Model Guidelines for Trust Enterprises' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures

Tai-Chai-Zon (IV) Tze No. 0924001078 Letter dated October 28, 2003 by the Ministry of Finance
Chin-Kuan-Yin (IV) Tze No. 0930034168 Letter dated December 7, 2004 by the Financial Supervisory Commission, Executive Yuan
Chin-Kuan-Yin (IV) Tze No. 09585006970 Letter dated March 28, 2006 by the Financial Supervisory Commission, Executive Yuan
Chin-Kuan-Yin (IV) Tze No. 09800247560 Letter dated June 24, 2009 by the Financial Supervisory Commission, Executive Yuan
Chin-Kuan-Yin-Peu-Tze No. 10300244580 Letter dated September 5, 2014 by the Financial Supervisory Commission
Chin-Kuan-Yin-Peu-Tze No. 10400179610 Letter dated September 9, 2015 by the Financial Supervisory Commission
Chin-Kuan-Yin-Peu-Tze No. 10600186050 Letter dated August 24, 2017 by the Financial Supervisory Commission
Chin-Kuan-Yin-Peu-Tze No. 1080133776 Letter dated October 24, 2019 by the Financial Supervisory Commission

Article 1

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

Article 2

A trust enterprise’s internal control system for the purposes of anti-money laundering and countering terrorism financing established in accordance with Article 6 of “ Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated by the Financial Supervisory Commission” and its amendment should be approved by the board of directors. Such internal control systems should include:

I. Policies and procedures for identifying, assessing, and managing the risk of money laundering and terrorism financing (“ML/TF”) established in accordance with “Guidelines to Trust Enterprise on Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program” (“Guidelines”). See attachment.
II. Anti-money laundering and countering the financing of terrorism (“AML/CFT”) programs established in accordance with the Guidelines and based on risk assessment result and scale of business to manage and mitigate the risks identified and to take enhanced control measures with respect to higher risk categories.
III. Procedures for supervising the compliance of AML/CFT regulations and the implementation of AML/CFT programs. Such procedures, subject to self-inspection and internal audit, should be

enhanced if necessary.

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

I. Generating a risk assessment report.
II. Considering all risk factors to determine the trust enterprise's level of risk and the appropriate measures to mitigate risks.
III. Having a mechanism in place for updating risk assessment report periodically to ensure the update of risk profile.
IV. Filing the risk assessment report to Financial Supervisory Commission ("FSC") after it is completed or updated.

The AML/CFT programs provided in subparagraph II of paragraph 1 should include following policies, procedures and controls:

I. Customer due diligence ("CDD")
II. Name screening on customers and related parties of a transaction.
III. Ongoing monitoring of accounts and transactions.
IV. Correspondent banking.
V. Record-keeping.
VI. Reporting of currency transactions that reach a certain amount.
VII. Reporting of suspicious ML/TF transactions and reporting in accordance with "Counter-Terrorism Financing Act".
VIII. Appointment of an AML/CFT responsible officer.
IX. Procedures for screening and hiring employees.
X. An ongoing employee training program.
XI. An independent audit function used to test the effectiveness of AML/CFT system.
XII. Others required in AML/CFT related regulations or by FSC.

A trust enterprise that has any foreign branch (or subsidiary) (referred to as the "branches" hereinafter) for trust businesses should establish group-level AML/CFT programs and implement such programs in all branches. In addition to the policies, procedures, and controls provided in the last paragraph, on condition that the regulatory requirements on data confidentiality regulations of R.O.C. and jurisdictions where the trust enterprise has any foreign branches are met, such programs should include:

I. Policies and procedures for sharing information within the group required for the purposes of CDD and ML/TF risk management.
II. In order to prevent money laundering and combat terrorism financing, if necessary, request foreign branches to provide information on customers, accounts, and transactions according to group-level compliance, audits, and AML/CFT functions. Information and analysis of abnormal transactions or activities should be included. If necessary, obtain the above information from the foreign branches through the group management measures.
III. Safeguards on the confidentiality and use of information exchanged, including protection against data breach.

