



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

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

1. INTRODUCTION

- 1.1 This “AML/CFT Guideline for Financial Institutions” is to supersede the one issued under Circular no. 072/B/2002-DSB/AMCM of 9th May 2002.
- 1.2 The previous guideline issued under the Circular mentioned above has incorporated the requirements of Decree-Law no. 24/98/M of 1st June for compulsory reporting of suspicious money laundering transactions, the concept of “know your customers (KYC)” of the Basel Committee on Banking Supervision and “customer due diligence (CDD)” among other essential criteria in the 40 Recommendations of the Financial Action Task Force (FATF) on anti-money laundering.
- 1.3 With the revision of the 40 Recommendations and the introduction of 9 Special Recommendations on combating terrorist financing by the FATF, fully implemented by Asia/Pacific Group on Money Laundering (APG) and Offshore Group of Banking Supervisors (OGBS), of which Macao has been a member, it is necessary to review and strengthen our supervisory measures to ensure consistency with international development.
- 1.4 The latest enactment of the laws and regulations in relation to prevention and suppression of money laundering and terrorist financing crimes has introduced new requirements that also demand a proper revision of the guideline.

2. SCOPE OF APPLICATION

- 2.1 This 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:
 - 2.1.1 Credit institutions with headquarters in Macao;
 - 2.1.2 Macao branches of credit institutions with headquarters abroad;



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

- 2.1.3 Overseas establishments of credit institutions with headquarters in Macao;
 - 2.1.4 Financial intermediaries with headquarters in Macao; and
 - 2.1.5 Macao branches of financial intermediaries with headquarters abroad.
- 2.2 This 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:
- 2.2.1 Finance companies authorized under Decree-Law no. 15/83/M of 26th February;
 - 2.2.2 Investment funds and investment fund management companies domiciled in Macao authorized under Decree-Law no. 83/99/M of 22nd November; and
 - 2.2.3 Offshore financial institutions, excluding those institutions engaging in insurance activities, authorized under the Offshore Regime of Decree-Law no. 58/99/M of 18th October and precedent law.

3. RISK OF MONEY LAUNDERING

- 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 of 3 years or over.
- 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 either to be broken up into smaller, less conspicuous amounts or the dirty money is 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, and from institution to



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

institution, 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 fides* financial instruments.

3.3 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 risk**. All of these risks are interrelated and can interact upon each other. The possible adverse effects of money laundering include:

3.3.1 Reputational damage, which can harm a company's share price and its relationship with customers;

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

3.3.3 Civil litigation in connection with laundered money and related crime;

4. APPLICABLE LEGISLATION

4.1 The Macao Financial System Act (FSA), approved by Decree-Law no. 32/93/M of 5th July, 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 should be recognized (Articles 40, 41, 47 and 48);

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



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

- 4.1.5 Consolidated supervision of the activity of institutions (Article 9);
- 4.1.6 Possibility of exchange of information between the Monetary Authority of Macao (AMCM) and other supervisory authorities (Paragraph 1 (b) of Article 79); and
- 4.1.7 Possibility to be precluded from banking secrecy duty by judicial order in case of criminal proceedings (Article 80).
- 4.2 Under Articles 22 and 34 of Decree-Law no. 5/91/M of 28th January on drugs control, any assets of value, including money and other valuables deposited with institutions, which have been acquired or entered into possession arising from crimes related to drugs are subject to forfeiture. For this purpose, under judiciary order or request of police with judiciary order, provision of information cannot be refused by the public or private entities including registration and tax departments when the information requester provides sufficiently concrete evidence and references for the case.
- 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 other assets will be confiscated, and 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 is transitionally applicable and will be 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 In April 2002, Law no. 4/2002 was passed to implement measures under the international conventions signed and ratified by the Central Government 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 to Macao SAR.
- 4.6 In April 2006, Law no. 2/2006 on prevention and suppression of money laundering crime was promulgated. As mentioned in point 3.1 above, Article 3 of the Law has established a clear definition of money laundering crime. Apart



