriate follow-up action.

9.6.4 Intermediary institutions

a) For wire transfers, intermediary institutions should ensure that the required originator and beneficiary information accompanied by the wire transfer is retained when processing an intermediary element of such wire transfer chains.

b) Where technical limitations prevent the required originator or beneficiary information accompanying a wire transfer from remaining with another related wire transfer, a record should be kept, for at least five years, by the receiving intermediary institutions of all the information received from the ordering institution or another intermediary institution.

c) Intermediary institutions should take reasonable measures to identify wire transfers that lack the required originator or beneficiary information. Such measures should be consistent with straight-through processing[19].

d) Intermediary institutions should have effective risk-based policies and procedures for determining: i) when to execute, reject, or suspend a wire transfer lacking the required originator or beneficiary information, and ii) the appropriate follow-up action.

[19] Straight-through processing refers to payment transactions that are conducted electronically without the need for manual intervention.

9.6.5 Batch transfers

a) The wire transfers, if contained within a batch transfer, should be accompanied with all the necessary originator/beneficiary information as required in 9.6.2.

b) For transactions using credit or debit cards for fund transfers, if processed within a batch transfer, the required information can be simplified to include at least originators' account number or card number.

c) Institutions should ensure that non-routine transactions of such funds transfers are not batched.

9.7 Correspondent banking

9.7.1 Correspondent banking[20] is the provision of banking services by one institution (the correspondent) to another institution (the respondent) to:

a) Meet its fund clearing, liquidity management and short-term borrowing or investment needs; and

b) Enable the latter to provide services and products to its own customers.

9.7.2 The correspondent institution acts as agent (intermediary) for the respondent institution and executes or processes payment or other transactions for customers of the respondent institution. In this connection, the correspondent institution often has limited information regarding the nature and purpose of the correspondent banking transactions due to non-existence of direct relationship with the underlying parties to the transactions and is not in a position to verify the identity of the relevant parties. As such, correspondent banking should be regarded as high-risk from a ML/TF perspective.

9.7.3 When establishing correspondent banking relationships, in addition to taking the customer due diligence measures required by 8.4.2, institutions should:

[20] In the Guideline, "correspondent banking" refers to cross-border correspondent relationships but institutions may also apply the same measures for local relationships.

a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business, including, but not limited to:

   i) Major business activities;

   ii) Domicile location;

   iii) Ownership and management structure; and

   iv) Purpose and intended nature of accounts or facilities.

b) Determine, based on the information from those publicly available databases, the reputation of the respondent institution and the quality of supervision, including the system of banking regulation and supervision in its domicile location, and whether it has been the subject of any ML/TF investigation or regulatory action in the recent past;

c) Assess if the institution's AML/CFT controls are adequate and effective;

d) Obtain top management approval before establishing any new correspondent banking relationships;

e) Clearly understand and document the respective responsibilities of each institution particularly from the AML/CFT perspective; and

f) Be satisfied where a correspondent banking relationship involves the maintenance of "payable-through accounts[21]" that:

   i) The respondent institution has performed all normal, adequate and ongoing customer due diligence and monitoring obligations on those customers that have direct access to the accounts of the correspondent institutions; and

   ii) The respondent institution is able to provide relevant customer due diligence information and identification data upon request to the correspondent institutions.

[21] "Payable-through accounts" refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

9.7.4 Institutions should avoid establishing business relationship with respondent institutions that are located in jurisdictions with poor AML/CFT compliance or included in statements of concern published by the FATF or other sanction lists with international implications.

9.7.5 Institutions should not establish or continue business relationships with any shell institutions in particular shell banks[22].

9.7.6 Institutions should perform periodic reviews and update of the risk profile of the respondent institutions. If a material change is detected in the profile of the respondent institution or in the relevant respondent account movements, institutions should perform a thorough review and update of the profile of the respondent institutions.

9.7.7 If, in the course of any review, a respondent institution refuses to provide the required due diligence information or its AML/CFT compliance is detected as inadequate or ineffective, institutions should adjust the relevant risk rating for the institution or consider terminating the relationship if appropriate.

9.8 Private banking

The features of private banking relationships can lead to higher ML/TF risks. Therefore, institutions should understand and manage the higher risks accordingly by establishing special criteria for private banking customers in the relevant customer acceptance policy, due diligence and ongoing monitoring measures, including but not limited to the following:

9.8.1 Acceptance of private banking customers should require approval by senior management;

9.8.2 Establishment of any private banking relationships should be on a face-to-face basis;

9.8.3 Enhanced due diligence should be performed throughout any private banking relationships, in particular getting comprehensive information on estimated net worth, source of funds, source of wealth, family background (spouse, parent etc.), forecasted account movement volume, and taking up references; and

[22] "Shell bank" refers to a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

9.8.4 Any private banking relationships should be subject to periodic review and ongoing monitoring. For proper ongoing monitoring, institutions should be aware of the personal profiles of the high-risk customers and be alert to sources of third-party information.

