Directions Governing Anti-Money Laundering and Countering Terrorism Financing of Banking Sector

1. These Directions are specifically adopted to strengthen the anti-money laundering and countering terrorism financing (AML/CFT) regime of the Republic of China (R.O.C.), and enhance soundness of the internal control and internal audit system of the banking industry in R.O.C.

2. In matters related to AML/CFT, a banking business shall in accordance with the Directions as well as relevant provisions in the "Money Laundering Control Act", "Terrorism Financing Prevention Act", "Regulations Governing Cash Transaction Reports (CTR) and Suspicious Transaction Reports (STR) by Financial Institutions", "Regulations Governing the Deposit Accounts and Suspicious or Unusual Transactions" and "Directions for Confirming Customer Identity in Domestic Remittance Operations of Financial Institutions".

3. The "banking business" referred to in the Directions include banks, credit cooperatives, postal service institutions which also handle the money transactions of deposit, transfer and withdrawal, bills finance companies, credit card companies and trust enterprises.

4. A banking business shall comply with the following provisions in undertaking customer due diligence (CDD) measures:

   (1) A banking business shall not keep anonymous accounts or accounts in fictitious names.

   (2) A banking business shall undertake CDD measures when:

      A. establishing business relations with any customer;

      B. carrying out occasional transactions with respect to:

         (A) cash receipt or payment in a single transaction (including all transactions recorded on cash deposit or withdrawal vouchers for accounting purpose), or the transaction of currency exchange of NTD 500,000 or more (including the foreign currency equivalent thereof); or

         (B) a cross-border wire transfer involving NTD30,000 or more (including the foreign currency equivalent thereof);

      C. there is a suspicion of money laundering or terrorist financing; or

      D. a banking business has doubts about the veracity or adequacy of

previously obtained customer identification data.

(3) The CDD measures to be taken by a banking business are as follows:

A. Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information. In addition, a banking business shall retain copies of the customer's identity documents or record the relevant information thereon.

B. Verifying that any person purporting to act on behalf of the customer is so authorized, identifying and verifying the identity of that person using reliable, independent source documents, data or information where the customer opens an account or conducts a transaction through an agent. In addition, the banking business shall retain copies of the person's identity documents or record the relevant information thereon.

C. Taking reasonable measures to identify and verify the identity of the beneficial owner of a customer.

D. Enquiring information on the purpose and intended nature of the business relationship when undertaking CDD measures.

(4) When the customer is a legal person or a trustee, a banking business shall, in accordance with the preceding Subparagraph, understand the business nature, ownership and control structure of the customer or trust (including trust-like legal arrangements) and obtain at least the following information to identify and verify the identity of the customer or the trust:

A. Name, legal form and proof of existence of customer or trust.

B. The powers that regulate and bind the legal person or trust, as well as the names of the relevant persons having a senior management position in the legal person or trustee

C. The address of the registered office of the legal person or trustee, and the address of its principal place of business.

(5) When the customer is a legal person, a banking business shall understand whether the customer is able to issue bearer shares and adopt appropriate measures for customers who have issued bearer shares to ensure its beneficial owners are kept up-to-date.

(6) When the customer is a legal person or a trustee, a banking business

shall, in accordance with Item C of Subparagraph (3), obtain the following information to identify the beneficial owners of the customer and take reasonable measures to verify the identity of such persons:

A. For legal persons:

(A) The identity of the natural persons who ultimately have a controlling ownership interest in a legal person. A controlling ownership interest refers to owning more than 25 percents of a company's shares or capital;

(B) To the extent that there is doubt under (A) above as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerting control through ownership interests is identified, the identity of the natural persons (if any) exercising control of the customer through other means.

(C) Where no natural person is identified under (A) or (B) above, a banking business shall identify the identity of the relevant natural person who holds the position of senior managing official.

B. For trustees: the identity of the settlor(s), the trustee(s), the trust supervisor, the beneficiaries, and any other person exercising ultimate effective control over the trust, or the identity of persons in equivalent or similar positions.