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

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

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

Article 3

The terms used in the Template are defined as follows:

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

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

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

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

V. “Occasional transaction” refers to a transaction between a trust enterprise and a person that has no business relationship with the trust enterprise.

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

VII. “Risk-based approach” refers to that a trust enterprise should identify, assess and understand the ML/TF risks that it is exposed to and take appropriate AML/CFT measures to effectively mitigate such risks. With such approach, a trust enterprise should take enhanced measures for higher risk scenarios while simplified measures may be taken for lower risk scenarios to effectively allocate resources and mitigate the identified ML/TF risks in the most appropriate and effective way.

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

Article 4

A trust enterprise should comply with following requirements when conducting CDD measures:

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

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

(ii) A customer refuses to provide relevant documentations required for the purpose of CDD

except that a trust enterprise may verify the client's identify using reliable, independent source of information.

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

(iv) Using counterfeit or altered identity documents.

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

(vi) The provided document data is suspicious or illegible; no supporting data is made available; or, the provided document data can't be verified.

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

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

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

II. A trust enterprise should perform CDD when:

(i) Establishing business relationship with a customer.

(ii) Carrying out any of following occasional transactions:

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

(iii) Identifying a suspicious ML/TF transaction.

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

III. A trust enterprise should take CDD measures as follows:

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

(ii) In the case that any person acts on behalf of a customer to establish business relationship

or conduct transactions, a trust enterprise should verify that the person purporting to act on behalf of the customer is so authorized. In addition, identify and verify the identity of that person in accordance with subparagraph III. (i), and retain hard copies of the agent's identity documents or record the relevant information thereon.

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

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

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

(i) Name;

(ii) Date of birth;

(iii) Permanent or residence address;

(iv) Official identification number;

(v) Nationality; and

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

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

(i) Any other names used or alias: such as the name used before marriage or change of name;

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

(iii) Landline or mobile telephone numbers.

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

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

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

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

(iii) The name, birthday, and nationality of persons holding the position of senior management (including directors, supervisors, chief executive officer, chief financial officer, authorized representatives, temporary manager, partners, authorized signatories,

or any natural person having an equivalent aforementioned position - a trust enterprise should determine the scope of senior management position by applying a risk-based approach) in an entity or trustee of a trust should be stated. The medium-risk or low-risk customers identified with the risk-based approach should only be subject to basic review (e.g., name verification). If there is any doubt, the information of birthday and nationality should be provided additionally. However, corporate clients who are classified as below may be exempted from the need of providing the information of birthday and nationality:

1. A public company or its subsidiary in Taiwan;
2. The listed companies or OTC companies and their subsidiaries that have their major shareholders disclosed according to the regulations of the place where it is listed overseas;
3. Financial institution incorporated or established in other jurisdiction where it is subject to regulatory requirements that are consistent with FATF AML/CFT standard, and investment vehicle managed by such financial institution;

(iv) Official identification number: such as identification number, tax identification number, registration number;

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

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

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

(i) For a customer that is an entity:

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

trust enterprise should identify the persons holding the position of senior management.

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

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

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

VIII. For a customer with whom a trust enterprise establishes business relationship, the trust enterprise should take following measures to verify the identity of the customer, the person acting on behalf of the customer, and the beneficiary owners of the customers:

(i) Verification through documents:

1. Individual:
   (1) Verification of identity or date of birth: obtain an unexpired official identification document that bears a photograph of the individual (e.g. identification card, passport, residence card, driving license, etc.) If there is doubt as to the validity of such documents, a trust enterprise should obtain

certification provided by an embassy official or a public notary. With respect to the identity or date of birth of the beneficial owners of an entity, a trust enterprise may not obtain original copies of the aforementioned document for verification, or may, according to the trust enterprise's internal operating procedures, request the entity and its authorized representative to provide a certification that specifies the identification data of the beneficiary owners. Part of the data on such certification, however, should allow a trust enterprise to perform verification through the certificate of incorporation, annual report, or other reliable source documents or data.