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

from strengthening the relevant sanction measures, Article 5 of the Law stipulates that legal entities committing money laundering crime have criminal responsibility. 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 In late April 2006, Law no. 3/2006 on prevention and suppression of terrorism crime was promulgated. Articles 4, 5 and 6 of the Law define what are terrorist organizations, other terrorist organizations and terrorism. Article 7 of the Law stipulates that any person provides or collects funds for the purpose to finance, totally or partially, terrorism activities shall be punished with a penalty of imprisonment from 1 to 8 years or even more severe penalty. As required by Article 11 of the same Law, the provisions in Articles 6, 7 and 8 of Law no. 2/2006 after adaptation are applicable to prevention and suppression of terrorist financing.
- 4.8 In May 2006, Administrative Regulation no. 7/2006 on preventive measures against money laundering and terrorist financing crimes was also promulgated. As required by Article 7 of the Administrative Regulation, those entities as mentioned in Article 2 thereof should report, within 2 working days, to the Office of Financial Intelligence (GIF¹) any transactions which indicate money laundering and/or financing of terrorism crime. In addition to the reporting obligation, Articles 3 and 4 of the same Administrative Regulation also establish obligation 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 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 will be considered an administrative offence and subject to a fine from ten thousand (MOP 10,000) to five hundred thousand Macao patacas (MOP 500,000) for a natural person and a fine 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



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

obtained from the money laundering activity exceeds a value more than half the maximum amount (i.e. MOP 250,000 for natural persons or MOP 2,500,000 for legal entities), the value of the fine will be double of the economic benefit, as laid down in Paragraph 3 of Article 9 of the said Administrative Regulation.

5. CUSTOMER ACCEPTANCE POLICY

- 5.1 For effectively implementing the anti-money laundering (AML) and combating the financing of terrorism (CFT) measures, institutions should first develop clear customer acceptance policies and procedures, including the classification of customers into categories of relative risks.
- 5.2 The policies should set up basic account opening requirements for customers with low risk and higher requirements with extensive due diligence for high-risk customers. The following criteria can be used in risk assessment of customers:
- 5.2.1 **Background of customers:** Customers with special public or high profile position opening accounts with large sum of money will have higher risk than a working individual with a small account balance.
- 5.2.2 **Country of origin:** foreign customers are of higher risk than local customers while customers coming from jurisdictions with lower standards of legal or judicial systems or where the political environment is unstable will have higher risk than those from advanced and stable jurisdictions. It would be helpful to obtain reference from public statements on this issue through international bodies².
- 5.2.3 **Business and profession:** Customers with normal business or profession for which the nature of activities can be easily identified will incur lower risk whereas the business or job nature is unusual and the source of income or fund movement is not clear will bring higher

¹ Portuguese abbreviation for the “Gabinete de Informação Financeira (Office of Financial Intelligence)” established by Despacho of Chief Executive no. 227/2006.

² 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.ogbs.net; www.egmontgroup.org; www.transparency.org.



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

risk. Besides, business and profession with large cash transactions will also incur higher risk of money laundering and terrorist financing.

5.2.4 **Source of wealth:** There will be lower risk for a regular pattern (same period and same channel) of income source.

5.3 The policies should determine proper procedures to avoid establishing business relationship with customers who are entities designated as terrorists by the United Nations Security Council (www.un.org/Docs/sc/), Macao SAR Government³, other jurisdictions, and other organizations or entities under interregional and international legal instruments, or customers who are designated as entities subject to sanctions announced locally or abroad, or customers from countries covered in the Non-Cooperative Countries or Territories (NCCT) List announced by the FATF (www.fatf-gafi.org) or in other sanction lists with international implications.

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

6. CUSTOMER IDENTIFICATION

6.1 Institutions should establish systematic procedures for verifying the identity of new customers and beneficial owners⁴, and should not open an account until the identity of a new customer is satisfactorily established. Once having opened an account, if an institution has subsequent doubts about the customer's true identity, which it cannot resolve satisfactorily, the institution should take steps to terminate business relationship. For this purpose, the following persons should also be subject to the same customer due diligence measures:

6.1.1 The person or entity that maintains account or business relationship with the institution or, when it appears that the person or entity asking

³ The list of entities designated as terrorist is announced by the notice of Chief Executive published in the official gazette of Macao SAR Government from time to time.