C. Unless otherwise provided for in the proviso of Subparagraph (2) of Point 7, a banking business is not subject to the aforementioned requirements of identifying and verifying the identity of shareholder or beneficial owner of a customer, provided the customer or a person having a controlling ownership interest in the customer is

(A) a R.O.C government entity;

(B) a enterprise owned by the R.O.C government;

(C) a foreign government entity;

(D) a public company and its subsidiaries;

(E) an entity listed on a stock exchange outside of R.O.C. that is subject to regulatory disclosure requirements of its principal shareholders, and the subsidiaries of such entity;

(F) a financial institution supervised by the R.O.C. government, and an investment vehicles managed by such institution;

(G) a financial institution incorporated or established outside R.O.C. that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the Financial Action Task Force on Money Laundering (FATF), and an investment vehicle managed by such institution; or

(H) Public Service Pension Fund, Labor Insurance, Labor Pension Fund and Postal Savings of R.O.C.

(7) A banking business should not establish a business relationship or carry out occasional transactions with a customer before completing the CDD process. However, a banking business may first obtain information on the identity of the customer and any beneficial owner and complete the verification following the establishment of business relationship, provided that:

A. money laundering and terrorist financing risks are effectively managed, including adopting risk management procedures with respect to the conditions under which a customer may utilize the business relationship to complete a transaction prior to verification;

B. it would be essential not to interrupt the normal conduct of business with the customer; and

C. verification of the identities of customer and beneficial owner will be completed as soon as reasonably practicable following the establishment of business relationship. The banking business shall terminate the business relationship if verification cannot be completed as soon as reasonably practicable and inform the customer in advance.

(8) Where a banking business is unable to complete the required CDD process on a customer, it should consider reporting suspicious transactions in relation to the customer.

(9) If a banking business suspects that a customer or transaction may relate to money laundering or terrorist financing and reasonably believes that performing the CDD process will tip-off the customer, it may choose not to pursue that process and file a suspicious transactions report instead.

5. If there exists any of the following situations in the CDD process, a banking business should decline to establish business relationship or carry out any transaction with the customer:

(1) The customer is suspected of using a fake name, a nominee, a shell entity, or a shell corporation to open an account;

(2) The customer refuses to provide the required documents for identifying and verifying his/her identity;

(3) Where a customer opens an account through a representative or an agent, it is difficult to check and verify the facts of representation or authorization and identity related information;

(4) The customer uses forged or altered identification documents or only provides photocopies of the identification documents;

(5) Documents provided by the customer are suspicious or unclear, or the customer refuses to provide other supporting documents, or the documents provided cannot be authenticated;

(6) The customer procrastinates in providing identification documents in an unusual manner;

(7) Other unusual circumstances exist in the process of establishing business relationship and the customer fails to provide reasonable explanations; or

(8) The customer is an individual, legal entity or organization sanctioned under the Terrorism Financing Prevention Act or a terrorist or terrorist group identified or investigated by a foreign government or an international anti-money laundering organization.

6. Ongoing customer due diligence:

(1) A banking business shall 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 whether and when CDD measures have previously been undertaken and the adequacy of data obtained. The aforementioned appropriate times include at least:

A. When the customer opens a new account or enters new business relationships;

B. When it is time for periodic review of the customer scheduled on the basis of materiality and risk; and

C. When it becomes known that there is a material change to customer's identity and background information.

(2) A banking business shall conduct ongoing due diligence on the

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

(3) A banking business shall periodically review the adequacy of customer identification information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date, particularly for higher risk categories of customers, for whom the banking business should conduct review at least once every year.

(4) A banking business is entitled to rely on the identification and verification steps that it has already undertaken, therefore a banking business is allowed not to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction unless it has doubts about the veracity of that information. Examples of situations that might lead a banking business to have such doubts could be where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile. In such events, the banking business shall conduct CDD again in accordance with the provisions of Point 4.

7. A banking business shall determine the extent of applying CDD and ongoing CDD measures under Subparagraph (3) of Point 4 and the preceding Point using a risk-based approach (RBA):

(1) For higher risk circumstances, a banking business shall apply enhanced CDD or ongoing CDD measures by adopting additionally at least the following enhanced measures:

A. Obtaining the approval of senior management before establishing or entering a new business relationship;

B. Adopting reasonable measures to understand the sources of wealth and the source of funds of the customer; in case the source of funds is deposits, understand further the source of deposits; and

C. Adopting enhanced ongoing monitoring of business relationship.

(2) For lower risk circumstances, a banking business may adopt simplified CDD measures, which shall be commensurate with the lower risk factors. However simplified CDD measures are not allowed in any of the following circumstances:

