“Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures”

Financial Supervisory Commission dated August 30, 2013
Jin-Guan-Yin-Fa-Zi No. 10200247510 Letter approval for recordation
Financial Supervisory Commission dated June 24, 2014
Jin-Guan-Yin-Fa-Zi No.10300160160 Letter approval for recordation
Financial Supervisory Commission dated May 11, 2015
Jin-Guan-Yin-Fa-Zi No. 10400092790 Letter approval for recordation
Financial Supervisory Commission dated February 19, 2016
Jin-Guan-Yin-Fa-Zi No.10500029440 Letter approval for recordation
Financial Supervisory Commission dated June 28, 2017
Jin-Guan-Yin-Fa-Zi No. 10610003210 Letter approval for recordation
Financial Supervisory Commission dated April 23, 2019
Jin-Guan-Yin-Fa-Zi No. 10801049540 Letter approval for recordation

Article 1

The Model Guidelines for Banks’ Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures (“Model Guidelines”) is established in accordance with the “Money Laundering Control Act”, “Counter-Terrorism Financing Act”, “Regulations Governing Anti-Money Laundering of Financial Institutions”, “Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated by the Financial Supervisory Commission” and “Regulations Governing Reporting on the Properties or Property Interests and Locations of Designated Sanctioned Individuals or Entities by Financial Institutions”.

Article 2

A bank’s internal control system for anti-money laundering and counter terrorism financing established in accordance with Article 6 of “Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated by the Financial Supervisory Commission”

should be approved by the board of directors, and the same should be applied to amendments thereof. Its contents should include the following:

I. Policies and procedures for identifying, assessing, and managing the risk of money laundering and terrorism financing ("ML/TF") established in accordance with the "Guidelines for Banks Regarding Assessment of Money Laundering and Terrorism Financing Risks and Adoption of Prevention Programs" ("Guidelines"-Annex).

II. Anti-money laundering and counter terrorism financing ("AML/CFT") programs established in accordance with the Guidelines and based on risk assessment result and scale of business to manage and mitigate the risks identified and take enhanced control measures with respect to higher risk categories.

III. Procedures for supervising the compliance of AML/CFT regulations and the implementation of AML/CFT programs. Such procedures, subject to self-inspection and internal audit, should be enhanced if necessary.

The identification, assessment and management of ML/TF risks provided in subparagraph I of last paragraph should at least cover the aspect of customers, geographic areas, and products, services, transactions or delivery channels, etc. In addition, a bank should comply with following rules:

I. Generating a risk assessment report.

II. Considering all risk factors to determine the bank's level of risk and the appropriate measures to mitigate risks.

III. Having a mechanism in place for updating risk assessment report periodically to ensure the update of risk profile.

IV. Filing the risk assessment report to Financial Supervisory Commission ("FSC") after it is completed or updated.

The AML/CFT programs provided in Subparagraph II of Paragraph 1 shall include following policies, procedures and controls:

I. Customer due diligence (“CDD”).

II. Name screening on customers and related parties of a transaction.

III. Ongoing monitoring of accounts and transactions.

IV. Correspondent banking.

V. Record-keeping.

VI. Reporting of currency transactions that reach a certain amount.

VII. Reporting of transactions suspected to involve money laundering or terrorism financing (“suspicious ML/TF transactions”) and reporting in accordance with “Counter-Terrorism Financing Act”.

VIII. Appointment of an AML/CFT responsible officer.

IX. Procedures for screening and hiring employees.

X. An ongoing employee training program.

XI. An independent audit function to test the effectiveness of AML/CFT system.

XII. Others required in AML/CFT related regulations or by FSC.

A bank that has any branch (or subsidiary) should establish group-level AML/CFT programs and implement such programs in all branches and subsidiaries. In addition to the policies, procedures and controls provided in preceding paragraph, on condition that the laws and regulatory requirements on data confidentiality of R.O.C. and jurisdictions where the bank has any foreign branch (or subsidiary) are met, such programs should include:

I. Policies and procedures for sharing information within the group required for the purposes of CDD and ML/TF risk management.

II. That group-level compliance, audit, and AML/CFT functions may be provided with customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. In addition, it should also include information and analysis conducted for abnormal transactions or activities. When it is considered necessary,

branches (or subsidiaries) may be provided with the aforementioned information through the group management functions.

III. Safeguards on the confidentiality and use of information exchanged, including security protection against information disclosure.

A bank should ensure its foreign branches (or subsidiaries) implement the AML/CFT measures of head office (or parent company) on condition that local regulatory requirements are met. In the case that regulatory requirements of the jurisdictions where head office (or parent company) and a branch (or subsidiary) are located differently, the branch (or subsidiary) should comply with the stricter ones. If there are any doubts in determining whether regulatory requirements are stricter or less strict, a bank should follow the determination of competent authorities in the jurisdiction where the bank's head office (or parent company) is located. If a bank's branch (or subsidiary) is not allowed to implement the measures of head office (or parent company) due to conflicting with foreign regulatory requirements, the bank should apply appropriate additional measures to manage ML/TF risks and inform FSC.

For any branch or subsidiary of a foreign financial group in Taiwan, with respect to the policies and procedures for identifying, assessing and managing ML/TF risks and the policies, procedures, and controls that AML/CFT programs should include, provided in subparagraph I and II of paragraph 1 and established in accordance with the Guidelines, if the group has established ones that are not less strict than and do not conflict with domestic regulatory requirements, such branch or subsidiary may apply the group's requirements.

The board of directors of a bank takes the ultimate responsibility for ensuring the establishment and maintenance of appropriate and effective AML/CFT internal controls. The board of directors and senior management should understand the bank's ML/TF risks and the implementation of AML/CFT programs, and take measures to form a strong AML/CFT culture.

Article 3

The terms used in the Model Guidelines are defined as follows:

I. "A certain amount" refers to TWD 500,000 (or equivalent foreign currency).

II. "Currency transaction" refers to receiving cash or paying cash in a single transaction (including any transaction that is recorded on a cash deposit or withdrawal slip for accounting purpose), or exchanging notes.

III. "Establishing business relationship" means that a person requests a bank to provide financial services and establish relationship that can continue for a duration, or that a person first approaches a bank as a potential customer and expects such relationship that may continue for a duration.

IV. "Customer" refers to a person that establishes business relationship with a bank (including a natural person, a legal person, an entity other than a legal person, or a trust) or a person with whom a transaction is carried out by a bank. This generally excludes the third parties of a transaction. For example, an ordering bank in an outward remittance transaction does not treat the receiver as its customer.

V. "Occasional transaction" refers to a transaction between a bank and a person that has no business relationship with the bank, including cash remittance, exchange of notes etc.