⁴ "Beneficial owner" refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

for an account to be opened, or a transaction to be carried out might not be acting on his own behalf, and those on whose behalf an account or business relationship is maintained;

- 6.1.2 Beneficiaries of the transactions conducted by professional financial intermediaries or any other persons or entities;
 - 6.1.3 Any person or entity connected with a financial transaction, who can pose a significant reputational or other risks to the institutions; and
 - 6.1.4 Persons who have access to safe deposit boxes not leased by them.
- 6.2 The customer identification process should be applied at the outset of the relationship and institutions are also required to carry out regular review of existing records to ensure that the records remain up-to-date and relevant. Special attention should be exercised in the case of high-risk customers⁵ to safeguard the institution from being used for money laundering or terrorist financing. Regular review of customer records should be conducted where:
- 6.2.1 Suspicion is noted, e.g. appearance of unusual transactions or transactions not in line with the nature of business or profession stated by the customers;
 - 6.2.2 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; and
 - 6.2.3 Records are obsolete, e.g. information being irrelevant or outdated.
- 6.3 Institutions should never agree to establish business relationship with a customer who provides a fictitious name or insists on anonymity. Whereas 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 supervisors.

⁵ "High risk customers" refer to non-resident customers, customers of private banking, legal persons or arrangements such as trusts that are personal asset holding vehicles, companies that have nominee shareholders or shares in bearer form and politically exposed persons (PEPs).



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

- 6.4 Institutions are required to set up account opening procedures for different types of accounts including accounts in name of an individual, a commercial business, a trust, an intermediary or a personalised investment company. There should be proper segregation of duties and all new customers and new accounts should be approved by officers with appropriate seniority.
- 6.5 Institutions should identify the persons mentioned in 6.1 above and take reasonable measures to verify the identity of those persons before or during the course of establishing business relationships or conducting transactions for occasional customers. If it is not practicable to do so, institutions should complete the identification and verification procedures as soon as possible after establishment of the relationships. Institutions are advisable to require a declaration from customers to disclose and confirm the identity of the beneficial owners if any.
- 6.6 Under all circumstances, institutions should establish as part of the account opening procedures, the purpose of the accounts or the facilities, or the nature of its operations.
- 6.7 There should be enhanced due diligence measures for establishing business relationship with high-risk customers, including senior level approval, extra documentation or information, and cautious verification. For instance, institutions may verify the identity and background of high-risk customers by referring to publicly available information, making additional data searches, and/or seeking third party verification like reference from other bankers of such customers.

7. **MINIMUM REQUIREMENTS FOR ESTABLISHING BUSINESS RELATIONSHIP**

7.1 **Personal customers**

7.1.1 Information to be obtained at the time of establishing the business relationship:

- a) Name and/or names used;
- b) Permanent residential address;



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

- c) Date and place of birth;
- d) Name of employer or nature of profession or business;
- e) Specimen signature;
- f) Source of funds; and
- g) Purpose or nature of account or facility.

7.1.2 Institutions should verify the above information against valid original documents of identity issued by governmental authority (examples including identity cards and passports). Such documents should be those that are most difficult to obtain illicitly.

7.1.3 For Macao residents, the proper identification documents are the “*Bilhete de Identidade de Residente Permanente*” (Permanent Resident Identity Card), “*Bilhete de Identidade de Residente Não Permanente*” (Non-permanent Resident Identity Card) and “*Bilhete de Identidade de Residente de Macau*” (Macao Resident Identity Card), all issued by the “*Direcção dos Serviços de Identificação*” (Identification Bureau) or other equivalent identification documents.

7.1.4 Particular care should be taken in accepting documents that are easily forged or which can be easily obtained in false identities in case of non-resident customers.