A. Where the customers are from or in countries and jurisdictions known to have inadequate AML/CFT regimes, including but not limited to those which designated by international organizations on AML/CFT as countries or regions with serious deficiencies in their AML/CFT regime , and other countries or regions that do not or insufficiently comply with the recommendations of international organizations on AML/CFT as forwarded by the Financial Supervisory Commission (FSC); or

B. Where a banking business suspects that money laundering or terrorist financing is involved.

8. Policies and procedures for checking the names of customers and trading counterparties:

(1) A banking business shall establish policies and procedures for checking the names of customers and trading counterparties using a risk-based approach to detect, match and filter customers or trading counterparties that are individuals, legal entities or organizations sanctioned under the Terrorism Financing Prevention Act or terrorists or terrorist groups identified or investigated by a foreign government or an international anti-money laundering organization, and handle related matters in compliance with Article 7 of the Terrorism Financing Prevention Act.

(2) The policies and procedures for checking the names of customers and trading counterparties of a banking business shall include at least matching and filtering logics, implementation procedures and inspection standards, and shall be documented.

(3) A banking business shall document its name and account checking operations and maintain the records for a time period in accordance with Point 10.

9. Ongoing monitoring of accounts and transactions:

(1) A banking business shall use a database to consolidate basic information and transaction information on all customers for inquiries by the head office and branches for AML/CFT purpose so

as to strengthen the bank's account and transaction monitoring ability. A banking business shall also establish internal control procedures for requests and inquiries as to customer information made by various entities, and shall exercise care to ensure the confidentiality of the information.

(2) A banking business shall establish policies and procedures for account and transaction monitoring using a risk-based approach and utilize information system to assist in the detection of suspicious transactions.

(3) A banking business shall review its policies and procedures for account and transaction monitoring based on AML/CFT regulations, nature of customers, business size and complexity, money laundering and terrorist financing related trends and information obtained from internal and external sources, and the results of internal risk assessment, and update those policies and procedures periodically.

(4) The policies and procedures for account and transaction monitoring of a banking business shall include at least the procedures for establishing a complete monitoring system, and carrying out the setting of parameters, threshold amounts, alerts and monitoring operations, the procedures for checking the monitored cases and reporting standards, and shall be documented.

(5) A complete monitoring system mentioned in the preceding Subparagraph shall include the patterns published by the trade associations and additional monitoring patterns in reference to the banking business' own money laundering and terrorist financing risk assessment or daily transaction information. Examples of monitoring patterns are as follows:

A. Where the total cash deposits or withdrawals into or from the same account on the same business day cumulatively reaches above NTD500,000 (including the foreign currency equivalent thereof) and the transactions do not appear to be commensurate with the account holder's status and income or are unrelated to the nature of the customer's business.

B. Where a customer makes multiple cash deposits or withdrawals at the same counter, which cumulatively reach above NTD500,000 (including the foreign currency equivalent thereof)

and the transactions do not appear to be commensurate with the customer's status and income or are unrelated to the nature of the customer's business.

C. Where a customer at the same counter at one time uses cash to make multiple outward remittances, or request the drawing of negotiable instruments (e.g., bank check, due-from-bank check, and bank draft), purchases NCD, traveler's checks, or other valuable securities, which in total exceeds NTD500,000 (including the foreign currency equivalent thereof) and the customer is unable to reasonably explain the purposes of those transactions.

D. Where the transactions involve a country or region with serious deficiencies in its AML/CFT regime and such transactions do not appear to be commensurate with the customer's status and income or is unrelated to the nature of the customer's business.

E. Where the ultimate beneficiary or transaction party is a terrorist or terrorist group as advised by the FSC based on information provided by foreign governments, or a terrorist organization identified or investigated by an international organization against money laundering; or where the transaction is suspected or bears reasonable reason to suspect to have been linked with a terrorist activity, terrorist organization or financing of terrorism.

F. Where the transaction amount exceeds a certain threshold and is clearly inconsistent with average account balance.

G. Where electronic transactions take place frequently over a short period of time and the cumulative transaction amount exceeds a certain threshold set by the banking business.

(6) A banking business shall document its ongoing account and transaction monitoring operation and maintain the records in accordance with Point 10.

10. A banking business shall keep records on all business relations and transactions with its customers in accordance with the following provisions:

(1) A banking business shall maintain, for at least five years, all necessary records on transactions, both domestic and international.