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

VII. "Risk-based approach" refers to that a bank should identify, assess and understand the ML/TF risks that it is exposed to and take appropriate AML/CFT measures to effectively mitigate such risks. With such approach,

a bank should take enhanced measures for higher risk scenarios while simplified measures may be taken for lower risk scenarios to effectively allocate resources and mitigate the identified ML/TF risks in the most appropriate and effective way.

VIII. "Related parties of a transaction" refer to any third party, which is other than a bank's customers, involved in a transaction, such as the receiver of an outward remittance, or the sender of an inward remittance, etc.

Article 4

A bank should comply with following requirements when conducting CDD measures:

I. A bank should avoid establishing business relationship or processing transactions if any of following scenarios is identified:

(I) A customers is suspected to use anonymous, fake name, figurehead, fictitious business or entity.

(II) A customer refuses to provide relevant documentations required for the purpose of CDD except that a bank may verify the client's identify using reliable, independent source of information.

(III) In the case that any person acts on behalf of a customer, it is difficult to verify that the person purporting to act on behalf of the customer is so authorized and the identity of that person.

(IV) Using counterfeit or altered identity documents.

(V) Identification documents presented are hard copies, except for the business that permits the use of hard copies or soft copies of identification documents with other alternative measures under applicable regulations.

(VI) A customer provides suspicious or unclear documents, or fails to provide other supportive evidence, or provides documents that are

unable to verify.

(VII) A customer delays the providing of required customer identification documents in an unusual manner.

(VIII) The parties with whom a bank establishes business relationship are designated individuals or entities sanctioned under Counter-Terrorism Financing Act and terrorists or terrorist groups that are identified or investigated. This requirement, however, does not apply to any payment made in accordance with Subparagraphs I to III of Paragraph 1 of Article 6 of "Counter-Terrorism Financing Act".

(IX) Other unusual scenarios occur when a bank establishes business relationship with or processes transactions for a customer and the customer fails to provide a reasonable explanation.

II. A bank should perform CDD when:

(I) Establishing business relationship with a customer.

(II) Carrying out any of following occasional transactions:

1. Transactions (including domestic remittance) above a certain amount, including situations where the transaction is carried out in several operations that appear to be linked.
2. Cross-border wire transfers above TWD 30,000 (or equivalent foreign currency).

(III) Identifying a suspicious ML/TF transaction.

(IV) It has doubts about the veracity and adequacy of previously obtained customer identification data.

III. A bank should take CDD measures as follows:

(I) Identifying the customer and verifying the customer identity using reliable, independent source documents, data or information, and retaining hard copies of customer identity documents or recording the relevant information thereon.

(II) In the case that any person acts on behalf of a customer to establish business relationship or conduct transactions, a bank should verify that the person purporting to act on behalf of the customer is so authorized. In addition, identify and verify the identity of that person in accordance with Subparagraph III.(i), and retain hard copies of the agent's identity documents or record the relevant information thereon.

(III) Identifying the beneficial owner and take reasonable measures, including using reliable source data or information, to verify the identity of the beneficial owner.

(IV) CDD measures should include understanding and, as appropriate, obtaining information on, the purpose and intended nature of the business relationship.

IV. For an individual customer, a bank should obtain at least following information to identify the customer identity when applying the requirements under last subparagraph:

(I) Name;

(II) Date of birth;

(III) Permanent or residence address;

(IV) Official identification number;

(V) Nationality; and

(VI) The purpose of residence or transaction of a foreign person (such as tourism, work, etc.).

V. For an individual customer that is identified by a bank as a high-risk customer or a customer that has certain high-risk factors in accordance with the bank's relevant requirements on customer ML/TF risk assessment, the bank should obtain at least any of the following information when establishing business relationship:

(I) Any other names used or alias: such as the name used before marriage

or change of name;

(II) Employer's address, post office box address, e-mail address (if any); or

(III) Landline or mobile telephone numbers.

VI. For a customer that is an entity or trustee of a trust, a bank, when applying the requirements under Subparagraph III, should understand the business nature and obtain at least following information of the customer or the trust (including any legal arrangement similar to a trust) to identify and verify the customer identity:

(I) The name, legal form, and proof of existence of the customer or trust;

(II) The articles of incorporation or similar powers that regulate and bind the entity or trust, except in following circumstances:

1. The entity or trust is one of entities provided in Subparagraph VII.(iii) without any circumstances provided in Subparagraph III.(i) and (ii) of Paragraph 1 of Article 6.
2. The entity customer confirmed has no articles of incorporation or similar powers;

(III) Following information of persons holding the position of senior management (including directors, supervisors, chief executive officer, chief financial officer, authorized representatives, temporary manager, partners, authorized signatories, or any natural person having equivalent aforementioned position, a bank should determine the scope of senior management position by applying a risk-based approach) in an entity or trustee of a trust:

1. Name;
2. Date of birth;
3. Nationality; and

(IV) Official identification number: such as identification number, tax

identification number, registration number;

(V) Registered address and main business addresses of an entity or trustee of a trust; and

(VI) The purpose of the business relationship of an offshore entity or trustee of a trust.

VII. For a customer that is an entity or trustee of a trust, a bank, when applying the requirements under subparagraph III.(iii), should understand the ownership and control structure of the customer, and identify the beneficial owners of the customer and take reasonable measures to verify the identity of such persons through following information:

(I) For a customer that is an entity:

1. The identity of the natural person(s) who ultimately has a controlling ownership interest in an entity (such as name, date of birth, nationality, and identification number, etc.). “Natural person(s) who ultimately have a controlling ownership interest in an entity” refers to any natural person that directly or indirectly owns more than 25 percent of shares or capital of the entity. In such case, a bank may request the customer to provide a shareholder register or other documents to support the identification of such person(s).
2. If no natural person is identified under Subparagraph VII.(i)1. or there is doubt as to whether the person(s) with the controlling ownership interest is the beneficial owner(s), the bank should identify the natural person(s) exercising control of the customer through other means. If necessary, a bank may obtain a certification from the customer to identify the beneficial owner(s).
3. If no natural person is identified under Subparagraph VII.(i)1. or VII. (i)1. above, a bank should identify the persons holding the position of senior management.

(II) For a customer that is a trustee of a trust: a bank should identify the settlor, the trustee, the protector, the beneficiaries, and any other natural person exercising ultimate effective control over the trust, or the persons in equivalent or similar positions.

