

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

1. These Directions are specifically adopted to strengthen the anti-money laundering and countering the financing of terrorism (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 comply 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 NTD 30,000 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 nature of business, ownership and control structure of the customer or trust (including trust-like legal arrangements) and obtain at least the following information to identify the customer or the trust and verify its identity:

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, if different, a 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 apply appropriate measures for customers who have issued bearer shares to ensure their 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 and take reasonable measures to

verify the identity of the beneficial owner(s):

A. For legal persons:

(A) The identity of the natural person(s) who ultimately has a controlling ownership interest in a legal person. A controlling ownership interest refers to owning more than 25 percent 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 is the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural person(s) (if any) exercising control of the 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(s) 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 natural person(s) exercising ultimate effective control over the trust, or the identity of person(s) in equivalent or similar position.

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(s) or beneficial owner(s) of a customer, provided the customer or the person having a controlling ownership interest in the customer is

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

(B) An 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 shall not establish the business relationship or conduct 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 its beneficial owner(s) and complete the verification after the establishment of business relationship, provided that:
- A. The money laundering and terrorist financing (ML/TF) 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. This is essential not to interrupt the normal conduct of business with the customer; and
  - C. Verification of the identities of the customer and its beneficial owner(s) will be completed as soon as reasonably practicable after the establishment of business relationship. A banking business shall advise its customer in advance that the business relationship will be terminated if verification cannot be completed as soon as reasonably practicable.
- (8) Where a banking business is unable to complete the required CDD process on a customer, it should consider filing a suspicious transaction report (STR) in relation to the customer.
- (9) If a banking business forms a suspicion of money laundering or terrorist financing and reasonably believes that performing the CDD process will tip-off the customer, it is permitted not to pursue that process and file an STR 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 firm, or a shell corporation or entity to open an account;
  - (2) The customer refuses to provide the required documents for identifying and verifying its identity;
  - (3) Whereas any person acts on behalf of a customer to open an account, it is difficult to check and verify the fact of 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 so that the documents cannot be authenticated, or the customer refuses to provide other supporting documents;
- (6) The customer procrastinates in providing identification documents in an unusual manner;
- (7) Other unusual circumstances exist in the process of establishing the business relationship and the customer fails to provide reasonable explanations; or
- (8) The customer is an individual, a legal person or an 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 due diligence:

- (1) A banking business shall apply CDD requirements 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 another new account or enters new business relationships with the banking business;
  - 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 to 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, its business and risk profile, including, where necessary, the source of funds.
- (3) A banking business shall periodically review the existing records to ensure that documents, data or information of the customer and its beneficial owner(s) collected under the CDD process are kept up-to-date and relevant, particularly for higher risk categories of

customers, whose reviews shall be conducted at least once every year.

- (4) A banking business can rely on existing customer records to undertake identification and verification. Therefore, a banking business is allowed to carry out transactions without repeatedly identifying and verifying the identity of an existing customer. However, a banking business shall conduct CDD measures again in accordance with Point 4 if it has doubts about the veracity of the records, such as, 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.
7. A banking business shall determine the extent of applying CDD and ongoing due diligence 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 perform enhanced CDD or ongoing due diligence 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. Taking 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. Conducting enhanced ongoing monitoring of business relationship.
  - (2) For lower risk circumstances, a banking business may apply 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 there is a suspicion of money laundering or terrorist

financing.

8. Policies and procedures for watch list filtering:

- (1) A banking business shall establish policies and procedures for watch list filtering, using a risk-based approach, to detect, match and filter whether customers or its trading counterparties are individuals, legal persons 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 watch list filtering shall include at least matching and filtering logics, implementation procedures and evaluation standards, and shall be documented.
- (3) A banking business shall document its name and account filtering operations and maintain the records for a time period in accordance with Point 10.

9. Ongoing account and transaction monitoring:

- (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 capability of account and transaction monitoring. A banking business shall also establish internal control procedures for requests and inquiries as to customer information 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, ML/TF trends and related information gathered from internal and external sources, and its risk assessment results, 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 complete ML/TF monitoring indicators, and carrying out the setting of parameters,

threshold amounts, alerts and monitoring operations, the procedures for examining the monitored cases and reporting standards, and shall be documented.