(2) A banking business shall keep all the following information for at

least five years after the business relationship is ended, or after the date of the occasional transaction:

A. All records obtained through CDD measures, such as copies or records of official identification documents like passports, identity cards, driving licenses or similar documents.

B. Account files.

C. Business correspondence, including inquiries to establish the background and purpose of complex, unusual large transactions and the results of any analysis undertaken.

(3) Transaction records maintained by a banking business must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

(4) A banking business shall ensure that information on transaction records and CDD information will be swiftly made available to the competent authorities when such requests are made with appropriate authority.

11. When conducting CDD, a banking business should use self-established database or information obtained from external sources to determine whether a customer or beneficial owner is a person who is or has been entrusted with a prominent function by a foreign government or an international organization (referred to as politically exposed persons (PEPs) hereunder):

(1) For a customer or beneficial owner determined to be a current PEP of a foreign government, a banking business shall treat the customer directly as a high-risk customer, and adopt enhanced CDD measures under Subparagraph (1) of Point 7.

(2) For a customer or beneficial owner determined to be a current PEP of an international organization, a banking business shall assess risks when establishing business relationship with the person and conduct annual review thereafter. In case of higher risk business relationship with such customers, the banking business shall adopt enhanced CDD measures under Subparagraph (1) of Point 7.

(3) The preceding two Subparagraphs apply to family members or close associates of PEPs.

(4) For former PEPs of foreign governments or international organizations, a banking business shall assess risks based on the

level of influence that the individual could still exercise, the seniority of the position that the individual held as a PEP, etc. If it is determined that the person is still a PEP, the provisions of the preceding three Subparagraphs shall apply.

12. A banking business shall establish specific policies and procedures for correspondent banking and other similar relationships, including at least:

(1) Gather sufficient publicly available information to fully understand the nature of the correspondent bank's business and to determine its reputation and quality of management, including whether it has complied with the AML/CFT regulations;

(2) Assess whether the correspondent bank has adequate and effective AML/CFT controls;

(3) Obtain approval from senior management before establishing relationships with a correspondent bank;

(4) Document the respective AML/CFT responsibilities of each institution;

(5) Where a correspondent relationship involves the maintenance of "payable–through accounts", it is necessary to identify that the correspondent bank has conducted CDD measures on the customer and that it is able to provide relevant CDD information upon request;

(6) The bank is prohibited from establishing correspondent relationship with any shell banks or any foreign financial organizations permitting any shell banks to use their accounts; and

(7) The aforementioned provisions apply when the correspondent bank is a foreign branch (subsidiary) of the banking business.

13. A banking business should assess the money laundering or terrorist financing risks that may arise in relation to the development of new products or services or new business practices (including new delivery mechanisms, use of new technologies for pre-existing or new products or business practices) and establish relevant risk management measures to mitigate those risks.

14. Wire transfers:

(1) A banking business shall conduct domestic and cross-border ordinary outgoing and incoming wire transfers involving foreign currencies in accordance with the Directions Governing Banking Enterprises for Operating Foreign Exchange Business.

(2) A banking business shall conduct domestic wire transfers involving NTD in accordance with the following rules:

A. The ordering financial institution of a domestic wire transfer should provide information on the originator and the beneficiary by any of the means below:

(A) Include in the wire transfer information on the originator and the beneficiary; or

(B) Include in the wire transfer the account number or a unique transaction reference number which permits traceability of the transaction and make information on the originator and the beneficiary available within three business days of receiving the request either from the beneficiary financial institution or from appropriate competent authorities.

B. The ordering financial institutions shall maintain all information on the originator and the beneficiary.

C. 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), the originator's address, or national identity number, or date and place of birth.

D. 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).

15. Internal control system:

(1) The internal control system established by a banking business according to Article 8 of "Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries", Article 5 of "Regulations Governing the Internal Controls and Audit System for Postal Remittances and Savings" or Article 33 of "Regulations Governing Institutions Engaging In Credit Card Business" shall contain the following

particulars:

A. The policies and procedures to identify, assess and manage its money laundering and terrorist financing risks.

B. An AML/CFT program established based on money laundering and terrorist financing risks and business size to manage and mitigate identified risks, which also includes enhanced control measures for higher risk situations.

C. Standard operational procedures for monitoring compliance with AML/CFT regulations and for the implementation of AML/CFT program, which shall be included in the self-inspection and internal audit system, and enhanced if necessary.

