



大豐銀行
BANCO TAI FUNG

TAI FUNG BANK LIMITED

MACAU

**ANTI-MONEY LAUNDERING AND COMBATING
FINANCING OF TERRORISM MANUAL**

FORTH REVISION

1 JUNE 2009



TABLE OF CONTENTS

Chapter One: Overview	1
1.1 Introduction.....	1
1.2 Bank Policy.....	1
1.3 Legislation on Money Laundering and Financing of Terrorism in Macau	1
1.4 Departmental/Branch Responsibilities.....	3
Chapter Two: Compliance Officer and Deputy Compliance Officer	4
2.1 Appointment	4
2.2 Roles and Responsibilities	4
Chapter Three: Customer Identification.....	5
3.1 General Policy.....	5
3.2 Personal and Joint Accounts	5
3.3 Company Accounts	6
3.4 Clubs, Societies, Associations and Charities Accounts	7
3.5 Trust, Nominee, Fiduciary Accounts or Client Accounts opened by Professional Intermediaries.....	7
3.6 Shell Banks and Shell Companies	8
3.7 Politically Exposed Persons	8
3.8 Outward Remittance	8
3.9 Inward Remittance	9
3.10 Safe Deposit Boxes and Safe Custody.....	9
3.11 Transactions Undertaken for Non-Account Holders (occasional customers).....	9
3.12 Investment Related Transactions	10
3.13 Loan Related Transactions.....	10



大豐銀行

BANCO TAI FUNG

3.14	Correspondent Banking	11
3.15	Introduced Business	11
3.16	Other Restrictions on Transactions	11
3.17	Maintaining and Updating Customer Information.....	12
Chapter Four: Record Keeping		13
4.1	Retention Period.....	13
4.2	Format of Retention	13
Chapter Five: Monitoring and Reporting Suspicious Transactions		14
5.1	Recognition	14
5.2	Transaction Monitoring.....	14
5.3	Report Obligation.....	15
5.4	Non-disclosure Obligation	16
Chapter Six: Training		17
6.1	Seminar	17
6.2	Reader Induction and Reinforcement	17
Chapter Seven: Amendments and publications		18



Chapter One: Overview

1.1 Introduction

The process of using the financial system to legitimise funds that have been acquired illegally is called “**Money Laundering**” and the funding, assisting in or facilitating the funding of individuals or organizations who or which are known or suspected as terrorists or being linked to terrorists or promoting terrorism is called the “**Financing of Terrorism**”. The use of the financial system for money laundering by criminals and for funding their activities by terrorists is of concern to the Office of Financial Intelligence (GIF), Judiciary Police, the Monetary Authority of Macau (AMCM) and other law enforcement authorities. It is also a concern to management of the Bank since inadvertent association with these criminal activities may lead to adverse publicity and direct loss from possible fraud. The Bank and the relevant staff member may also commit a criminal offence for knowingly processing or assisting in the processing of illegal money in order to disguise its origin or for facilitating or assisting in facilitating the financing of terrorism.

1.2 Bank Policy

In accordance with the guidelines issued by AMCM, Tai Fung Bank has laid down policy for protection against money laundering and financing of terrorist activities using the banking system. All employees should adhere strictly to the policy regardless of the products or services provided. Therefore, under no circumstances will the Bank offer products or services or provide assistance in transactions where staff has good reason to suspect that the customer is associated with money laundering and terrorist activities. Any staff member who fails to adhere to any of the policies will be subject to disciplinary actions.