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

2. Entity or trustee of a trust: obtain certified articles of incorporation, government-issued business license, partnership agreement, trust instrument, certification of incumbency, etc. If a trust is managed by a financial institution described in paragraph 1 of Article 5 of Money Laundering Control Act, a certification issued by the financial institution may substitute for the trust instrument of the trust unless the jurisdiction where the financial institution is located is one of jurisdictions described in subparagraph III of paragraph 1 of Article 6.

(ii) Verification through non-documentary methods (if necessary), for example:

1. Contacting the customer by telephone or letter after an account has been opened.
2. Checking references provided by other financial institutions.
3. Cross-checking information provided by the customer with other reliable public information or private database, etc.

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

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

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

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

(iv) Site visit.

(v) Obtaining prior trust enterprise reference and contacting with the trust enterprise regarding the customer.

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

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

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

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

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

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

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

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

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

1. There is no suspicion of ML/TF;
2. The customer is assessed as a low ML/TF risk customer;
3. The transaction is approved by senior management, whose level is determined on the basis of the trust enterprise's internal consideration for risk; and
4. The names of recipients do not match with lists established for AML/CFT purposes.

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

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

1. The trust enterprise should complete customer identity verification no later than 30 working days after the establishment of business relationship.

2. If customer identity verification remains uncompleted 30 days after the establishment of business relationship, the trust enterprise should suspend business relationship with the customer and refrain from carrying out further transactions (except to return funds to their sources, to the extent that this is possible).
3. If customer identity verification remains uncompleted 120 days, the trust enterprise should terminate business relationship with the customer.

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

(i) Requesting the customer to require bearer share holders who ultimately have a controlling ownership interest to notify the customer to record their identity, and requesting the customer to notify the trust enterprise immediately when the identity of such share holder changes.

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

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

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

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

(iii) If the persons holding senior management position in the customer are PEPs entrusted by a domestic or foreign government or international organization, the trust enterprise should take into account the influence that such person exerts on the customer, to determine whether the customer is subject to EDD measures provided in subparagraph (i)

of paragraph I of Article 6.

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

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

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

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

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

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

(iii) The trust enterprise should perform EDD measures with respect to a private trust enterprise customer.

(iv) The trust enterprise should perform EDD measures with respect to a customer rejected by other financial institutions.

(v) For a non-face-to-face customer, the trust enterprise should perform CDD procedures that are as effective as those performed in the ordinary course of business and must include special and sufficient measures to mitigate the risks.

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

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

(viii) If the trust enterprise knows or is required to presume the source of fund of a customer is corruption or abuse of public assets, the trust enterprise should not accept, or should terminate, the business relationship with the customer if relevant regulatory requirements

are met.

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

(x) When the trust enterprise suspects certain customers or transactions may be involved in ML/TF and reasonably believe that performing CDD procedures may allow the customer to become aware of such information, the trust enterprise may be exempted from implementing such procedures and instead report a suspicious ML/TF transaction.

(xi) For other requirements regarding to establishing business relationship, please refer to the trust enterprise's internal regulations.

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

(i) In the situation described in subparagraph I. (viii), the trust enterprise may decline the request of establishing business relationship or terminate the business relationship.

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

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

Article 5

The CDD measures conducted by a trust enterprise should include following requirements in ongoing due diligence on customer identity:

I. The trust enterprise should scrutinize transactions undertaken throughout the course of all transactions to ensure that the transactions being conducted are consistent with the trust

enterprise's knowledge of the customer, their business, and risk profile including where necessary, the source of funds.