(III) The requirements under Subparagraph III(iii) do not apply to a customer or a person having control over the customer that is one of the following entities, unless the customer or the person meets the description provided in Subparagraph III(i) or Subparagraph III(ii) or has issued bearer shares:

1. R.O.C government;
2. R.O.C. government-owned enterprise;
3. Foreign government;
4. Domestic public company or its subsidiaries;
5. Company listed in other jurisdiction where it is required to disclose majority shareholders, and the subsidiaries of such company;
6. Financial institution supervised by R.O.C. government, and investment vehicle managed by such financial institution;
7. Financial institution incorporated or established in other jurisdiction where it is subject to regulatory requirements that are consistent with FATF AML/CFT standard, and investment vehicle managed by such financial institution. A bank should retain relevant documentation (such as record of public information search, AML policies and procedures of the financial institution, record of negative news search, certification of the financial institution, etc.) with respect to such financial institution and investment vehicle.
8. Certain funds managed by R.O.C. government; or
9. Employee stock ownership trust, or employee savings ownership trust.

VIII. For a customer with whom a bank establishes business relationship, the

bank should take following measures to verify the identity of the customer, the person acting on behalf of the customer, and the beneficiary owners of the customers:

(I) Verification through documents:

1. Individual:

(1) Verification of identity or date of birth: obtain an unexpired official identification document that bears a photograph of the individual (e.g. identification card, passport, residence card, driving license, etc.). If there is doubt as to the validity of such documents, a bank should obtain certification provided by an embassy official or a public notary. With respect to the identity or date of birth of the beneficial owners of an entity, a bank may not obtain original copies of the aforementioned document for verification, or may, according to the bank's internal operating procedures, request the entity and its authorized representative to provide a certification that specifies the identification data of the beneficiary owners. Part of the data on such certification, however, should allow a bank to perform verification through the certificate of incorporation, annual report, or other reliable source documents or data.

(2) Verification of address: obtain bills, account statements, or official documents, etc. from the individual.

2. Entity or trustee of a trust: obtain certified articles of incorporation, government-issued business license, partnership agreement, trust instrument, Certification of Good Standing, etc. If a trust is managed by a financial institution described in paragraph 1 of Article 5 of Money Laundering Control Act, a certification issued by the financial institution may substitute for the trust instrument of the trust unless the jurisdiction where the financial institution is located is one of

jurisdictions described in subparagraph III of paragraph 1 of Article 6.

(II) Verification through nondocumentary methods (if necessary), for example:

1、Contacting the customer by telephone or letter after an account has been opened.

2、Checking references provided by other financial institutions.

3、Cross-checking information provided by the customer with other reliable public information or private database, etc.

IX. For a customer identified by a bank as a high-risk customer or a customer that has certain high-risk factors in accordance with the bank's relevant requirements on customer ML/TF risk assessment, the bank should perform enhanced verification, for example:

(I) Obtaining a reply, signed by the customer or the authorized signatory of the entity, for a letter mailed to the address provided by the customer, or contacting the customer by telephone.

(II) Obtaining evidence that supports an individual's sources of wealth and sources of funds.

(III) Obtaining evidence that supports the sources of funds and destinations of funds of an entity or trustee of a trust, such as a list of main suppliers, a list of main customers, etc.

(IV) Site visits.

(V) Obtaining prior bank reference and contacting with the bank regarding the customer.

X. A bank is not allowed to establish business relationship or conducting occasional transaction with a customer before completing CDD. If following requirements are met, however, a bank may complete verification after the establishment of the business relationship following the obtaining of identification data of the customer and beneficial owner:

(I) The ML/TF risks are effectively managed. This includes the bank should take risk control measures with respect to the scenario that a customer may take advantage of verifying identity after transaction completed;

(II) This is essential not to interrupt the normal conduct of business with customers; and

(III) The bank ensures verification of the identity of the customer and beneficial owner is carried out as soon as it is reasonably practicable. If the bank fails to complete the verification of identity of the customer and beneficial owner in a reasonably practicable timeframe, it should terminate the business relationship with the customer and inform the customer in advance.

XI. If a bank permits the establishment of the business relationship with a customer before completing customer identity verification, the bank should adopt relevant risk control measures, including:

(I) Establishing a timeframe for the completion of customer identity verification.

(II) Before the completion of customer identity verification, business unit supervisory officer should periodically review the business relationship with the customer and periodically keep senior management informed of the progress of customer identity verification.

(III) Limiting the number of transactions and types of transaction before the completion of customer identity verification.

(IV) Keeping the customer from making payment to any third party unless following requirements are met:

1. There is no suspicion of ML/TF;
2. The customer is assessed as a low ML/TF risk customer;

3. The transaction is approved by senior management, whose level is determined on the basis of the bank's internal consideration for risk; and
4. The names of recipients do not match with lists established for AML/CFT purposes.

(V) If there is any doubt as to the authenticity, appropriateness or intention of the customer or beneficial owner, the exception provided in Subparagraph XI.(iv) does not apply.

(VI) A bank should determine the "reasonably practicable timeframe" provided in subparagraph X.(iii) based on a risk-based approach to the extent that timeframes are differentiated according to risk level. For example:

1. The bank should complete customer identity verification no later than 30 working days after the establishment of business relationship.
2. If customer identity verification remains uncompleted 30 days after the establishment of business relationship, the bank should suspend business relationship with the customer and refrain from carrying out further transactions (except to return funds to their sources, to the extent that this is possible).
3. If customer identity verification remains uncompleted 120 days, the bank should terminate business relationship with the customer.

XII. For a customer that is a legal person, a bank should understand whether the customer is able to issue bearer shares by reviewing the article of incorporation or requesting a certification from the customer, and take one of the following measures to ensure the update of beneficial owners:

(I) Requesting the customer to require bearer share holders who ultimately have a controlling ownership interest to notify the customer to record their identity, and requesting the customer to notify the bank

immediately when the identity of such share holder changes.

(II) Requesting the customer, after each shareholders' meeting, to update the information of beneficial owners and provide identification data of any shareholder that holds a certain percentage (or above) of bearer shares. The customer should notify the bank immediately if, through other means, it is aware of the identity of any shareholder who ultimately has a controlling ownership interest changes.

XIII. When conducting CDD, a bank should utilize an appropriate risk management mechanism to determine whether the customer, its beneficial owners or persons holding senior management position in the customer are or were politically exposed persons ("PEPs") entrusted by a domestic or foreign government or international organization.

(I) If the customer and its beneficial owners are PEPs entrusted by a foreign government, the bank should treat such customer as a high-risk customer and take enhanced due diligence ("EDD") measures provided in Subparagraph (i) of paragraph I of Article 6.

(II) If the customer and its beneficial owners are PEPs entrusted by a domestic government or international organization, the bank should perform risk assessment when establishing business relationship with the customer and re-perform in every subsequent year. For a customer treated by the bank as a high-risk customer, the bank should take EDD measures provided in Subparagraph (i) of Paragraph I of Article 6.

(III) If the persons holding senior management position in the customer are PEPs entrusted by a domestic or foreign government or international organization, the bank should take into account the influence that such person exerts on the customer, to determine whether the customer is subject to EDD measures provided in Subparagraph (i) of Paragraph I of Article 6.