(2) The money laundering and terrorist financing risks mentioned in Item A of the preceding Subparagraph shall be identified, assessed and managed in accordance with the following provisions:

A. Risk assessment should be documented;

B. Risk assessment should consider all risk factors and cover at least customers, geographic areas, products and services, transactions and delivery channels to determine the level of overall risk, and appropriate measures to mitigate the risks; and

C. There should be a risk assessment update mechanism in place to ensure that risk data are kept up-to-date.

(3) The AML/CFT program mentioned in Item B of Subparagraph (1) shall include the following policies, procedures and controls:

A. Verification of customer identity;

B. Checking of names of customers and trading counterparties;

C. Ongoing monitoring of accounts and transactions;

D. Correspondent banking business;

E. Record keeping;

F. Reporting of currency delivery above a certain amount;

G. Reporting of suspicious transactions;

H. Appointment of a compliance officer at the management level to take charge of AML/CFT compliance matters;.

I. Employee screening and hiring procedure;

J. Ongoing employee training program;

K. An independent audit function to test the effectiveness of AML/CFT system; and

L. Other matters required by the AML/CFT regulations and the competent authorities.

(4) A banking business having foreign branches and subsidiaries shall establish a group-level AML/CFT program, which shall include the policies, procedures and controls mentioned in the preceding Subparagraph, and in addition, the following particulars without violating the information confidentiality regulations of the ROC and countries or jurisdictions at where the foreign branches and subsidiaries are located:

A. Policies and procedures for sharing information within the group required for the purposes of CDD and money laundering and terrorist financing risk management;

B. Group-level compliance and audit functions to be provided with customer, account and transaction information from foreign branches and subsidiaries when necessary for AML/CFT purposes; and

C. Adequate safeguards on the confidentiality and use of information exchanged.

(5) A banking business shall ensure that its foreign branches and subsidiaries apply AML/CFT measures, to the extent that the laws and regulations of host countries or jurisdictions so permit, consistent with the home country requirements. Where the minimum requirements of the countries where its head office and branches or subsidiaries are located are different, the branch or subsidiary shall choose to follow the criteria which are higher. However, in case there is any doubt regarding the determination of higher or lower criteria, the determination by the competent authority of the place at where the head office of the banking business is located shall prevail. If a foreign branch or subsidiary is unable to adopt the same criteria as the head office due to prohibitions from foreign laws and regulations, appropriate additional measures should be taken to manage the risks of money laundering and terrorist financing, and a report shall be made to the competent authorities.

(6) The board of director and senior management of a banking business should understand its money laundering and terrorist financing risks and the operation of its AML/CFT program, and adopt measures to

create a culture of AML/CFT compliance.

16. Dedicated compliance unit and chief AML/CFT compliance officer:

(1) A banking business shall set up an independent, dedicated AML/CFT compliance unit under the president, or the legal compliance unit or risk management unit of the head office. The AML/CFT compliance unit may not handle businesses other than AML/CFT and shall be staffed with adequate manpower and resources appropriate to the size and risks of the business. The board of directors of the banking business shall appoint a senior officer to act as the chief AML/CFT compliance officer and vest the officer full authority in AML/CFT implementation. The officer should report to the board of directors, supervisors (board of supervisors) or the audit committee at least semiannually, or whenever a major regulatory violation is discovered. A banking business that is not a domestic bank is not required to set up such a dedicated compliance unit, but shall be staffed with an adequate number of AML/CFT personnel appropriate to the size and risks of its business, and its board of directors shall appoint a chief compliance officer and make sure that its AML/CFT personnel and the chief AML/CFT compliance officer do not hold concurrent posts that may have a conflict of interest with their AML/CFT responsibilities.

(2) The dedicated compliance unit or chief AML/CFT compliance officer mentioned in the preceding paragraph shall be charged with the following duties:

A. Supervising the planning and implementation of policies and procedures for identifying, assessing and monitoring money laundering and terrorist financing risks.

B. Coordinating and supervising bank-wide AML/CFT risk identification and assessment.

C. Monitoring and controlling money laundering and terrorist financing risks.

D. Developing an AML/CFT program.

E. Coordinating and supervising the implementation of AML/CFT program.

F. Confirming compliance with AML/CFT regulations, including the relevant compliance template or self-regulatory rules produced

by the financial services trade association and approved by the FSC.