7.1.5 Where there is face-to-face contact, the appearance should be verified against a governmental document bearing a photograph and even in non-face-to-face situations, at least one copy of governmental document bearing a photograph should be gathered by the institutions.

7.1.6 Regarding information other than the identity of customers, institutions should exercise duly care to verify the truth of the information provided. For example, the address can be checked against a recent utility bill of the customers.

7.2 Corporate and other business customers

7.2.1 Information to be obtained:



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

- a) Incorporation or equivalent documents issued by the relevant government agencies. For locally incorporated companies, company search report from the “*Conservatória dos Registos Comercial e de Bens Móveis*” (Businesses and Vehicles Registry), tax declaration for the “*Direcção dos Serviços de Finanças*” (Finance Services Bureau), certificate of incorporation, business registration certificate, memorandum and articles of association, etc. For companies incorporated abroad, apart from equivalent documents as mentioned for local ones, certificate of good standing and other relevant documents. If original documents could not be obtained, copies of the documents should be properly certified⁶. Where certified documents are accepted, it is the responsibility of the institutions to satisfy themselves that the certifier is appropriate;
- b) Valid identification document of the principal shareholders, beneficial owners, directors and other persons authorized to operate the accounts, including the resolution of the board of directors to open an account and authorization for those who will operate the account;
- c) Nature of business; and
- d) Purpose or nature of account or facility.

7.2.2 If possible, institutions should take reasonable measures to verify whether the corporate customer operates its stated business at the stated address. Institutions should obtain evidence for all the information specified above to verify the legal status of the companies. 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 structure or ownership occur subsequently, further checks should be made.

⁶ 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 serving 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.



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

7.2.3 Institutions need to be vigilant in preventing corporate business entities from being misused by natural persons. Institutions should understand the structure of the companies sufficiently to determine the true identity of the ultimate owners or those beneficial owners who have control over the companies and/or the funds.

7.2.4 For other customers with appropriate legal personality such as non-profit organizations and foundations, similar relevant information specified above should be obtained, recorded and verified.

7.3 Introduced business

7.3.1 In case customers are referred by other institutions or introducers, proper care should be exercised to determine whether the introducers can be relied upon and the following criteria should be observed:

- a) The introducers should be regulated and supervised and should follow the same customer due diligence practices identified in this guideline;
- b) Institutions should satisfy themselves as to the reliability of the systems put in place by the introducers to verify the identity of the customers;
- c) For all introduced business, all relevant identification data and other documentation pertaining to the customers' identity, upon request, should be immediately available to the institutions who should carefully review such information as provided.

7.3.2 Under any circumstances, the institutions relying on customer due diligence performed by other institutions or introducers are still responsible for verification of the identity of the customers so referred.

8. BUSINESS RELATIONSHIPS REQUIRING ENHANCED DUE DILIGENCE

8.1 Trust, nominee and fiduciary accounts or client accounts opened by professional intermediaries



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

- 8.1.1 Institutions should establish whether the customers are acting on behalf of other persons as trustees, nominees or professional intermediaries (e.g. lawyers or accountants). If so, institutions should obtain satisfactory evidence of the identity of any intermediaries and of the persons on whose behalf they are acting, as well as details of the nature of the trust or other arrangements in place.
- 8.1.2 Whatever the nature of the customer relationship, institutions should obtain the identity of its customers, even if these are represented by professional intermediaries, such as lawyers or accountants. The procedures for identifying nominee customers are no different from those for identifying other customers. Special care should also be exercised in initiating business transactions with “shell companies⁷”. Satisfactory evidence of the identity of their beneficiary owners should be obtained. 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 establish any business relationships.
- 8.1.3 In relation to customers that are legal arrangements (express trusts⁸ or similar arrangements), the institutions should also take reasonable measures to identify the settlors⁹, trustees¹⁰, beneficiaries¹¹ and any other persons involved in the structuring of the arrangement (e.g. a protector).