1.3 Legislation on Money Laundering and Financing of Terrorism in Macau

To be in line with the international community to combat against money laundering and financing of terrorism, the Government of Macau has introduced a new legal framework composed of three tiers which include laws adopted by the Legislative Council, administrative regulations published by the Chief Executive and guidelines or instructions issued by the respective supervisory authorities to address these problems. By force of Law No. 2/2006 enacted on 3rd April 2006 and Law No. 3/2006 enacted on 10th April 2006,



大豐銀行

BANCO TAI FUNG

money laundering and financing of terrorism are made criminal offences and individuals or corporate entities committing such offences are subject to criminal liabilities. The Administrative Regulation No. 7/2006 published on 15th May 2006 establishes the statutory duty to prevent money laundering and financing of terrorism and defines the scope of economic operators and their respective supervisory authorities that must observe such duty and the Administrative Ruling No. 227/2006 published on 7th August 2006 provides the basis for setting up the Office of Financial Intelligence (GIF) to collect information related to money laundering and financing of terrorism and to handle reports on such activities. The supervisory authorities named in Administrative Regulation No. 7/2006 shall issue guidelines or instructions to the economic operators they oversee for the latter to follow in their operations.

As set out in Article 3 of the Law No. 2/2006, any act or acts to convert, transfer or dissimulate properties or proceeds from illicit activities punishable with a maximum penalty of imprisonment of 3 years or more, or to knowingly process or assist in the processing of illicit proceeds in order to disguise their illegal origin, or to assist the culprit of such offences and/or his accomplices to circumvent prosecution and penalty shall be punishable with a penalty of imprisonment from 2 to 8 years. Any person who provides or collects funds for the purpose of financing, totally or partially, terrorist activities is punishable with a penalty of imprisonment from 1 to 8 years or more as laid down in Article 7 of the Law No. 3/2006. By virtue of paragraph 4 of the same article, it is strictly prohibited to unveil to any person that he is being under investigation. Article 2 of both legislations also provides that the rules of the Criminal Code are applicable to offences stipulated in the above Laws as supplementary measures. Under articles 22 and 34 of Decree-Law No. 5/91/M, all assets associated with or derived from offences against drugs control are subject to forfeiture and assets originated from criminal offences shall likewise be confiscated under paragraph 2 of Article 103 of the Criminal Code.

Additionally the Administrative Regulation No. 7/2006 establishes the statutory duty for every person to disclose his knowledge of any transactions associated with money-laundering and financing of terrorism. It also requires various economic operators, including banks, to report the operations suspected of involving conversion, transfer or dissimulation of illicit properties or proceeds and/or financing of terrorism to the Office of Financial Intelligence (GIF) within 2 working days after realization of the transactions as stipulated in Article 7 of the said Regulation. Such disclosure will not be treated as a breach of professional confidentiality owed to the customers. Failure to comply with the obligation is punishable with a fine of MOP10,000.00 to MOP50,000.00 for an individual, or in case of a corporate entity, a fine of MOP100,000.00 to



大豐銀行

BANCO TAI FUNG

MOP5,000,000.00 or the double of the value the corporate entity benefits from the offence if that value is more than half of the maximum fine.

In concert with efforts of the international community to combat terrorist activities, the anti-terrorism measures under relevant resolutions of the United Nations Security Council are made applicable in Macau SAR under Law No. 4/2002.

1.4 Departmental/Branch Responsibilities

It is the responsibility of each department and branch manager to ensure that each staff is fully aware of the Bank's policy and procedural requirements and their on-going compliance. Besides, he must ensure that all personnel under his supervision are adequately trained in detecting and reporting transactions suspected of being related to money laundering or other illegal activities and/or financing of terrorism. Human Resources Department will provide necessary training support to help the department and branch managers to well play this role. The Internal Audit Department will conduct from time to time routine or spot investigations to ensure that all departments/branches are acting in compliance with legal and supervisory as well as internal procedural requirements.

Since August 2008, the Bank has established a Risk Management Department, under which an AML/CFT Team is specially set up to monitor the activities of suspected customers and to oversee if departments/branches act in compliance with AML/CFT regulations. The Team also assists the Compliance Officers and the AML & CFT Committee in formulating necessary and timely measures for the proper management of day-to-day operations.

