Directions Governing Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business, Electronic Payment Institutions and Electronic Stored Value Card Issuers

1. These Directions are adopted to strengthen the anti-money laundering and countering terrorism financing (AML/CFT) regime of the Republic of China (R.O.C.), and to enhance the soundness of the internal control and internal audit system of the banking business, electronic payment institutions and electronic stored value card issuers.

2. In matters related to AML/CFT internal controls, banking business, electronic payment institutions and electronic stored value card issuers shall comply with these Directions as well as relevant provisions in the "Money Laundering Control Act", "Terrorism Financing Prevention Act", "Regulations Governing the Deposit Accounts and Suspicious or Unusual Transactions" and "Directions for Confirming Customer Identity in Domestic Remittance Operations of Financial Institutions."

3. Terms used in these Directions are defined as follows:
   (1) "Banking business" includes banks, credit cooperatives, postal institutions handling postal savings and remittance businesses, transfer and withdrawal, bills finance companies, credit card companies and trust enterprises.
   (2) "Electronic payment institution" means an institution approved to engage in electronic payment business pursuant to the Act Governing Electronic Payment Institutions.
   (3) "Electronic stored value card issuer" means an institution approved to issue electronic stored value cards pursuant to the Act Governing Issuance of Electronic Stored Value Cards.

4. 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 and whether it has been investigated or received regulatory action in connection with money laundering or terrorist financing (ML/TF);
   (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 party;
   (5) Where a correspondent relationship involves in "payable–through accounts", it should be required to satisfy themselves that the respondent bank has performed customer due diligence

(CDD) measures on customers who may direct access to the accounts of the correspondent bank; and is able to provide relevant CDD information upon request to the correspondent bank;

(6) The banking business is prohibited from entering into correspondent relationship with shell banks and shall satisfy themselves that respondent financial institutions do not permit their accounts to be used by shell banks;

(7) For a correspondent bank that is unable to provide the aforementioned information upon the request of the banking business, the banking business may decline the correspondent bank's application to open an account, suspend transactions with the correspondent bank, file a suspicious ML/TF transaction report or terminate business relationship ;

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

5. Banking business, electronic payment institutions and electronic stored value card issuers should assess ML/TF risks before launching 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 identified risks.

6. 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) Include the account number or a unique transaction reference number which permits the transaction to be traced back to the originator and the beneficiary and make information available within three business days of receiving the request either from the beneficiary financial institution or from appropriate competent authorities. However Law enforcement authorities should be able to compel immediate production or such information and the banking business shall respond accordingly.

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).

(3) A banking business that fails to conduct wire transfers in compliance with the preceding two subparagraphs is not allowed to engage in wire transfer business.

7. Internal control system:

(1) The AML/CFT internal control system established by a banking business, electronic payment institution or electronic stored value card issuer and any subsequent amendment thereto shall be approved by its board of directors (council), and shall contain of the following:

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 risk identification, assessment and management mentioned in Item A of the preceding subparagraph should cover at least customers, geographic areas, products and services, transactions and delivery channels and contain of the following:

A. A risk assessment report should be produced.

B. Risk assessment should consider all risk factors to determine the level of overall risk, and appropriate measures to mitigate the risks.

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

D. When risk assessment is completed or updated, the risk assessment report shall be submitted to the Financial Supervisory Commission (FSC) for recordation.

(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 currency transaction report (CTR);

G. Filing suspicious ML/TF transaction report (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 FSC.

(4) A banking business, electronic payment institution or electronic stored value card issuer having foreign branches (or subsidiaries) shall establish a group-wide programmers against ML/FT which should be applicable, and appropriate to, all branches (or subsidiaries) of the financial group. The AML/CFT program shall include the policies, procedures and controls mentioned in the preceding subparagraph, and in addition, contain of the following 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 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, electronic payment institution or electronic stored value card issuer shall ensure that its foreign branches (or subsidiaries) apply AML/CFT measures to the extent that the laws and regulations of host countries or jurisdictions so permit, and those measures should be consistent with those adopted by the head office (or parent company). Where the minimum requirements of the countries where its head office (or parent company) 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, electronic payment institution or electronic stored value card issuer is located shall prevail. If a foreign branch (or subsidiary) is unable to adopt the same criteria as the head office (or parent company) due to prohibitions from foreign laws and regulations, appropriate additional measures should be taken to manage the ML/TF risks, and report to FSC.

(6) The board of directors (council) of a banking business, electronic payment institution or electronic stored value card issuer takes the ultimate responsibility of ensuring the establishment and maintenance of appropriate and effective AML/CFT internal controls. The board of directors and senior management of a banking business, electronic payment institution or electronic stored value card issuer should understand the company's ML/TF risks and the operation of its AML/CFT program, and adopt measures to create a culture of AML/CFT compliance.

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

(1) A banking business, electronic payment institution or electronic stored value card issuer shall be staffed with adequate number of AML/CFT personnel and resources appropriate to the size and risks of its business. The board of directors (council) of the banking business, electronic payment institution or electronic stored value card issuer shall appoint a senior officer to act as the chief AML/CFT compliance officer and vest the officer full authority in coordinating and supervising AML/CFT implementation and 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. A domestic bank shall, in addition, 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 and such AML/CFT compliance unit shall not handle businesses other than AML/CFT.