(5) Complete ML/TF monitoring indicators mentioned in the preceding Subparagraph shall include the suspicious indicators published by the trade associations and the additional ones developed by the banking business in reference to its ML/TF risk assessment or daily transaction information. Examples of the suspicious indicators 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), purchase 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 transaction records and CDD information will be available swiftly to the competent authorities when such requests are made with appropriate authority.
11. When conducting CDD measures, a banking business should use self-established database or information obtained from external sources to determine whether a customer or the 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 the 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 the beneficial owner determined to be a current PEP of an international organization, a banking business shall assess the PEP's 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 a PEP who is no longer entrusted with a prominent public function by a foreign government or an international organization, a banking business shall assess such person's 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 respondent 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 respondent bank has adequate and effective AML/CFT controls;
  - (3) Obtain approval from senior management before establishing new relationships with respondent banks;
  - (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 for the correspondent bank satisfying itself that the respondent bank has performed CDD obligations on its customer and that it is able to provide relevant CDD information upon request;
  - (6) The bank is prohibited from establishing correspondent banking relationships with any shell banks or any respondent financial

institutions permitting their accounts to be used by shell banks; and  
(7) The aforementioned provisions apply when the respondent bank is a foreign branch (subsidiary) of the banking business.

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

14. Wire transfers:

(1) A banking business shall conduct domestic and cross-border outward and inward 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 information on the originator and the beneficiary accompanying the wire transfer; or

(B) Only include the account number or a unique transaction reference number which permits the transaction to be traced back 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 ML/TF risks.
  - B. An AML/CFT program established based on ML/TF 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 the AML/CFT program, which shall be included in the self-inspection and internal audit system, and enhanced if necessary.
- (2) The ML/TF 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 or 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. Customer due diligence;
  - B. Watch list filtering;
  - C. Ongoing due diligence of accounts and transactions ;
  - D. Correspondent banking business;
  - E. Record keeping;
  - F. Filing CTR;

- G. Filing STR;
  - H. Appointment of a compliance officer at the management level in 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 or subsidiaries shall establish a group-wide 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 host countries or jurisdictions:
- A. Policies and procedures for sharing information within the group required for the purposes of CDD and ML/TF risk management;
  - B. Group-level compliance and audit functions to require foreign branches and subsidiaries to provide customer, account and transaction information 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 host countries 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 home country 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 shall be applied to manage the ML/TF risks, 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 ML/TF risks and the operation of its AML/CFT

program, and adopt measures to foster 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 shall 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 it shall be staffed with an adequate number of AML/CFT personnel appropriate to the size and risks of its business, its board of directors shall also appoint a chief compliance officer, and it shall ensure 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 ML/TF risks.
  - B. Coordinating and supervising the implementation of the bank-wide AML/CFT risk identification and assessment.
  - C. Monitoring and controlling ML/TF 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 specimen or self-regulatory rules formulated 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(s) 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 regulations and requirements of the host country. 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 a legal compliance officer. If the AML/CFT compliance officer holds other concurrent posts, the foreign business unit should communicate the fact with the competent authority of the host country to confirm the holding of other concurrent posts not resulting in or potentially leading to the conflict of interest, and report the matter to the FSC for recordation.
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 ML/TF 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 control system for AML/CFT. The chairman, president, chief auditor and Chief AML/CFT compliance officer shall jointly issue a

statement on internal control for AML/CFT (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 its duty.
- (2) The Chief AML/CFT compliance officer, the personnel of dedicated AML/CFT unit and the AML/CFT supervisors 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 years;
  - B. Having attended not less than 24 hours of courses recognized by the competent authority, passed the exams and received the completion certificate 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, are allowed to receive the aforementioned certificate within six months after the appointment/assignment, and the AML/CFT supervisors of domestic business units are allowed to receive such certificate within one year after the appointment/assignment; or
  - C. Having received an AML/CFT professional certificate issued by a domestic or international institution recognized by the competent authority.
- (3) The Chief AML/CFT compliance officer, the personnel of dedicated AML/CFT unit and the AML/CFT supervisors 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 its parent company) every year. The training shall cover at least newly amended laws and regulations, trends and typologies of ML/TF risks. The training hours can be offset in the year when the person obtains an AML/CFT professional certificate issued by a domestic or international



institution recognized by the competent authority.

- (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 course 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 its parent company).
  - (5) A banking business shall arrange appropriate hours and contents of orientation and on-the-job training for AML/CFT, according to the nature of the job, for its legal compliance personnel, internal auditors and business personnel to familiarize them with their AML/CFT duties and equip them with such professional know-how.
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.