In addition, all bank staff must understand the bank's business and the related operations or functions they are responsible for, transactions processed in their responsible areas, and how such transactions can be used as vehicles for laundering money or financing terrorism. In case of doubt or suspicion, prompt consultation with or reporting to the responsible Departmental General Manager and the Bank's Compliance Officer, or his deputy when he is absent, should be made.



Chapter Two: Compliance Officer and Deputy Compliance Officer

2.1 Appointment

Senior staff shall be appointed by the Bank, with the subsequent approval of AMCM, as Compliance Officer and Deputy Compliance Officer respectively, playing the role to ensure compliance with all regulatory guidelines and rules relating to the prevention of money-laundering and terrorist activities. The Compliance Officers will be assisted by a special “Anti-Money Laundering and Combating Financing of Terrorism (AML & CFT) Committee” comprised of members mainly from operations and control departments, as well as by the AML/CFT Team, to carry out their assigned roles and responsibilities.

2.2 Roles and Responsibilities

Compliance Officer and Deputy Compliance Officer play a consultative, monitoring, management and operations role to:

- a) Provide guidance on development of compliance policies and guidelines relating to money laundering and financing of terrorism;
- b) Set direction on effective ways of securing compliance, namely, induction through policies and guidelines, fostering through classroom training and reinforcement via annual refresher review of guideline;
- c) Update employees of the Bank of money laundering and terrorist financing related statutory and regulatory requirements;
- d) Report to the President Office on relevant compliance issues;
- e) Liaise with staff members on reports submitted for suspicious cases;
- f) Advise on evaluating suspicious cases to see whether there are reasonable grounds to believe that a suspicious case should be reported to the Office of Financial Intelligence (GIF);
- g) Review all reports prior to the submission to external parties;
- h) Keep a register of all reports submitted by staff members and made to the external parties;
- i) Liaise with regulatory authorities and respond to their enquiries; and
- j) Liaise with compliance officers of correspondents on issues relating to the prevention of money laundering and financing of terrorism.



大豐銀行

BANCO TAI FUNG

Chapter Three: Customer Identification

3.1 General Policy

To ensure that the Bank is not used as a channel for criminal or terrorist funds, we must adopt the principles of “**Know Your Customer**” and “**Customer Due Diligence**”. We should make reasonable efforts to determine the customer’s true identity and verify the bona fide of new customers as required by Article 106 of the Macau Financial System Act. Anonymous accounts or accounts in obviously fictitious names should not be established. If possible, prospective customer should be interviewed personally.

Apart from identity, we should also obtain from new customers information regarding their background, country of origin, business or profession, source of wealth and other information as the “AML & CFT” Committee may deem necessary to evaluate the level of risk associated with such customers. The opening of accounts in favour of customers with higher risks requires the approval of officers with more seniority. Nevertheless, we should not establish or maintain relationship with any person or corporate entity that declines to provide the required information to us.

3.2 Personal and Joint Accounts

We should ensure that the individual should produce primary identification such as Macau identity card, passport or other official identification documents issued by the government to confirm that he is the beneficial owner of the account. If there is doubt about whether an identification document is genuine, contact should be made with the Department of Identification, the Immigration Section of the Macau Police Force or the relevant consulates in Macau to ascertain whether details on the document are correct.

Satisfactory evidence to establish the identity of new customer(s) should include:

- Name and/or names used;
- Permanent residential address;
- Telephone number;
- Date and place of birth;
- Occupation and name of employer (if not self-employed); or
- Nature of business and name of firm (if self-employed);
- Source of funds; and



大豐銀行

BANCO TAI FUNG

- Purpose or intended use of account or facility.

3.3 Company Accounts

A) Limited company and sole proprietorship

The following documents should be obtained with copies for file (the necessity may depend upon which type of company is):

- a) Company search (within 3 months from the issue date);
- b) Official Gazette, certified deed of incorporation or Memorandum and Article of Association;
- c) M1, M7 and/or M8 forms;
- d) Board resolution to open an account and to confer authority on those who will operate it (if necessary);
- e) Identification documents of sole proprietor, beneficial owners and persons authorized to operate the account (in case of a sole proprietorship).
- f) Identification documents of principal shareholders, beneficial owners, directors and persons authorized to operate the account (in case of a limited company).