(IV) For PEPs that had been entrusted by a domestic or foreign government or international organization, the bank should take into account relevant risk factors to assess their influence, and determine whether they are subject to the requirements under (i) to (iii) above by applying a risk-based approach.

(V) The requirements under (i) to (iv) above also apply to family members and close associates of PEPs. The scope of aforementioned family members and close associates should be determined in accordance with the regulations established under Paragraph 4 of Article 7 of Money Laundering Control Act.

(VI) The requirements under (i) to (v) do not apply to the beneficial owners of or persons holding senior management positions in the entities described in Subparagraph (iii) 1 to 3 and 8.

XIV. Other requirements that a bank should comply with when conducting CDD:

(I) When the bank establishes a business relationship with a customer, conducts financial transaction above a certain amount with an occasional customer, or suspects the identification data of a customer is insufficient for CDD purpose, the bank should perform CDD through government-issued or other documents and keep records.

(II) The bank should perform EDD measures with respect to an account opened by, or a transaction processed by a professional intermediary on behalf of a customer.

(III) The bank should perform EDD measures with respect to a private banking customer.

(IV) The bank should perform EDD measures with respect to a customer rejected by other bank.

(V) For a non-face-to-face customer, the bank should perform CDD procedures that are as effective as those performed in the ordinary

course of business and must include special and sufficient measures to mitigate the risks.

(VI) For a customer establishing business relationship with the bank through internet, the bank should comply with relevant operating Model Guidelines developed by the Bankers Association of the Republic of China ("Association") and approved by regulators.

(VII) For a customer that establishes business relationship with the bank through an authorized person, or that is suspected by the bank after the establishment of business relationship, the bank should verify the customer identity by contacting the customer by telephone, letter, or visit.

(VIII) For a customer that establishes business relationship with the bank through letter, after the establishment of business relationship, the bank should mail a registered letter with a return for verification.

(IX) If the bank knows or is required to presume the source of fund of a customer is corruption or abuse of public assets, the bank should not accept, or should terminate, the business relationship with the customer if relevant regulatory requirements are met.

(X) For a customer that fails to complete relevant CDD procedures, the bank should consider reporting a suspicious ML/TF transaction regarding to the customer.

(XI) When the bank suspects certain customers or transactions may be involved in ML/TF and reasonably believe that performing CDD procedures may allow the customer aware of such information, the bank may not implement such procedures and instead report a suspicious ML/TF transaction.

(XII) For other requirements regarding to establishing business relationship, please refer to the bank's internal regulations.

XV. In the cases below where a bank may take following measures to the extent that the contract between the bank and the customer allows:

(I) In the situation described in Subparagraph I.(viii), the bank may decline the request of establishing business relationship or terminate the business relationship.

(II) For a customer that is recalcitrant in CDD, refuses to provide information of beneficial owners an persons holding controlling interest in the customer, etc., or fails to explain the nature, intent, or source of fund of the transactions, etc., the bank may suspend the transactions, or suspend or terminate the business relationship.

XVI. In the case that a customer in a business relationship or transaction is described in Subparagraph I.(viii), a bank should report suspicious ML/TF transaction in accordance with Article 10 of Money Laundering Control Act. If such customer is a designated individual or entity sanctioned under Counter-Terrorism Financing Act, the bank is prohibited from the activities described in Paragraph 1 of Article 7 of Counter-Terrorism Financing Act since the date of knowledge, and should report in accordance with the requirements of Counter-Terrorism Financing Act (please download the reporting format on the website of the Investigation Bureau, Ministry of Justice). If the bank is involved in the activities described in the Subparagraphs 2 and 3 of Paragraph 1 of Article 6 of Counter-Terrorism Financing Act before aforementioned individuals or entities are listed as designated individuals or entities, the bank should obtain the approval of the Ministry of Justice in accordance with the Counter-Terrorism Financing Act.

Article 5

The CDD measures conducted by a bank should include following requirements

in ongoing due diligence on customer identity:

I. The bank should scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the bank's knowledge of the customer, their business and risk profile, including where necessary, the source of funds.

II. The bank should periodically review the sufficiency of the information used to identify customer and beneficial owners and ensure the update of such information. High-risk customers, especially, should be subject to at least annual review. For other customers, the bank should determine the frequency of review by applying a risk-based approach.

III. When conducting CDD measures, a bank may rely on the customer identification data previously obtained and kept, and is not required to conduct such measures each time when the customer processes a transaction. If the bank has doubts about the veracity and adequacy of previously obtained customer identification data, identifies a suspicious ML/TF transaction, or there is material change in the transaction or account activities of the customer that is inconsistent with its business profile, the bank should re-conduct CDD measures in accordance with the requirements of Article 4.

Article 6

For the measured adopted to confirm customer identity and the continuing review mechanism stated in Article 4, Paragraph 3 and in the preceding paragraph, the intensity of review shall be determined in accordance with the risk-based approach, including:

I. For higher risk situations, the bank should take enhanced CDD and ongoing due diligence measures, which at least include following additional enhanced measures:

(I) Before establishing or adding new business relationship, the bank

should obtain the approval of certain level senior management, determined according to the bank's internal consideration of risk.

(II) The bank should take reasonable measures to understand the source of wealth and source of funds of the customer. The source of funds refer to the original source that generates such funds (e.g. salary, investment proceeds, disposal of real estate, etc.).

(III) Conducting enhanced ongoing monitoring of the business relationship.

II. For customers from high ML/TF risk jurisdictions, the bank should apply enhanced measures proportionate to the risks.

III. For lower risk situations, the bank may take simplified measures commensurate with the lower risk factors. Simplified measures, however, should not be permitted in one of the following situations:

(I) Customers are high ML/TF risk jurisdictions, which include but are not limited to the jurisdictions, published by international anti-money laundering organizations and notified by FSC, that have serious deficiencies in AML/CFT, and other jurisdictions that fail to comply with or completely comply with the recommendations of such organizations.

(II) The bank has sufficient reason to suspect the customers or transactions may be involved in ML/TF.

A bank may take following simplified due diligence measures:

I. Lower the frequency of updating customer identification data.

II. Lower the extent to which the bank conducts ongoing monitoring, and review transactions that reach a reasonable amount.

III. The bank is not required to collect specific information or take special measures to understand the purpose and the nature of the business relationship if these can be inferred from the transaction types or existing business relationship.

A bank should apply CDD measures to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account when CDD measures have previously been undertaken and the adequacy and sufficiency of data obtained.