10. ONGOING MONITORING

10.1 Effective ongoing monitoring is vital for understanding of customers' activities and an integral part of effective AML/CFT systems.

10.2 Institutions should have reasonable understanding of the normal account activity of their customers so as to identify transactions falling outside the regular pattern of an account's activity and pay special attention to the business relationships and transactions involving persons connected with those jurisdictions not applying sufficiently AML/CFT measures similar to the ones prescribed in this Guideline.

10.3 Institutions should have proper systems in place to continuously detect all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. This can be done by establishing in transaction monitoring systems certain parameters for a particular class or category of accounts to detect such transactions that require special attention. Institutions should examine the background and purpose of such transactions, while relevant findings, handling outcomes, decision made and the rationale of the decision should be properly recorded. Where institutions are dissatisfied that any of such transactions are reasonable, the transactions should be considered as suspicious for timely report to the GIF.

10.4 The extent of ongoing monitoring should be commensurate with the risk rating of the customers. For those high-risk customers, institutions should take enhanced due diligence measures and more intensive ongoing monitoring. For proper monitoring and follow-up, the AML/CFT Compliance Officer and/or other officers with appropriate authority should be provided with periodic reports with adequate information of the accounts of high-risk customers, including but not limited to unusual transactions, large transactions and aggregate total of business relationships with the institutions.

10.5 Institutions should also have monitoring systems for high-risk cash transactions and transfers to third parties. Periodic reports of such transactions should be submitted to the AML/CFT Compliance Officer and/or other officers with appropriate authority for review and follow-up.

10.6 Where transactions in cash or by bearer cheques or cashier orders exceeding certain amounts are conducted for customers, institutions should obtain adequate information to understand the transactions and to ensure that the transactions are commensurate with the customers' profiles. For instance, institutions may consider obtaining additional information on the source of funds like invoices, certification and other reliable sources of evidence. Where institutions are dissatisfied that any of such transactions are reasonable, the transactions should be considered as suspicious for timely report to the GIF.

10.7 Where transactions are performed by persons on behalf of the account holders, e.g. when cash is deposited into an existing account by persons whose names do not appear on the mandate of that account, care and vigilance are required. Where the transactions involve an amount equal to or exceeding MOP/HKD 120,000 or equivalent in any other currencies, the identity of all the persons involved in the transactions should be recorded.

11. OCCASIONAL TRANSACTIONS

11.1 Occasional transactions refer to those transactions initiated by the customers who do not have pre-established business relationship with the institutions or initiated by existing customers but not conducted through their accounts, in relation to wire transfers, currency exchanges, encashment of traveller's cheques, money/postal orders, cashier orders, bank drafts, or gift cheques, etc.

11.2 For all occasional cross-border and domestic wire transfers regardless of the amount, or any other occasional transactions mentioned in 11.1 in an amount equal to or exceeding MOP/HKD 120,000 [23] or equivalent in any other currencies, or a few such transactions that appear to be linked (e.g. when several transactions are made by the same customer in a short period of time) and aggregate to an amount equal to or exceeding the aforesaid threshold, proper records of the following information should be kept by institutions:

11.2.1 Wire transfers

Institutions should ensure that the transfers are accompanied by the information specified in 9.6.2.

11.2.2 Money changing transactions

a) Transaction reference number;

[23] Without prejudice to the stipulations in other specific laws and regulations.

b) Date and time of transaction;

c) Currencies and amount exchanged;

d) Exchange rate;

e) Name, number and type of valid identification document of customer; and

f) Telephone number or address of customer.

11.2.3 Encashment transactions

a) Transaction date and reference;

b) Instrument type, currency and amount;

c) Exchange rate;

d) Name, number and type of valid identification document of customer; and

e) Telephone number, or address or account number if any, of customer.

11.2.4 For any other occasional transactions, similar relevant information specified above should be recorded.

11.3 Institutions should record and exercise reasonable measures to verify the identity of the customers by reference to their valid official identification documents.

11.4 Institutions should also understand whether the occasional transactions are realized by a customer on behalf of some other persons. In such case, the identification information of all the persons involved in the transactions should be recorded.

11.5 Any occasional transactions equal to or exceeding MOP/HKD 250,000 or equivalent in any other currencies should be considered as high-risk transactions subject to additional control measures as follows:

11.5.1 The transactions should be countersigned or approved by officers with appropriate authority;

11.5.2 Adequate customer due diligence measures like obtaining information on the source of funds and purpose of the transactions should be applied; and

11.5.3 Periodic reports listing the high-risk occasional transactions should be submitted to the AML/CFT Compliance Officer or other officers with appropriate authority for reviewing and monitoring.