When we become aware of subsequent changes to the company structure or ownership, or suspicions are aroused by a change in the pattern of transactions, a further search should be conducted.

Other compulsory or supplementary information that must or may be considered:

- Information and credentials that identify the prospective account, its authorized signatories and the nature of the business (obtain on best effort basis);
- Financial statements, annual reports, marketing brochures (obtain on best effort basis);
- Source of funds (compulsory); and
- Purpose of the account and a description of the expected type and volume of account activity (compulsory).

Special attention must be paid to the request for opening of accounts in favour of locally incorporated company/sole proprietorship that does not have business or physical presence in Macau and the shareholder(s)/owner(s) of which is/are non



大豐銀行

BANCO TAI FUNG

resident(s) of Macau or off-shore company/companies incorporated either in Macau or overseas. If the shareholder or owner of a company is another corporate entity, the ultimate beneficial owner must be properly identified in accordance with the criteria stated above.

In case of financial institutions, the responsible staff should ensure that the institution concerned is on the relevant regulator's list of regulated institutions.

B) Companies incorporated outside Macau

The opening of accounts for such companies is not accepted, unless approved by senior level or arranged by acceptable correspondents as per our internal procedural requirements.

Documents comparable to those listed in Section A should be obtained. These documents should be verified by qualified persons such as notary publics/lawyers/accountants (preferably in the country of incorporation) and if necessary further certified by the Consulate of the People's Republic of China in or nearest to the country of incorporation or authorized personnel of our correspondents.

3.4 Clubs, Societies, Associations and Charities Accounts

For accounts to be opened in favour of clubs, societies, associations or charities, we should obtain documentation to satisfy ourselves with the legitimate purpose of the organization e.g. by requesting for the relevant certificate issued by the Department of Identification of Macau and a copy of the constitution. Copy of identification documents of all the authorized signatories should also be obtained.

3.5 Trust, Nominee, Fiduciary Accounts or Client Accounts opened by Professional Intermediaries

The opening of trust, nominee and fiduciary accounts or client accounts by professional intermediaries is not accepted.



3.6 Shell Banks and Shell Companies

The opening of accounts for both shell banks and shell companies is not accepted.

3.7 Politically Exposed Persons

The opening of accounts for politically exposed persons, their associates and family members from countries or territories outside Macau SAR is not recommended and the acceptance thereof should be approved by the compliance officer or his deputy. Request to open accounts in favour of those from Macau SAR may be entertained subject however to satisfaction of customer identification criteria stated above.

3.8 Outward Remittance

Save outward remittances by means of “**Moneygram**” in which case the maximum amount should not exceed USD10,000.00 or the equivalence thereof, all other outward remittances on behalf of non-account holders are not accepted except for transaction that is HKD20,000.00 or less or of an equivalent amount in any other currency. For all outward remittances, the following particulars of the transaction should be recorded regardless of the amount:

- a) Transaction reference number;
- b) Transaction type, currency, amount and value date of the remittance;
- c) Date of remitter’s instructions;
- d) Instruction details
 - Name of beneficiary;
 - Address or account number of beneficiary;
 - Name and address or identifiable codes of beneficiary bank;
 - Remitter’s message to beneficiary (if any);
- e) Name, identity card number (or any other document of identity or travel document number with place of issue) of remitter or his representative must be verified if he appears in person; and
- f) Telephone number and address of remitter.