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

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

Article 6

A trust enterprise should determine the extent to which it conducts CDD and ongoing due diligence measures described in paragraph 3 of Article 4 and Article 5 by applying a risk-based approach, including:

I. For higher risk situations, the trust enterprise should take enhanced CDD and ongoing due diligence measures, which at least include following additional enhanced measures:
   (i) Before establishing or adding new business relationship, the trust enterprise should obtain the approval of certain level senior management, determined according to the trust enterprise's internal consideration of risk.
   (ii) The trust enterprise should take reasonable measures to understand the source of wealth and source of funds of the customer. The source of funds refers to the original source that generates such funds (e.g. salary, investment proceeds, disposal of real estate, etc.)
   (iii) Conducting enhanced ongoing monitoring of the business relationship.

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

III. For lower risk situations, the trust enterprise may take simplified measures commensurate with the lower risk factors. Simplified measures, however, should not be permitted in one of the following situations:
   (i) Customers are high ML/TF risk jurisdictions, which include but are not limited to the jurisdictions, published by international anti-money laundering organizations and notified by FSC, that have serious deficiencies in AML/CFT, and other jurisdictions that

fail to comply with or completely comply with the recommendations of such organizations.

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

A trust enterprise may take following simplified due diligence measures:

I. Lower the frequency of updating customer identification data.

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

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

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

Article 7

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

I. Obtain immediately the necessary information concerning CDD measures.

II. Take measures to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay.

III. Satisfy itself that the third party is regulated, and supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements.

IV. Satisfy itself that the jurisdiction where the third party is located has AML/CFT regulatory requirements consistent with FATF standard.

Article 8

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

I. The trust enterprise should establish policies and procedures for name screening on customers and related parties of a transaction, by applying a risk-based approach, to detect, match, and filter whether customers, persons holding senior management position of a customer, beneficial owners of a customer, or related parties of a transaction are designated individuals or entities sanctioned under Counter-Terrorism Financing Act, or terrorists or terrorist groups identified or investigated by foreign governments or international organizations. In the case of true hit, the trust enterprise should undertake the measures provided in subparagraph XVI of Article 4.

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

III. The trust enterprise should record the result of name screening and keep such record in accordance with the requirements of Article 13.

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

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

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

(iii) The logic of matching and filtering.

(iv) Model validation.

(v) Whether data output is correct and complete.

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

Article 9

A trust enterprise's ongoing monitoring of accounts and transactions should be conducted as follows:

I. The trust enterprise should integrate customer information data and transaction data throughout the company step-by-step by information systems for enquiries processed by the head office and branches for the purpose of AML/CFT, in order to enhance its capacity of account and transaction monitoring. With respect to the customer data requested or enquired about by each business unit, the trust enterprise should establish an internal control procedure and ensure the confidentiality of the data.

II. The trust enterprise should establish policies and procedures for ongoing monitoring of accounts and transactions by applying a risk-based approach and use information systems to

assist the identification of suspicious ML/TF transactions.

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

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

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

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

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

(iii) The logic of detection scenario.

(iv) Model validation.

(v) Data input.

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

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

VIII. For red flag transactions identified in accordance with last subparagraph, the trust enterprise should determine whether such transactions are reasonable (e.g. whether such transactions are apparently incommensurate with the identity, income, or scale of business of the customer, unrelated to the customer's business profile, do not match the customer's business model, no reasonable economic purpose, no reasonable explanation, no reasonable purpose, or unclear source of funds or explanation), complete the investigation as to whether or not they are suspected of money laundering or terrorism financing as soon as possible and keep review records. If after the investigation the trust enterprise determines such transaction is not a suspicious ML/TF transaction, the trust enterprise should record the reason for the decision. If after the investigation the trust enterprise determines such transaction is suspicious ML/TF

transaction, no matter how much is the amount of the transaction, it should record the transaction on a report form designated by the Investigation Bureau of the Ministry of Justice and immediately submit the form to the Bureau upon the approval of the responsible supervisor, and the report submission shall not be more than two business days after the supervisor's approval. The same procedure applies to the transactions that have not yet been completed.