G. Supervising the reporting on suspicious transactions and on the properties or property interests and location of individuals or legal entities designated by the Terrorism Financing Prevention Act to the Investigation Bureau, Ministry of Justice.

(3) The foreign business unit of a banking business shall be staffed with an adequate number of AML/CFT personnel in view of the number of local branches, and the size and risks of its business, and appoint an AML/CFT compliance officer to take charge of related compliance matters.

(4) The appointment of an AML/CFT compliance officer by the foreign business unit of a banking business shall comply with the local regulations and the requirements of the local authorities. The AML/CFT compliance officer shall be vested with full authority in AML/ CFT implementation, including reporting directly to the chief AML/CFT compliance officer mentioned in Subparagraph (1), and should not hold other posts, except for the post of legal compliance officer. If the AML/CFT compliance officer holds other concurrent posts, the foreign business unit should communicate the fact with the local competent authority to confirm that the holding of other concurrent posts will not result or potentially result in conflict of interest, and report the matter to the competent authority for record.

17. Implementation and statement of internal AML/CFT control system:

(1) The domestic and foreign business units of a banking business shall appoint a senior manager to act as the supervisor to take charge of supervising the AML/CFT related matters of the business unit, and conduct self-inspection in accordance with the Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries.

(2) The internal audit unit of a banking business shall audit the following matters and submit audit opinions in accordance with the Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries:

A. Whether the money laundering and terrorist financing risk

assessment and the AML/CFT program meet the regulatory requirements and are vigorously implemented; and

B. The effectiveness of AML/CFT program.

(3) The president of a banking business should oversee that respective units prudently evaluate and review the implementation of internal AML/CFT control system. The chairman, president, chief auditor and chief AML/CFT compliance officer shall jointly issue a statement on internal AML/CFT control (see attached), which shall be submitted to the board of directors for approval and disclosed on the website of the banking business within three months after the end of each fiscal year, and filed via a website designated by the competent authority.

18. Employee hiring and training:

(1) A banking business shall establish prudent and appropriate procedures for employee screening and hiring, including examining whether the prospective employee has character integrity and the professional knowledge required to perform their duties.

(2) The chief AML/CFT compliance officer, the personnel of dedicated AML/CFT unit and the AML/CFT supervisor of domestic business units of a banking business shall possess one of the following qualification requirements:

A. Having served as a compliance officer or AML/CFT personnel on a full-time basis for at least three (3) years;

B. Having attended not less than 24 hours of courses recognized by the competent authority, passed the exams and received completion certificates therefor. Chief AML/CFT compliance officers and personnel of dedicated AML/CFT units who are appointed/assigned to the post prior to June 30, 2017 may receive the aforementioned certificates within six (6) months after the appointment/assignment, and the AML/CFT supervisors of domestic business units may receive such certificates within one year after the appointment/assignment; or

C. Having received a domestic or international AML/CFT professional certificate issued by an institution recognized by the competent authority.

(3) The chief AML/CFT compliance officer, the personnel of dedicated

AML/CFT unit and the AML/CFT supervisor of domestic business units of a banking business shall attend not less than 12 hours of training offered by institutions recognized by the competent authority or by the parent financial holding company (including its subsidiaries) or the employing banking business (including parent company) every year. The training shall cover at least newly amended laws and regulations, trends and patterns of money laundering and terrorist financing risks. If the person has obtained a domestic or international AML/CFT professional certificate issued by an institution recognized by the competent authority in a year, the certificate may be used to offset the training hours for the year.

(4) The AML/CFT supervisor and the AML/CFT officer and personnel of foreign business units of a banking business shall attend not less than 12 hours of training on AML/CFT offered by foreign competent authorities or relevant institutions. If no such training is available, the personnel may attend training courses offered by institutions recognized by the competent authority or by the parent financial holding company (including its subsidiaries) or the employing banking business (including parent company).

(5) A banking business shall arrange appropriate hours of orientation and on-the-job training of suitable contents on AML/CFT in view of the nature of its business for its legal compliance personnel, internal auditors and business personnel to familiarize them with their AML/CFT duties and equip them with the professional knowhow to perform their duties.

19. If a banking business violates the Directions, the FSC may take appropriate sanctions commensurate with the seriousness of the violations in accordance with Articles 61-1, 129 of the Banking Act, the Money Laundering Control Act and other relevant regulations.