8.2 Non-face-to-face customers

- 8.2.1 For local customers, the accounts should not be opened without the physical presence of the customers for interview and the account

⁷ “Shell company” refers to a company that exists in name only, or that there may be no employees, physical office and operations / business activity.

⁸ “Express trust” refers to a trust clearly created by the settlor, usually in the form of a document e.g. written deed of trust.

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 the assets in a trust fund separate from his/her own assets. They invest and dispose of them in accordance with the settlor’s trust deed, taking account of any letter of wishes. These may also be a protector, who may have power to veto the trustees’ proposals or remove them, and/or a custodian trustee, who holds the assets to the order of the managing trustees.

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.



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

opening procedures specified above should be exercised to ensure the verification of the identification of customers.

8.2.2 For non-resident customers, institutions should apply equally effective customer identification procedures and ongoing monitoring standards for non-face-to-face customers as for those available for interview. There should also be specific and adequate measures to mitigate the higher risk including:

- a) Certification of documents presented, e.g. the documents certified and/or verified by a respondent institution or a third party on which the institution can rely;
- b) Requisition of additional documents to complement those required for face-to-face customers, e.g. information provided by another institution subject to similar customer due diligence standards;
- c) Referral by an introducer who is subject to the identification procedures stated above;
- d) Requiring the first payment to be carried out through an account in the customer's name with another institution subject to similar customer due diligence standards.

8.3 Politically exposed persons

8.3.1 Business relationships with individuals who are or have been entrusted with prominent public functions in a jurisdiction outside Macao and with persons or companies clearly related to them may expose an institution to significant reputational and/or legal risks. Such politically exposed persons (PEPs) include Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials, their family members and close associates. There is always a possibility that, especially in jurisdictions where corruption is pervasive, such persons may have abused their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc. Therefore, enhanced due diligence should be exercised by institutions for business relationship with such foreign PEPs.



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

- 8.3.2 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.
- 8.3.3 Institutions should gather sufficient information from a new customer, and check publicly available information or commercial electronic databases of PEPs, in order to establish whether or not the customer is a PEP. Institutions should investigate the source of funds before accepting a PEP as customer. The decision to open an account for a PEP should be taken at senior level. Where a customer has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a PEP, senior level approval is required for continuing the business relationship.
- 8.3.4 Institutions should take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs. Where financial institutions have business relationship with a PEP, they should conduct enhanced ongoing monitoring on that relationship.

8.4 **Funds transfers**

- 8.4.1 For all funds transfers, ordering institutions should obtain and maintain the information of customers and other relevant information as required in point 4.1.1 of the AML/CFT Guideline on Large Cash Transactions promulgated by the same Notice. However, the funds transfers do not include financial institution-to-financial institution transfers and settlements where both the originator person and the beneficiary person are financial institutions acting on their own behalf.
- 8.4.2 The funds transfers, if contained within a batch transfer, should be accompanied with all necessary originator information as required in point 8.4.1 above. For transactions using credit or debit cards to effect the funds transfers, if processed within a batch transfer, the required information can be simplified to include at least originators' account number or card number. Institutions should ensure that non-routine transactions of such funds transfers are not batched.



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

8.5 Correspondent banking

8.5.1 Correspondent banking is the provision of a current or other liability account and related services by one institution (the correspondent institution) to another institution (the respondent institution) to meet its fund clearing, liquidity management and short-term borrowing or investment needs. When establishing correspondent relationships, institutions should consider the following factors:

- a) Respondent institution's management;
- b) Major business activities;
- c) Where the institution locates (institutions should avoid establishing business relationship with respondent institutions that locate in jurisdictions with poor KYC/CDD or AML/CFT controls or are included in the NCCT list published by the FATF);
- d) Purpose or nature of accounts or facilities; and
- e) The identity of any other third parties that may have access to the correspondent services.

8.5.2 Institutions should gather sufficient information on their respondent institutions to understand their business nature, reputation and supervision, and to see whether there are any money laundering or terrorist financing investigations or regulatory actions against the respondent institutions and should avoid establishing business relationship with any shell institutions including shell banks¹².