Article 7

A bank should perform CDD measures by itself. If regulatory requirements or FSC otherwise permits the bank may reply on third-parties to identify and verify the identity of customers, the person on behalf of the customer, or beneficial owners of the customer, or the purpose or nature of business relationship, the ultimate responsibility for CDD measures remain with the bank relying on the third party, which should be required to:

I. Obtain immediately the necessary information concerning CDD measures
II. Take measures to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay.
III. Satisfy itself that the third party is regulated, and supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements.
IV. Satisfy itself that the jurisdiction where the third party is located has AML/CFT regulatory requirements consistent with FATF standard.

Article 8

A bank's mechanism for name screening on customers and related parties of a transaction should be conducted as follows:

I. The bank should establish policies and procedures for name screening on customers and related parties of a transaction, by applying a risk-based approach, to detect, match, and filter whether customers, persons holding

senior management position of a customer, beneficial owners of a customer, or related parties of a transaction are designated individuals or entities sanctioned under Counter-Terrorism Financing Act, or terrorists or terrorist groups identified or investigated by foreign governments or international organizations. In the case of true hit, the bank should undertake the measures provided in Subparagraph XVI of Article 4.

II. The policies and procedures for name screening on customers and related parties of a transaction should include at least the logic of matching and filtering, the operating procedure for name screening, and the standard of review, and should be documented.

III. The bank should record the result of name screening, and keep such record in accordance with the requirements of Article 15.

IV. The name screening mechanism should be subject to testing, including:

(I) Whether the sanction list and threshold setting are determined by applying a risk-based approach.

(II) Whether the mapping between data input and system data field is correct and complete.

(III) The logic of matching and filtering.

(IV) Model validation.

(V) Whether data output is correct and complete.

V. The bank should determine whether such mechanism continues to appropriately reflect the risk identified and update the mechanism at proper time.

Article 9

A bank’s ongoing monitoring of accounts and transactions should be conducted as follows:

I. The bank should integrate customer information data and transaction data throughout the company step-by-step by information systems for enquiries

processed by the head office or branch for the purpose of AML/CFT, in order to enhance its capacity of account and transaction monitoring. With respect to the customer data requested or enquired by each business unit, the bank should establish an internal control procedure and ensure the confidentiality of the data.

II. The bank should establish policies and procedures for ongoing monitoring of accounts and transactions by applying a risk-based approach and use information systems to assist the identification of suspicious ML/TF transactions.

III. The bank should review its policies and procedures for ongoing monitoring of accounts and transactions and update periodically to take into account regulatory requirements on AML/CFT, customer profiles, the size and complexity of business, the trend and information related to ML/TF obtained from internal or external sources, the result of internal risk assessment, etc.

IV. Policies and procedures for ongoing monitoring of accounts and transactions should include at least complete and documented monitoring types, parameters, thresholds, operating procedures for the conducting and monitoring of alerts, procedures for reviewing monitoring cases, and the standard of reporting.

V. The mechanism provided in last subparagraph should be subject to testing, including:

(I) Internal control procedure: review the roles and responsibilities of persons or business units related to the mechanism for monitoring accounts and transactions.

(II) Whether the mapping between data input and system data field is correct and complete.

(III) The logic of detection scenario.

(IV) Model validation.

(V) Data input.

VI. In the cases where the bank identifies or has reasonable grounds to suspect customers, or the funds, assets or intended or performed transactions of the customers are related to ML/TF, regardless of the amount, value, or whether transactions are completed, the bank should perform enhanced review of the customer identity.

VII. The red flags for transactions suspected to involve money laundering or terrorism financing provided in the Annex are not exhaustive. The bank should select or develop suitable red flags based on its size of assets, geographic areas, business profile, customer base profile, characteristics of transactions, and the bank's internal ML/TF risk assessment or information of daily transactions, to identify red flag transactions of potential ML/TF.

VIII. For red flag transactions identified in accordance with last subparagraph, the bank should determine whether such transactions are reasonable (e.g. whether such transactions are apparently incommensurate with the identity, income, or scale of business of the customer, unrelated to the customer's business profile, do not match the customer's business model, no reasonable economic purpose, no reasonable explanation, no reasonable purpose, or unclear source of funds or explanation), the bank shall complete the review process as quickly as possible to determine whether the transaction is suspected of involving ML/TF activity, and keep review records. If the bank examines and determines such transaction is not a suspicious ML/TF transaction, the bank should record the reason for the decision. If the bank examines and determines such transaction is a suspicious ML/TF transaction, regardless of the amount of the transaction, the bank shall promptly file a report with the Investigation Bureau in a format prescribed by the Bureau after the report has been approved by the responsible chief compliance officer at the bank. The same process shall apply to attempted

transactions.

IX. With respect to red flags for transactions suspected to involve money laundering or terrorism financing, the bank should determine the ones that are required to be monitored with the assistance of related information systems by applying a risk-based approach. For those that are monitored without the assistance of information systems, the bank should also, by other means, assist employees to determine whether transactions are suspicious ML/TF transactions when they are processed by customers. The assistance of information system cannot replace the judgment of employees. The bank is still required to strengthen employee training to allow employees capable of identifying suspicious ML/TF transactions.

Reporting of suspicious ML/TF transactions:

I. When an employee of a business unit identifies any abnormal transaction, the employee should immediately report such transaction to a supervisory officer.

II. The supervisory officer should determine as soon as possible whether such transaction is subject to reporting requirements. If it is determined that such transaction should be reported, the supervisory officer should immediate request the employee complete a report (please download the reporting format on the website of the Investigation of Bureau, Ministry of Justice).

III. The bank should submit the approved report to the responsible unit.

IV. After the report is submitted by the responsible unit and approved by AML/CFT Responsible Officer, the bank should file the report immediately to the Investigation of Bureau, Ministry of Justice.

V. In the case of an apparently significant and urgent suspicious ML/TF transaction, the bank should immediately report to the Investigation of Bureau, Ministry of Justice by fax or other feasible means and then immediately submit the hard copy of the report. The bank is not required

to submit the hard copy of the report, provided that the Investigation of Bureau, Ministry of Justice confirms the receipt of such report by sending a fax reply (please download the format on the website of the Investigation of Bureau, Ministry of Justice. In addition, the bank should retain the fax reply.

Requirements on the confidentiality of reporting data and information are as follows:

I. Employee at all levels should keep the reporting of suspicious ML/TF transactions confidential and should not disclose such information. A bank should provide employees trainings or materials on how to avoid the disclosure of such information in the interaction with customers and in daily operation.

II. All documents related to such reporting should be classified as confidential. In the cases of any disclosure, a bank should take measures in accordance with relevant requirements.

III. AML responsible unit, compliance officers or internal auditors should be able to timely obtain customer identification data and transaction record to the extent that requirements on confidentiality are met.

A bank should record the result of monitoring of accounts or transactions and keep such record in accordance with the requirements of Article 15.