3.9 Inward Remittance

Save inward remittances by means of “**Moneygram**” in which case the maximum amount should not exceed USD10,000.00 or the equivalence thereof and may be paid in cash, all other inward remittances in favour of non-account holders are not accepted except for transaction that is HKD20,000.00 or less or of an equivalent amount in any other currency and must be paid to beneficiary by means of a “**non-negotiable**” and “**account payee only**” cashier order. For all inward remittances, the following particulars of the transaction should be recorded regardless of the amount:

- a) Transaction reference number;
- b) Transaction type, currency, amount and value date of the remittance;
- c) Date of remitter’s instructions;
- d) Instruction details
 - Name and address or account number of beneficiary;
 - Name and address or account number of remitter;
 - Name and address or identifiable codes of remitting bank;
 - Remitter’s message to beneficiary, if any; and
- e) Name and identity card number (or any other document of identity or travel document number with place of issue) of beneficiary must be verified if he appears in person.

3.10 Safe Deposit Boxes and Safe Custody

Safe deposit boxes may be opened to non-account holders provided that they are local residents or non-residents duly authorized to carry on business or to work in Macao; subject however to satisfaction of customer identification criteria stated above. Nevertheless, safe deposit boxes opened in favour of non-residents that do not maintain account relationship with us are not recommended. Requests to hold boxes, parcels and sealed envelopes in safe custody in the vault or other areas of the office premise for both account holders and non-account holders should **NOT** be entertained. Exception requires the approval of the President Office.

3.11 Transactions Undertaken for Non-Account Holders (occasional customers)

Where transactions are undertaken for non-account holders e.g. where funds are



大豐銀行

BANCO TAI FUNG

deposited into any existing account by persons whose names do not appear on the mandate of that account, care and vigilance are required. If the transaction is a high-risk cash transaction which involves amounts in excess of HKD20,000.00 or the equivalence thereof and is unusual, the customer should be requested to produce positive evidence of personal identity and source of funds. The name, number and type of identification document of the customer as well as his telephone number, or address or account number, if any, must be properly recorded and copy of the identification document should be kept on file, if necessary.

For encashment of travellers' cheques and other instruments payable by us, regardless of the amount, satisfactory evidence of identity should be obtained (e.g. a current valid passport or Macau identity card) with the name of the presenter and the number and type of his identification document recorded on the reverse side of the cashed cheque or instrument. If the amount of the cheque or instrument is over HKD20,000.00 or the equivalence thereof, the telephone number, or address or account number, if any, of the presenter must also be taken down. For all encashment transactions by means of credit cards, regardless of the amount, the card holder must be identified by the criteria applied to high-risk cash transactions.

In general, transactions undertaken for non-account holders should only be restricted to remittances, cash exchanges, gift cheques and cash withdrawals by means of credit cards and the amounts of such transactions should preferably be under the threshold established for each of them.

3.12 Investment Related Transactions

Investment related transactions should not be undertaken for customers without establishing account relationship with us and all settlements of such transactions must be made through the account. Request by customers for placing in our custody investment instruments such as bonds, certificates of deposit and securities which are not acquired by means of the bank or its authorized representative must not be accepted unless information regarding the source of such instruments is obtained to our satisfaction.

3.13 Loan Related Transactions

Loan related transactions, including trade related advances, should not be undertaken



大豐銀行

BANCO TAI FUNG

for customers without establishing account relationship with us and all payments and repayments of such transactions must be made through the account, save syndicate loans wherein we are not mandated. A customer requesting for a loan or other banking facilities must inform the bank the purpose of the loan, the source of collateral and the origin of funds for repayment. Apart from normal credit appraisal, the customer is also required to be identified according to the criteria stated above.

3.14 Correspondent Banking

Transactions with correspondents that are based in countries or territories without adequate and effective “**Know Your Customer**”/“**Customer Due Diligence**” or “**Anti-Money Laundering**”/“**Combating Financing of Terrorism**” controls should not be accepted.

Direct deposits effected without our knowledge by a customer or his representative into the Bank’s account with our overseas correspondents for whatsoever purpose should be refused and rejected even if our correspondents inadvertently accept such deposits.