8.5.3 Institutions should also assess and ascertain if the respondent institutions' AML/CFT controls are adequate and effective. Top management approval should be required before establishing any new correspondent relationships. The respective responsibilities of each institution in AML/CFT should also be documented.

¹² "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.



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

8.5.4 Where a correspondent relationship involves the maintenance of “payable-through accounts¹³”, institutions should be satisfied that:

- a) Their customers (the respondent institutions) have performed all normal customer due diligence obligations on those customers that have direct access to the accounts of the correspondent institutions; and
- b) The respondent institutions are able to provide relevant customer identification data upon request to the correspondent institutions.

9. ONGOING MONITORING OF HIGH-RISK ACCOUNTS

9.1 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.

9.2 For all accounts, institutions should have systems in place to detect unusual or suspicious patterns of account activity. This can be done by establishing certain parameters for a particular class or category of accounts to detect unusual or irregular transactions that require particular attention. Any such transactions or transactions not consistent with the normal activities of the customers should be recorded for review of the senior officer or AML/CFT Compliance Officer of the institutions for their further follow-up. Reference can be made to the examples of suspicious transactions provided by AMCM.

9.3 For those higher risk accounts classified according to their customer acceptance policies (please also refer to 6.2 and 8 for examples of high-risk customers), institutions should establish control systems for monitoring these accounts:

9.3.1 Senior officers and/or AML/CFT Compliance Officers of institutions should be provided with periodic reports with adequate information of the higher risk accounts, including but not limited to unusual transactions and aggregate total of business relationship with the institutions;

¹³ “Payable-through accounts” refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

9.3.2 Management in charge of private banking should be aware of the personal profiles of the high-risk customers and be alert to sources of third party information. Transactions in large amount done by these customers should require senior level approval.

10. AML/CFT COMPLIANCE OFFICER

10.1 Institutions should designate a Compliance Officer responsible for AML/CFT compliance. The designation of the AML/CFT Compliance Officer requires prior approval from the AMCM. In addition to appropriate competence and experience, the following criteria should also be considered:

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

10.1.2 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

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

11. RISK MANAGEMENT

11.1 The board of directors or top management of institutions should establish an effective AML/CFT system and ensure its effective implementation by establishing appropriate procedures. The Compliance Officer should coordinate and follow up all internal reports on high-risk customers and suspicious transactions.

11.2 There should be internal procedures to assess whether institutions' AML/CFT policies and legal requirements for reporting suspicious transactions are complied with. Institutions' internal audit plays an important role in independently evaluating risk management and controls. The compliance check for AML/CFT policies and procedures should be included in the audit programme to ensure the effectiveness of the control systems.



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

11.3 All institutions should have an ongoing employee training programme so that staff members are adequately trained in AML/CFT measures and other relevant procedures. The training programme should be designed according to different needs of staff, in particular, new staff, front line staff, supervisory staff and staff with compliance and audit functions. For instance, new staff members should be educated the importance of AML/CFT policies and other 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 pattern of suspicious transactions. Supervisory staff members should be trained in skills in monitoring proper execution of the policies and procedures. The training for staff members with compliance and audit functions should be focused on the corresponding fields. Regular refresher training should be provided to ensure that all staff members are reminded of their responsibilities and are kept informed of new developments.

12. RETENTION OF RECORDS

12.1 Institutions should keep all records of customer information, including entries of the accounts and details of transactions involving fund transfer for at least 5 years (without prejudice to the stipulations in other laws and regulations¹⁴) 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. Institutions should also keep records of the identification data obtained through the customer due diligence process, account files and business correspondence for at least 5 years (without prejudice to the stipulations in other laws and regulations¹⁵) after termination of the business relationships.

12.2 The above records should be retained by way in accordance with Article 6 of Administrative Regulation no. 7/2006. In addition, the records should be readily available to the competent authorities in Macao for investigation when necessary.

¹⁴ For example, article 49 of the Commercial Code imposes a minimum period of 10 years for the keeping of all the books, correspondence and other documentation related to the activity of financial institutions and other companies.