Article 10

Regarding filing of a report of the property or property interests of a designated individual, legal person or entity and the place thereof in accordance with Article 7 of the Counter-Terrorism Financing Act, the bank shall comply with the following provisions:

I. After learning of the case, the unit-in-charge at the head office shall submit the report for approval by the appointed chief compliance officer

mentioned in the preceding article, and then promptly file the report with the Investigation Bureau, Ministry of Justice (referred to as "MJIB") in the format and manner prescribed by the MJIB. The report shall be filed within two business days following the date of approval.

II. In the event of an apparent significant and urgent case, the bank should a report to the MJIB as soon as possible by fax or other available means and submit a make-up report in a format (please download from the format from the website of MJIB) and manner prescribed by the MJIB subsequently. However, a make-up report is not required if the MJIB has confirmed the receipt of report by sending a reply in a prescribed format by fax. The bank should maintain the faxed reply from the MJIB.

III. The bank shall produce an annual report as of December 31 (the "settlement record date") in a format (please download the format from the website of MJIB) specified by MJIB. The report shall state all properties or property interests of designated sanctioned individuals, legal entities or groups managed or held by the financial institution as of the settlement record date and the report shall be submitted to the MJIB for reference before March 31 of the following year.

The reporting records, transaction documents and annual reports mentioned in the preceding paragraph shall be maintained in their original forms for five years.

Article 11

A bank should establish certain policies and procedures with respect to cross-border correspondent banking or similar business, and the content thereof shall at least include the following:

I. Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a ML/TF investigation

or regulatory action.

II. Assess whether the respondent institution has appropriate control policies in place in AML/CFT and the effectiveness of such policies.

III. Before establishing cross-border correspondent relationship with the respondent institution, the bank should obtain approval from certain level senior management, determined according to the bank's internal consideration of risk.

IV. Document the respective AML/CFT responsibilities of each institution.

V. With respect to "payable-through accounts" involved in cross-border correspondent banking, be satisfied that the respondent institution has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank, if necessary.

VI. The bank is prohibited from establishing correspondent banking relationship with shell banks or respondent institutions that permit their account to be used by shell banks.

VII. For a respondent institution that fails to provide the aforementioned information requested by the bank, the bank may decline to open an account, suspend transactions, report suspicious ML/TF transactions, or terminate the business relationship.

VIII. In the case that the respondent institution is the bank's foreign branch (or subsidiary), aforementioned requirements of this Article also apply.

Article 12

Prior to the launch of new products or new business practices (including new delivery mechanism, the use of new technologies for pre-existing or new products or businesses), a bank should perform ML/TF risk assessment for such products or business practices and take measures to manage and mitigate the

risks identified.

Article 13

A bank should comply with following requirements on remittance:

I. The bank should comply with the requirements of “Directions Governing Banking Enterprises for Operating Foreign Exchange Business” to conduct the domestic and cross-border foreign exchange outward and inward remittance.

II. An ordering bank should comply with following requirements on domestic New Taiwan Dollar remittance:

(I) Provide required and accurate originator information and required beneficiary information by any of the means below:

1. Providing the information of the originator and the beneficiary with the remittance transaction.

2. Providing the account number of the originator and the beneficiary or a transaction reference number which permits traceability of the transaction with the remittance transaction, and providing the information of the originator and the beneficiary within 3 business days of receiving a request either from the beneficiary financial institution or from competent authorities. However, in cases where prosecutors office, judicial organ, or police agency and subordinate branch requests the bank to provide such information immediately, the bank should provide accordingly.

3. Where the amount of a single remittance is less than NT$ 30,000, unless it is subject to suspicious ML/TF activities, the originator information may not be required to be confirmed.

(II) Maintain the following required information on the originator and the beneficiary in accordance with Article 12 of the Regulations

Governing Anti-Money Laundering of Financial Institutions:

1. The aforementioned originator information shall include: name of the originator, the originator account number where such an account is used to process the transaction (if not available, a unique transaction reference number that permits traceability), and the information by any of the means below:
   (1) National identity number;
   (2) The originator's address; or
   (3) Date and place of birth.
2. The aforementioned beneficiary information shall include: name of the beneficiary and the beneficiary account number (if not available, a unique transaction reference number that permits traceability).

III. In case where the bank fails to comply with the requirements of last two subparagraphs, it is prohibiting from conducting remittance business.

IV. A beneficiary financial institution shall conduct domestic wire transfers in NTD in accordance with the following rules:

(I) Maintain risk-based policies and procedures for determining when to execute, reject, or suspend a wire transfer lacking the information specified under Subparagraph 2, Paragraph 2 hereof, and conducting the appropriate follow-up action.

(II) Retain the received information of the originator and the beneficiary in accordance with Article 12 of the Regulations Governing Anti-Money Laundering of Financial Institutions.

Article 14

A bank should comply with following requirements on currency transactions above a certain amount:

I. The bank should verify customer identity and retain relevant

documentation.

II. The bank should comply with following requirements on the measures of the verification of customer identity:

(I) Verify customer identity with the identification documents or the passport provided by the customer, and record the name, date of birth, address, telephone number, account number where the account is used to process the transaction, transaction amount, and identification number of the customer. In case where the customer is the owner of the account used to process transactions, however, the bank may not verify the identity but describe the transaction is processed by the account owner on transaction records.

(II) In case where the transaction is processed by a person acting on behalf of the customer, the bank should verify the person's identity with the identification documents or the passport provided by the person, and record the name, date of birth, address, telephone number, account number where the account is used to process transactions, transaction amount, and identification number of the person.

(III) In case where the transaction is an occasional transaction, the bank should verify the customer identity in accordance with the requirements of Subparagraph III of Article 4.

III. Except for the situations described in paragraph 2 and paragraph 3, the bank should report such transactions within 5 business days after the completion of transactions in the way of media reporting (please download the format on the website of the Investigation of Bureau, Ministry of Justice) to the Investigation of Bureau, Ministry of Justice. In case where the bank fails to complete media reporting with a justified reason, it may submit a hard copy of the report after obtaining the approval from the Investigation of Bureau, Ministry of Justice.

IV. The bank should retain the reporting data and relevant documentations submitted to the Investigation of Bureau, Ministry of Justice in accordance with the requirements of Article 15.

The bank is exempt from reporting following currency transactions above a certain amount to the Investigation of Bureau, Ministry of Justice but remains required to verify customer identity and retain relevant documentations:

V. Payments deposited into an account opened by a government, a government-owned enterprise, an entity commissioned to exercise public authority (within the scope of commission), a public or private school, a public utility, and a fund established by a government in accordance with applicable regulatory requirements.