Direct deposits by a customer or his representative into a correspondent’s account with the Bank for whatsoever purpose should also be refused and rejected, unless prior arrangement has been made with the correspondent.

3.15 Introduced Business

Save customers that are referred by the Bank’s correspondents, no other introduced business should be accepted and customers of introduced business should also be identified properly.

3.16 Other Restrictions on Transactions

Transactions involving customers that are based in non-cooperative countries and territories (NCCT) or the like are not accepted.

Transactions involving customers that are sanctioned by or based in countries and territories sanctioned by the Macau SAR Government and/or the United Nations Security



Council are strictly prohibited and should be reported immediately to the authorities.

Transactions involving customers that are subject to sanction or based in countries and territories subject to sanction of other foreign governments or international organizations should be avoided provided that such refusal or rejection does not violate or contradict with the rules and regulations of the Macau SAR Government.

3.17 Maintaining and Updating Customer Information

Account activities must be monitored regularly to determine whether they are consistent with the customer's normal and expected activity. Transactions or patterns of activities which are considered inconsistent with a customer's profile should be scrutinized for propriety and reported to the responsible Departmental General Manager and Compliance Officer as soon as possible. Department/Branch managers and the "AML & CFT Committee" must check "**Customer Daily Aggregate Cash/Transfer Deposit/Withdrawal Exceed Limit Report**" and "**Customer Daily Money Exchange Report**" and Functional Department managers must check each month "**Customer Monthly Aggregate Cash/Transfer Deposit/Withdrawal Exceed Limit Report**" and "**Inward/Outward Remittance Monthly Report**" to verify if the irregular situation stated above has already occurred. Members from the "AML & CFT" committee will conduct surprise audits on a random basis to test if the results of departmental/branch checks are satisfactory, in addition to carrying out verifications if holders of newly opened accounts meet our "**Know Your Customers**" requirements and such holders as well as remitters and beneficiaries of both inward/outward remittances are not among the various lists of sanctioned criminals and/or terrorists released or instructed to be observed by the Macau SAR. Full departmental/branch checks will be conducted on a spot basis at least once annually at such times as the Compliance Officer deems fit and reports of findings and recommendations must be filed with the "AML & CFT" Committee.

Customer information must be updated within a reasonable period of time and customers will be segmented into different levels of risk according to their latest information as well as a number of factors to be determined from time to time by the "AML & CFT" Committee. Customers with higher risks should be monitored with more intensity.



Chapter Four: Record Keeping

4.1 Retention Period

The following document retention period should be observed:

A) *Account opening records*

Copies of identification documents should be kept in file for no less than 10 years following the closing of an account opened on or after 2nd September 1991. For an account opened before 2nd September 1991, the same retention period applies only if copies of identification documents have been subsequently obtained from customers.

B) *Account ledger/statement records*

10 years from entering the transaction into the ledger.

C) *Records in support of entries in the accounts in whatever form (e.g. credit/debit slips, vouchers)*

10 years from when the records were created. In situations where the records relate to on-going investigations, or transactions that have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed. If in doubt, advice from the Compliance Officer should be obtained.

D) *Records in support of remittance transactions for non-account holders*

10 years from when the records were created.

4.2 Format of Retention

Retention is to be made by way of original documents, microfilm, or in computerized form.



Chapter Five: Monitoring and Reporting Suspicious Transactions

5.1 Recognition

Staff should always be on the alert of suspicious transactions which usually are inconsistent with a customer's known, legitimate business or personal account activities or with the normal business for that type of account.

We should know enough about the customer's business to recognize that a transaction, or a series of transactions, is unusual. If the handling staff, especially when handling unusual or substantial transaction, is not familiar with the customer, he should refer to the supervisor or the Manager of the Department/Branch (where the account was opened) for more information and guidance.

5.2 Transaction Monitoring

Staff should always be on the alert of the following types of **CASH** transactions at the equivalent amount of HKD100,000.00 or above except for deposit into an account where the equivalent amount is set at HKD200,000.00 or above:

- Deposit;
- Purchase of foreign currency bank notes;
- Purchase of travellers cheques;
- Deposit to credit card account; and
- Payment of insurance premium.