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

Reporting of suspicious ML/TF transactions:

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

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

III. After the report is approved, the trust enterprise should submit the report to the responsible unit.

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

V. In the case of an apparently significant and urgent suspicious ML/TF transaction, the trust enterprise should immediately report to the Investigation of Bureau, Ministry of Justice by fax or other feasible means and then immediately submit the hard copy of the report. The trust enterprise is not required to submit the hard copy of the report, provided that the Investigation of Bureau, Ministry of Justice confirms the receipt of such report by sending a fax reply (please download the format on the website of the Investigation of Bureau, Ministry of Justice. In addition, the trust enterprise should retain the fax reply.

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

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

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

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

A trust enterprise should record the result of monitoring of accounts or transactions and keep such record in accordance with the requirements of Article 13.

Article 10

A trust enterprise should adopt the following measures in accordance with Article 7 of the Counter-Terrorism Financing Act with respect to places where property or property interests of the designated party is located.

I. After learning of the case, the unit-in-charge at the head office shall submit the report for approval by the appointed chief compliance officer mentioned in the preceding article, and then promptly file the report with the Investigation Bureau, Ministry of Justice (referred to as the "MJIB" hereunder) in the format and manner prescribed by the MJIB after. The report shall be filed within two (2) business days following the date of approval.

II. In the event of an obviously significant and urgent case, the financial institution should make a report to the MJIB as soon as possible by fax or by other available means and afterwards submit a make-up report in a format (downloaded from the website of MJIB) and manner prescribed by the MJIB. A make-up report is not required if the MJIB has confirmed the receipt of the report by sending a reply in a prescribed format by fax. The trust enterprise should maintain the faxed reply from the MJIB.

III. Trust enterprises shall produce an annual report as of December 31 every year (the "settlement record date"), and the report shall be made in the format determined by the MJIB (downloaded from the website of MJIB). The report shall state, based on Article 7 of the Counter-Terrorism Financing Act, all properties or property interests of designated sanctioned individuals, legal entities or groups managed or held by the trust enterprise as of the settlement record date and

the report shall be submitted to the MJIB for reference before March 31 the following year.

The reporting records, transaction documents and annual reports mentioned in the preceding paragraph shall be maintained in their original forms for five (5) years.

Article 11

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

Article 12

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

I. The trust enterprise should verify customer identity and retain relevant documentation.

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

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

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

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

III. Except for the situations described in paragraph 2, the trust enterprise should report such transactions within 5 business days after the completion of transactions in the way of media

reporting (please download the format on the website of the Investigation of Bureau, Ministry of Justice) to the Investigation of Bureau, Ministry of Justice. In case where the trust enterprise fails to complete media reporting with a justified reason, it may submit a hard copy of the report after obtaining the approval from the Investigation of Bureau, Ministry of Justice.

IV. The trust enterprise should retain the reporting data and relevant documentations submitted to the Investigation of Bureau, Ministry of Justice in accordance with the requirements of Article 13.

For government agencies, public institutions, institutions exercising public power (within the scope of the trusteeship), other financial institutions, public and private schools, public utilities, and funds setup by governments, when the trust is setup according to the regulations or as a result of a contractual relationship, a trust fund exceeding a certain amount of currency transactions is exempted from being reported to the Investigation Bureau, Ministry of Justice, but the identity of the customer should still be confirmed and the relevant records and vouchers should be reserved.

For the transactions described in the preceding paragraph that are exempted from being reported, in a case where a suspicious ML/TF transaction is identified, the trust enterprise should remain subject to the requirements of Article 10 of Money Laundering Control Act and paragraph 3 of Article 7 of Counter-Terrorism Financing Act.