VI. Payments collected or maid for a government treasury by a financial institution acting as its commissioned bank.

VII. Inter-financial institution transactions and funding activities. However, in case where cash payments above a certain amount maid to a customer of another financial institution through an inter-financial institution account, such as cashing a check issued by another financial institution, the bank should remain subject to relevant requirements to conduct such transactions.

VIII. Payments made by a public welfare lottery retailer for the purpose of acquiring lottery for sale.

IX. Payment collected under a collection service (excluding the payments deposited into an account used to collect capital contribution from shareholders, and payments collected for credit card bill), provided that the payment notice clearly specifies the counterparty's name, identification number (including a reference number which permits traceability of the transaction party's identity), type and amount of the transaction. However, the duplicate copy of the payment notice should be retained as an evidence

of the transaction.

For an entity account opened by department stores, wholesale stores, convenience store chains, gas stations, hospitals, clinics, transportation businesses, restaurants, and hotels, etc. which must often or regularly deposit cash above a certain amount based on business needs, the bank may, after verifying such needs, submit a list of such entities to the Investigation Bureau, Ministry of Justice for approval. If the Investigation Bureau, Ministry of Justice provide no comment against the list in 10 days, payments deposited into such account are exempt from verification and reporting on a case-by-case basis. The bank should perform at least annual review of the counterparty. If the counterparty with which the bank no longer has the business relationship described in this paragraph, the bank should report to the Investigation Bureau, Ministry of Justice.

For the transactions described in last two paragraphs, in case where a suspicious ML/TF transaction is identified, the bank should remain subject to the requirements of Article 10 of Money Laundering Control Act and Paragraph 3 of Article 7 of Counter-Terrorism Financing Act.

Article 15

A bank should keep records on customers and transactions with hard copies or electronic data in accordance with following requirements:

I. The bank should maintain, for at least five years, all necessary records on transactions, both domestic and international. However, in case where laws otherwise provide a longer period for record-keeping, the bank should comply with such laws. The aforementioned necessary records include:

(I) The name, or account number or identifier of each party involved in a transaction.

(II) Date of transaction.

(III) Currency and amount of transaction.

(IV) The way funds are deposited or withdrew, such as cash, checks, etc.

(V) Destination of funds.

(VI) Ways to provide instructions or authorities.

II. For currency transactions above a certain amount, the bank should keep relevant records on the verification and reporting of such transactions for at least 5 years in the original manner. For ways to record the information obtained through the CDD procedures, the bank may determine a way to record such information based on its own consideration and the principle of consistency across the entire bank.

III. For the reporting of a suspicious ML/TF transactions, the bank should keep relevant records of reporting for at least 5 years in the original manner.

IV. The bank should keep following information after the business relationship is ended, or after the date of occasional transaction for at least 5 years. However, in case where laws otherwise provide a longer period for record-keeping, the bank should comply with such laws:

(I) All records obtained through the CDD measures, e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents.

(II) Account files.

(III) Business correspondence, including the information of the background or purpose of complex, unusual large transactions obtained from enquiries, and the result of any analysis undertaken.

V. The records kept by the bank should be sufficient to permit reconstruction of individual transactions so as to provide evidence for the determination of criminal activity.

VI. The bank should ensure to rapidly provide transaction records, the CDD information, and relevant information, etc. to competent authorities upon appropriate authority.

Article 16

The bank should deploy adequate and sufficient AML/CFT officers and resources according to its size and risks, etc. The board of directors should appoint a senior officer to serve as AML/CFT responsible officer, who should be sufficiently authorized to coordinate and supervise AML/CFT affairs, and ensure such officers and responsible officer do not take other responsibility which conflicts with their AML/CFT responsibilities. In addition, domestic banks and the institution in charge of postal savings and remittance business should establish an independent AML/CFT responsible unit under chief executive officer, head office compliance unit, or risk management unit. Such unit is prohibited from dealing with affairs other than AML/CFT.

Responsible unit and responsible office described in the preceding paragraph are in charge of following affairs:

I. Supervising the planning and implementation of policies and procedures for identifying, assessing and monitoring ML/TF risks.
II. Coordinating and supervising the implementation of the bank-wide ML/TF risk identification and assessment.
III. Monitoring risks related to ML/TF.
IV. Developing AML/CFT programs.
V. Coordinating and supervising the implementation of AML/CFT programs.
VI. Confirming the compliance with relevant AML/CFT regulatory requirements, including relevant Model Guidelines or self-regulatory rules established by associations of financial services industry and approved by FSC.
VII. Supervising the reporting of suspicious ML/TF transactions and properties or property interests and locations of designated individuals or entities sanctioned under Counter-Terrorism Financing Act to the Investigation

Bureau, Ministry of Justice.

The responsible officer described in Paragraph I should report to the board of directors and supervisors (board of supervisors) or audit committee at least every half year. If any significant non-compliance is identified, responsible officer should immediate report to the board of directors and supervisors (board of supervisors) or audit committee.

A foreign business unit of the bank should deploy adequate and sufficient AML/CFT officers by taking into account the number of local branches, size of business, risks, etc. and appoint a head responsible for supervising AML/CFT affairs.

The appointment of AML/CFT head of the bank's foreign business unit should meet local regulatory regulations and the requirements of local competent authorities. The head should be sufficiently authorized to coordinate AML/CFT affairs, including that the head may directly report to the responsible office described in Paragraph 1, and should not take other responsibilities except compliance head. In case where the head may take other responsibilities, the bank should discuss with local competent authorities to ensure such arrangement has no concern in conflict of interest and report to FSC.

Article 17

A domestic and foreign business unit of a bank should appoint a senior officer to serve as a supervisory officer responsible for supervising the implementation of AML/CFT and the implementation of self-inspection of the business unit.

The internal audit unit of a bank should audit and provide auditor opinion on following matters:

I. Whether ML/TF risk assessment and AML/CFT programs meet regulatory requirements and are implemented.

II. The effectiveness of AML/CFT programs.

Responsibilities of internal audit unit:

I. Determining the matters subject to audit according to internal control measures and relevant regulations, conducting periodic audit, and testing the effectiveness of AML/CFT programs and risk management quality of operations, departments and branches (or subsidiaries).

II. The auditing method should cover independent transaction testing, including selecting transactions related to high-risk products, customers, and geographic areas to verify the bank has effectively implemented relevant AML/CFT regulatory requirements.

III. In case where any deficiency in the implementation of specific management measures is identified, internal audit unit should periodically report to AML/CFT responsible officer for review and provide such information as a reference of employee training.

IV. In case where internal audit unit identifies any intentional disguise of significant non-compliance but fails to disclose such information, head office competent unit should take appropriate actions.