12. RETENTION OF RECORDS

12.1 Institutions should maintain, for at least 5 years from the date of completion of the transactions notwithstanding that the customers may have terminated the account relationship with the institutions subsequent to the transactions, all necessary records on the transactions, both domestic and cross-border. Such records should be sufficient to permit reconstruction of individual transactions, including the amounts and types of currency involved, if any, so as to provide, if necessary, evidence for prosecution of criminal activity.

12.2 Institutions should also maintain, for at least 5 years after the termination of the business relationship or the date of the occasional transaction, all records obtained through customer due diligence measures, account files and business correspondence, and results of any ongoing review, monitoring or analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions).

12.3 Institutions should ensure that all customer due diligence information and transaction records are available swiftly to competent authorities upon request.

13. REPORTING OF SUSPICIOUS TRANSACTIONS

13.1 General

13.1.1 Transactions indicating signs of money laundering and/or financing of terrorism crime, or transactions suspiciously involving converting, transferring or dissimulating illegally obtained funds or properties in order to conceal the true ownership and origin of the funds or properties to make them appear to have originated from a legitimate source, are considered suspicious money laundering and/or terrorist financing transactions, or in abbreviation, suspicious transactions.

13.1.2 Institutions should report all suspicious transactions to the GIF within the prescribed time limit, regardless of the amount of the transaction.

13.1.3 Institutions should also make a suspicious transaction report to the GIF when unable to complete transactions (attempted transactions), or customer due diligence, regardless of whether or not the relationship has commenced or the transaction has been conducted.

13.1.4 Institutions should have properly documented procedures with respect to the detection and reporting of the suspicious transactions, which should cover the following:

a) There should be a clearly defined channel for reporting suspicious transactions detected by staff at all levels to the AML/CFT Compliance Officer;

b) The AML/CFT Compliance Officer should maintain, in accordance with 12, a register of all such reports submitted by the staff, which should include full details of the suspicious transactions, relevant analysis, reasons for reporting to the GIF or not, follow-up actions and other relevant information; and

c) When decision is made to report the suspicious transactions detected by the relevant staff, the AML/CFT Compliance Officer is required to report the transactions to the GIF within the prescribed time limit. It is essential that the report of the suspicious transactions should be made swiftly and not subject to undue delay or bureaucracy.

13.1.5 The report of suspicious transactions should include all relevant information for the identification of the customers specified in the Guideline and indicate the transactions detected as falling outside the normal pattern of activity of the customers.

13.1.6 Reporting of suspicious transactions should be made in the standard form prescribed by the GIF.

13.2 Tipping-off and confidentiality

13.2.1 Shareholders, board members, employees, auditors, advisors, mandataries and any other persons of the institutions covered in the Guideline cannot disclose ("tip-off") to customers or third parties any

information related to suspicious transactions that is obtained during the course of their duties. This is not intended to inhibit information sharing under 5.7.1.

13.2.2 According to paragraph 3 of Article 7 of Law no. 2/2006 and Article 11 of Law no. 3/2006, any entities reporting suspicious transactions in good faith are legally protected from assuming any responsibility and are not considered having violated any secrecy obligation.

13.3 Punishment

Non-compliance with the reporting requirement stipulated in Article 7 of Administrative Regulation no. 7/2006 will constitute an administrative offence, punishable by a fine from ten thousand (MOP 10,000) to five hundred thousand Macao patacas (MOP 500,000) for a natural person and from one hundred thousand (MOP 100,000) to five million Macao patacas (MOP 5,000,000) for a legal entity, in accordance with Paragraph 1 of Article 9 of the same Administrative Regulation, or, when the economic benefit obtained from the money laundering activity exceeds a value more than half the maximum limit (i.e. MOP 250,000 for natural persons or MOP 2,500,000 for legal entities), such limit will be double of the economic benefit, as laid down in Article 9 of the said Administrative Regulation. At the same time, any non-compliance with the requirements of the Guideline will also constitute administrative offence, punishable by the penalty measures established in Chapter II of Part IV of the FSA.

14. FINAL PROVISIONS

14.1 Institutions should implement all the measures stipulated in the Guideline from the effective date. For those accounts or business relationships that existed before the effective date of the Guideline, institutions should take a risk-based approach to identify high-risk customers who should be subject to review on a priority basis, and to establish criteria for triggering review of the lower risk accounts or business relationships (e.g. unusual transactions, transactions in large amount or transaction patterns not commensurate with background) in order to fully comply with the requirements of the Guideline eventually for all accounts and business relationships.

14.2 Any queries about the implementation of the Guideline should be directed to the Banking Supervision Department of the AMCM.