Article 13

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

I. The trust enterprise should maintain, for at least five years, all necessary records on transactions, both domestic and international. However in case where laws otherwise provide a longer period for record-keeping, the trust enterprise should comply with such laws. The aforementioned necessary records include:
   (i) The name, or account number or identifier of each party involved in a transaction.
   (ii) Date of transaction.
   (iii) Currency and amount of transaction.
   (iv) The way funds are deposited or withdrew, such as cash, checks, etc.
   (v) Destination of funds.
   (vi) Ways to provide instructions or authorities.

II. For currency transactions above a certain amount, the trust enterprise should keep relevant records on the verification and reporting of such transactions for at least 5 years in the original

manner. For ways to record the information obtained through the CDD procedures, the trust enterprise may determine a way to record such information based on its own consideration and the principle of consistency across the entire trust enterprise.

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

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

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

(ii) Account or contract files.

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

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

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

Article 14

The trust enterprise should deploy adequate and sufficient AML/CFT officers and resources according to its size and risks, etc. The board of directors should appoint a senior officer to serve as the AML/CFT responsible officer, who should be sufficiently authorized to coordinate and supervise AML/CFT affairs, and ensure such officers and responsible officer do not take other responsibilities which conflict with their AML/CFT responsibilities. In addition, domestic banks engaging in trust enterprise should establish an independent AML/CFT responsible unit under the chief executive officer, head office compliance unit, or risk management unit. If a trust enterprise does not have a responsible unit designated, the responsible unit specified in this Template should be responsible for such matters and the responsible supervisor should be responsible for management.

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

I. Supervising the planning and implementation of policies and procedures for identifying,

assessing and monitoring ML/TF risks.

II. Coordinating and supervising the implementation of the trust enterprise-wide ML/TF risk identification and assessment.
III. Monitoring risks related to ML/TF.
IV. Developing AML/CFT programs.
V. Coordinating and supervising the implementation of AML/CFT programs.
VI. Confirming the compliance with relevant AML/CFT regulatory requirements, including relevant Templates or self-regulatory rules established by associations of financial services industry and approved by FSC.
VII. Supervising the reporting of suspicious ML/TF transactions and properties or property interests and locations of designated individuals or entities sanctioned under Counter-Terrorism Financing Act to the Investigation Bureau, Ministry of Justice.

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

A foreign business unit (referred to as the "Foreign Business Unit" hereinafter) of the trust business responsible for trust operation should deploy adequate and sufficient AML/CFT officers by taking into account the number of local branches, size of business, risks, etc. and appoint a head responsible person for supervising AML/CFT affairs.

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

Article 15

A domestic and foreign business unit of a trust enterprise responsible for trust business should appoint a senior officer to serve as a supervisory officer responsible for supervising the implementation of AML/CFT and the implementation of self-inspection pursuant to the relevant requirements of the "Implementation Rules of Internal Audit and Internal Control System of

Financial Holding Companies and Banking Industries" of the business unit.

The internal audit unit of a trust enterprise should audit and provide auditor opinion on following matters in accordance with the "Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries":

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

Responsibilities of internal audit unit:

I. Determining the matters subject to audit according to internal control measures and relevant regulations, conducting periodic audit, and testing the effectiveness of AML/CFT programs and risk management quality of operations, departments and branches.
II. The auditing method should cover independent transaction testing, including selecting transactions related to high-risk products, customers, and geographic areas to verify the trust enterprise has effectively implemented relevant AML/CFT regulatory requirements.
III. In case where any deficiency in the implementation of specific management measures is identified, internal audit unit should periodically report to AML/CFT responsible officer for review and provide such information as a reference of employee training.
IV. In case where internal audit unit identifies any intentional disguise of significant non-compliance but fails to disclose such information, the competent unit in the head office should take appropriate actions.