A bank's chief executive officer should supervise each unit to the extent that the implementation of AML/CFT internal control system is assessed and reviewed by each unit in a prudent manner. The chairman, chief executive officer, chief auditor (audit manager), and AML/CFT responsible officer should jointly issue a statement for AML/CFT internal control system and submit to board of directors for approval. Within 3 months after the end of each fiscal year, the bank should disclose the statement on its website and publish the statement through a website designated by FSC.

For a branch of a foreign bank located in Taiwan, the requirements of the Model Guidelines regarding to the board of directors or supervisors may be satisfied by persons authorized by the head office. The statement described in the preceding paragraph may be jointly issued by a representative for litigious and non-

litigious matters, AML/CFT responsible officer, and a senior auditor responsible for Taiwan area, etc.

Article 18

A bank should ensure the establishment of high quality standard procedures for screening and hiring employees, including reviewing whether a candidate has decent personality and professional knowledge required for the job.

A bank's AML/CFT responsible officer, AML/CFT officers, and domestic business unit supervisory officers should meet one of following requirements within 3 months after the appointment. The bank should establish relevant control mechanism to ensure the compliance of such requirements:

I. Having at least 3-year experience as a compliance officer or AML/CFT officer.

II. Attending at least 24-hour training classes provided by an institution recognized by FSC and obtaining a certificate of completion after passing an exam. For a person who has been qualified for a compliance officer, however, may be treated as meeting the qualification requirement provided in this subparagraph after attending 12-hour AML/CFT training classes.

III. Obtaining a domestic or international AML/CFT professional certificate issued by an institution recognized by FSC.

The bank's AML/CFT responsible officer, AML/CFT officers, and domestic business unit supervisory officers should attend at least 12-hour AML/CFT trainings each year provided by the bank or external training institutions agreed by AML/CFT officer described in Paragraph 1 of Article 16. Such trainings should at least cover new updates on regulatory requirements, and ML/TF trends and red flags. Those who obtain domestic or international AML/CFT professional certificates issued by an institution recognized by FSC may be exempt from satisfying the requirements on training hour for the same year.

The bank's foreign business unit supervisory officer and AML/CFT head and officers should have AML expertise, be familiar with local regulatory requirements, and attend 12-hour AML/CFT trainings provided by local competent authorities or relevant institutions. In case where local competent authorities or relevant institutions do not provide AML/CFT trainings, such persons may attend the trainings provided by the bank or external training institutions agreed by AML/CFT responsible officer described in Paragraph 1 of Article 16.

The bank should arrange AML/CFT trainings each year that have appropriate contents and training hours determined according to the nature of business for its directors, supervisors, chief executive officer, compliance officers, internal auditors and salesmen, to allow them to understand their AML/CFT duties and have the expertise required for such duties.

If employees meet one of the following descriptions, the bank should examine the affairs that they are responsible for by sampling and, if necessary, may seek assistance from internal audit unit.

I. Employees have luxury lifestyle that is inconsistent with their salary.
II. Employees has scheduled for leave but do not take the leave without a reason.
III. Employees fail to explain the large amount inflow or outflow in their account.

In case where employees have one of the following contributions to AML/CFT, a bank should reward them appropriately:

I. Employees identify suspicious ML/TF transactions and report such transactions in accordance with relevant AML regulatory requirements to the extent that they contribute to the prevention or investigation of criminal activities.
II. Employees attend domestic or foreign AML/CFT seminars with

outstanding performance, or collect foreign regulatory requirements and provide materials that are valuable to the bank's AML/CFT activities.

A bank may take following measures to conduct orientations and trainings:

I. Orientations: a bank should arrange orientations to include at least certain-hour training classes on AML/CFT regulatory requirements and legal responsibilities of employees of financial services industry to allow new employees to understand relevant regulatory requirements and responsibilities.

II. Training:

(I) Initial trainings on regulatory requirements: after Money Laundering Control Act and Counter-Terrorism Financing Act enter into force or get amended, the bank should conduct trainings on such regulatory requirements for employees within a shortest period to introduce Money Laundering Control Act, Counter-Terrorism Financing Act, and relevant regulatory requirements, and explain the bank's relevant measures in response to those changes. AML/CFT responsible unit should be responsible for planning such trainings and having employee training unit implement the trainings.

(II) Regular training:

1. Each year employee training unit should periodically conduct relevant trainings for employees to learn, in order to strengthen the judgment of employees, implement AML/CFT functions, and prevent employees from non-compliance. Such trainings may be arranged into other professional trainings to include appropriate relevant classes.
2. The trainings may be instructed by employees trained by the bank. In addition, the bank may invite scholars or experts as instructors if necessary.
3. To allow employees to sufficiently understand the characteristics and

types of ML/TF in order to facilitate the identification of "suspicious ML/TF transactions", the trainings should be supplemented by real cases in addition to the introduction of relevant regulatory requirements.

4. AML/CFT responsible unit should periodically understand an employee's attendance in trainings. For an employee who never attends, AML/CFT responsible unit should urge the employee to attend relevant trainings if necessary.
5. In addition to internal trainings, the bank may select employees to attend trainings provided by external training institutions.

III. Lectures for specific topics: in order to enhance employees' understanding of AML/CFT regulatory requirements, the bank may conduct lecturers for specific topics and invite scholars or experts to visit the bank as lecturers.

Article 19

Others that require attention:

I. In case where customers meet one of the following descriptions, a bank's employees should decline their requests in a euphemistic manner and report to direct managers.
   (I) Insisting not to provide relevant data for identity verification when being told it is necessary according to regulatory requirements.
   (II) Any individuals or entities compel or attempt to compel bank employees not leave transaction records or complete reporting form.
   (III) Attempting to persuade employees not to collect data that is required to complete the transaction.
   (IV) Enquiring the possibility of avoiding being reported.
   (V) Eager to explain the source of fund is clean or the transaction is not for money laundering purpose.
   (VI) Insisting transactions must be completed immediately without a

reasonable explanation.

(VII) Descriptions provided by the customers apparently do no match the transactions.

(VIII) Attempting to provide interest to employees to obtain the bank's services.

II. In case where a bank also operates other business, relevant Model Guidelines for such business should apply to the department in charge of the business as well. For example, in case where a bank also operates bills business, Model Guidelines for Bills Finance Companies Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures should apply to the department operating bills business.

Article 20

When the FSC or the entrusted institution conducts audit on a bank in accordance with Article 10 of the "Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated by the Financial Supervisory Commission", the bank shall provide the relevant books, documents, electronic data files or other relevant materials. The aforementioned materials, whether stored in hard copy, electronic file, e-mail or any other form, shall be provided, and the bank shall not circumvent, reject or obstruct the inspection for any reason.

Article 21

The Model Guidelines should be implemented after the approval of the board of directors of the Association and FSC. In the case of amending the Model Guidelines, the requirement of this Article also apply.