(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 company-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 related financial services association and accepted by the FSC for recordation.

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 chief AML/CFT compliance officer mentioned in Subparagraph (1) hereof should report to the board of directors (council) and supervisors (board of supervisors) or the audit committee at least semiannually, or whenever a major regulatory violation is discovered.

(4) The foreign business units of a banking business, electronic payment institution or electronic stored value card issuer 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 the coordination and supervision of related compliance matters.

(5) The appointment of an AML/CFT compliance officer by the foreign business unit of a banking business, electronic payment institution or electronic stored value card issuer 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 coordination and supervision, 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.

9. Implementation, audit and statement of internal AML/CFT control system:
   (1) The domestic and foreign business units of a banking business, electronic payment institution or electronic stored value card issuer shall appoint a senior manager to act as the supervisor to take charge of supervising AML/CFT related matters of the business unit, and conduct self-inspection.
   (2) The internal audit unit of a banking business, electronic payment institution or electronic stored value card issuer shall audit the following matters and submit audit opinions on:
      A. whether the ML/TF risk assessment and the AML/CFT program meet the regulatory requirements and are implemented; and
      B. the effectiveness of AML/CFT program.
   (3) The president of a banking business, electronic payment institution or electronic stored value card issuer should oversee the respective units to 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 (council) for approval and disclosed on their website of the banking business within three (3) months after the end of each fiscal year, and filed via a website designated by the FSC.
   (4) For the branches of a foreign bank or foreign credit card company in Taiwan, the authorized personnel of its head office shall be responsible for matters concerning the board of director or supervisors under these Directions. The statement mentioned in the preceding subparagraph shall be jointly issued by the litigious/non-litigious agent and chief AML/CFT compliance officer of the branch in Taiwan as well as officer in charge of audit operation in Taiwan area.

10. Employee hiring and training:
   (1) A banking business, electronic payment institution or electronic stored value card issuer hall 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, electronic payment institution or electronic stored value card issuer shall possess one of the following qualification requirements in three (3) months after appointment/assignment to the post and the financial institution shall set out relevant control mechanism to ensure compliance with the provisions hereof:

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 offered by institutions recognized by the FSC, passed the exams and received completion certificates therefor. But personnel who have met the qualification requirement for legal compliance personnel are deemed to meet the qualification requirement under this Item after they have attended at least 12 hours of training on AML/CFT offered by institutions recognized by the FSC; or

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

(3) Personnel mentioned in the preceding subparagraph who are appointed/assigned to the post prior to June 30, 2017 may be deemed as qualified if he or she meets any of the qualification requirements below:

A. Meeting the qualification requirement set out in Item A or Item C after 6 months of appointed.

B. Meeting the qualification requirement set out in item 2 of the preceding subparagraph within the time periods specified below:

(A) For the chief AML/CFT compliance officer and AML/CFT personnel of a banking business, meeting the qualification requirement within six (6) months after appointment/assignment to the post.

(B) For the chief AML/CFT compliance officer and AML/CFT personnel of an electronic payment institution or electronic stored value card issuer, meeting the qualification requirement before December 31, 2017.

(C) For AML/CFT supervisor of domestic business units of a banking business, electronic payment institution or electronic stored value card issuer, meeting the qualification requirement within one year after appointment/assignment to the post.

(4) The chief AML/CFT compliance officer, AML/CFT personnel and the AML/CFT supervisor of domestic business units of a banking business, electronic payment institution or electronic stored value card issuer shall attend not less than 12 hours of training on AML/CFT offered by internal or external training units consented by the chief AML/CFT compliance officer mentioned under Subparagraph (1) of Point 8 herein 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 FSC in a year, the certificate may be used to offset the training hours for the year.

(5) The AML/CFT supervisor and the AML/CFT officer and personnel of foreign business units of a banking business, electronic payment institution or electronic stored value card issuer shall possess professional knowledge in AML/CFT, be well informed in relevant local regulations, and attend not less than 12 hours of training on AML/CFT offered by foreign competent authorities or relevant institutions every year. If no such training is available, the personnel may attend training courses offered by internal or external training units consented by chief AML/CFT compliance officer mentioned under Subparagraph (1) of Point 8 herein.

(6) A banking business, electronic payment institution or electronic stored value card issuer shall arrange appropriate hours of orientation and on-the-job training of suitable contents on AML/CFT every year in view of the nature of its business for its directors (council members), supervisors, president, 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.

11. If a banking business, electronic payment institution or electronic stored value card issuer violates these Directions, the FSC may impose appropriate sanctions commensurate with the seriousness of the violations in accordance with Articles 61-1 and 129 of the Banking Act, Articles 35 and 48 of the Act Governing Electronic Payment Institution, Articles 25 and 31 of Act Governing Issuance of Electronic Stored Value Cards and other relevant regulations.