Transactions can be monitored by reviewing the "**Customer Daily Aggregate Cash/Transfer Deposit Exceed Limit Report**". However, staff and managers are required to watch for transactions which are below the threshold of exception reports but with a pattern that is out of normal characteristics of the account nature.

When Department/Branch managers are reviewing the reports, the "**reasonableness of transaction profile based on the business nature / income of customer and / or know your customer principle**" should be taken into careful consideration. Symptoms of likely "launder" transactions must be considered. Suspicion should immediately be



reported to the responsible Departmental General Manager and Compliance Officer.

The reports should be kept in chronological order for 3 years for periodic review by Internal Audit Department and the Compliance Officer.

5.3 Report Obligation

A staff member who suspects or has reasonable grounds to believe that a customer is associated with money laundering or terrorist activities must promptly file a proposal for investigation to his Department/Branch manager who should issue his comments for subsequent decision of the responsible Departmental General Manager who, together with his own opinion, will submit the proposal to the Compliance Officer.

The Compliance Officer will evaluate whether there are reasonable grounds for such belief and will then promptly report the case to the President Office for ultimate report to the Office of Financial Intelligence (GIF) unless he considers, and records his opinion, that such reasonable grounds do not exist.

Whether the case has or has not been reported to the Office of Financial Intelligence (GIF), a copy of the proposal, together with copies of all documents purporting to be related to the case, should be filed with the Compliance Officer who must communicate to the staff member, by whom the investigation is requested, the final outcome of his proposal.

In case a staff member deems necessary that a suspicious case be reported directly to the Compliance Officer, he may submit his proposal to the latter without having first to obtain the consent of his superior and if a staff member has sufficient grounds to believe that a suspicious case must be revealed to the Office of Financial Intelligence (GIF) for further investigation, he may so state in his proposal and the Compliance Officer can not deny his request despite apparent disparity of opinion. If a decision has been made by any staff member who includes but is not limited to the Compliance Officer that a suspicious case be unveiled to the Office of Financial Intelligence (GIF), the relevant case must be communicated thereto within two working days as specified by Article 7 of the Administrative Regulation No. 7/2006. Nevertheless, the name of the staff that reports a suspicious case should by no means be disclosed unless the court so orders.



大豐銀行
BANCO TAI FUNG

5.4 Non-disclosure Obligation

All shareholders, directors and staff member must not disclose, alert or give hints to any third party, either wittingly or inadvertently, that a customer is connected with suspicious transactions pursuant to Paragraph 4 of Article 7 of Law No. 2/2006 and staff member must exercise extreme caution in follow-up requests of information from customers that are being suspected or under investigation.



大豐銀行
BANCO TAI FUNG

Chapter Six: Training

6.1 Seminar

Anti-money laundering and combating financing of terrorism concepts are incorporated in training courses for different levels of staff. Refresher courses on prevention of money laundering and financing of terrorism will be conducted on a need basis. Compliance Officer should arrange the relevant staff to attend external training courses on this issue. Proper register of attendance should be maintained.

6.2 Reader Induction and Reinforcement

New recruits have to read all guidelines on prevention of money laundering and combating financing of terrorism issued by AMCM as well as all internal manual, guidelines and circulars on this subject during the orientation period. Annually, the Department/Branch manager should circulate the Corporate Compliance Manual to the staff for refresher study. The Human Resources Department should also annually arrange the staff to attend internal refresher courses on prevention of money laundering and combating financing of terrorism.



大豐銀行
BANCO TAI FUNG

Chapter Seven: Amendments and publications

The material of this manual may from time to time be amended subjected to governing laws or internal reinforcement of guidelines. The amendments shall be submitted to the President Office for approval and shall be published internally as well as publicly posted onto our websites.

END