¹⁵ As footnote 14 above.



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

13. REPORTING OF SUSPICIOUS TRANSACTIONS

- 13.1 Transactions indicating signs of money laundering crime and/or financing of terrorism crime as prescribed in Law no. 2/2006 and Law no. 3/2006, or transactions 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.
- 13.2 As required by Article 7 of Administrative Regulation no. 7/2006, the institutions covered in this guideline should report any suspicious transactions to the Office of Financial Intelligence (GIF) within 2 working days after realization of the transactions (please also refer to point 14 – Transitional and Final Provisions).
- 13.3 Institutions should have properly documented procedures with respect to the detection and reporting of the suspicious transactions, which should cover the following:
- 13.3.1 There should be a clearly defined channel for reporting suspicious transactions detected by staff at all levels to the AML/CFT Compliance Officer;
- 13.3.2 The AML/CFT Compliance Officer should maintain a register of all such reports submitted by the staff, which should include full details of the suspicious transactions, evidence of analysis of the transactions undertaken, and the reasons for decision to report or not to report the transactions to the GIF indicated in 13.2 above; and
- 13.3.3 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 indicated in 13.2 above, within 2 working days after realization of the transactions. It is essential that the report of the suspicious transactions should be swift and not subject to undue delay of bureaucracy.
- 13.4 The report of suspicious transactions should include all relevant information for the identification of the customers specified in this guideline and indicate



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

the transactions detected as falling outside the normal pattern of activity of the customers.

- 13.5 The shareholders, directors, officers and any employees of the institutions covered in this guideline cannot disclose any information contained in the report to any third parties including the customers connected with the suspicious transactions, pursuant to Paragraph 4 of Article 7 of Law no. 2/2006.
- 13.6 According to paragraph 3 of Article 7 of Law no. 2/2006, any entities reporting suspicious transactions in good faith are legally protected from assuming any responsibility and are not considered having violated any secrecy obligation.
- 13.7 Non-compliance with the reporting requirement stipulated in Article 7 of Administrative Regulation no. 7/2006 is considered an administrative offence, which shall be punishable with a fine from ten thousand (MOP 10,000) to five hundred thousand Macao patacas (MOP 500,000) for a natural person and a fine 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 amount (i.e. MOP 250,000 for natural persons or MOP 2,500,000 for legal entities), the value of the fine will be double of the economic benefit, as laid down in Paragraph 3 of Article 9 of the said Administrative Regulation. On the other hand, any non-compliance with the requirements laid down in this guideline will also be considered administrative offence and subject to penalty measures under Chapter II of Part IV of the Financial System Act.

14. TRANSITIONAL AND FINAL PROVISIONS

- 14.1 This guideline will come into effect on 12th November 2006, which is in line with the effective date of Administrative Regulation no. 7/2006.
- 14.2 As stipulated in Paragraph 1 of Article 10 of Law no. 2/2006, Decree-Law no. 24/98/M of 1st June is transitionally applicable up to the effective date of Administrative Regulation no. 7/2006. Therefore, report of suspicious transactions should continue to be sent to the Judiciary Police under advice to the AMCM during the transitional period.



澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

- 14.3 After the end of the transitional period, i.e. 12th November 2006, suspicious transactions should be reported to GIF directly, but no longer under advice to the AMCM. Proper instructions will be issued opportunely to financial institutions for submitting to the AMCM certain periodic statistics in respect of their reporting of suspicious transactions.
- 14.4 Reporting of suspicious transactions should be made in the standard form to be advised by the AMCM in writing.
- 14.5 Institutions should implement the measures stipulated in this guideline on all new accounts or new business relationships from the effective date. For existing accounts or business relationships, institutions should take a risk-based approach to identify higher 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).
- 14.6 Within a month from the date of the guideline, each institution should submit an application to AMCM for prior approval for designation of an AML/CFT Compliance Officer.
- 14.7 Any queries about the implementation of the guideline should be directed to the Banking Supervision Department of the AMCM.