A trust enterprise's chief executive officer should supervise each unit to the extent that the implementation of AML/CFT internal control system is assessed and reviewed by each unit in a prudent manner. The chairman, chief executive officer, chief auditor, and AML/CFT responsible officer should jointly issue a statement for AML/CFT internal control system and submit to board of directors for approval. Within 3 months after the end of each fiscal year, the trust enterprise should disclose the statement on its website and publish the statement through a website designated by FSC. For a Taiwan branch of a foreign bank engaging in trust enterprise, the requirements of the Template regarding to the board of directors or supervisors may be satisfied by persons authorized by the head office. The statement described in last paragraph may be jointly issued by a representative for litigious and non-litigious matters, AML/CFT responsible officer, and a senior auditor responsible for the Taiwan area, etc.

Article 16

A trust enterprise should establish prudent and appropriate procedures for screening and hiring employees, including reviewing whether a candidate has decent personality and professional knowledge required for the job.

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

I. Having at least 3-year experience as a compliance officer or AML/CFT officer.
II. Attending at least 12-hour training classes provided by an institution recognized by FSC and obtaining the certificate of completion after passing an exam.
III. For a person who has been qualified for a compliance officer, however, may be treated as meeting the qualification requirement provided in subparagraph II after attending 12-hour AML/CFT training classes.

The trust enterprise's AML/CFT responsible officer, AML/CFT officers, and domestic business unit supervisory officers should attend at least 12-hour AML/CFT trainings each year provided by the trust enterprise or external training institutions agreed by AML/CFT officer described in paragraph 1 of Article 14. Such trainings should at least cover new updates on regulatory requirements, and ML/TF trends and red flags. Those who obtain domestic or international AML/CFT professional certificates issued by an institution recognized by FSC may be exempt from satisfying the requirements on training hour for the same year.

The trust enterprise's foreign business unit supervisory officer and AML/CFT head and officers should have AML expertise, be familiar with local regulatory requirements, and attend 12-hour AML/CFT trainings provided by local competent authorities or relevant institutions. In case where local competent authorities or relevant institutions do not provide AML/CFT trainings, such persons may attend the trainings provided by the trust enterprise or external training institutions agreed by AML/CFT responsible officer described in paragraph 1 of Article 14.

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

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

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

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

I. Employees identify suspicious ML/TF transactions and report such transactions in accordance with relevant AML regulatory requirements to the extent that they contribute to the prevention or investigation of criminal activities.
II. Employees attend domestic or foreign AML/CFT seminars with outstanding performance, or collect foreign regulatory requirements and provide materials that are valuable to the trust enterprise's AML/CFT activities.

A trust enterprise may take following measures to conduct orientations and trainings:

I. Orientations: a trust enterprise should arrange orientations to include at least certain-hour training classes on AML/CFT regulatory requirements and legal responsibilities of employees of financial services industry to allow new employees to understand relevant regulatory requirements and responsibilities.
II. Trainings:
    (i) Initial trainings on regulatory requirements: after Money Laundering Control Act and Counter-Terrorism Financing Act enter into force or get amended, the trust enterprise should conduct trainings on such regulatory requirements for employees within a shortest period to introduce Money Laundering Control Act, Counter-Terrorism Financing Act, and relevant regulatory requirements, and explain the trust enterprise's relevant measures in response to those changes. AML/CFT responsible unit should be responsible for planning such trainings and having employee training unit implement the trainings.
    (ii) Regular trainings:
        1. Each year employee training unit should periodically conduct relevant trainings for employees to learn, in order to strengthen the judgment of employees, implement AML/CFT functions, and prevent employees from non-compliance. Such trainings may be arranged into other professional trainings to include appropriate relevant classes.

2. The trainings may be instructed by employees trained by the trust enterprise. In addition, the trust enterprise may invite scholars or experts as instructors if necessary.
3. To allow employees to sufficiently understand the characteristics and types of ML/TF in order to facilitate the identification of suspicious ML/TF transactions, the trainings should be supplemented by real cases in addition to the introduction of relevant regulatory requirements.
4. AML/CFT responsible unit should periodically understand an employee's attendance in trainings. For an employee who never attends, AML/CFT responsible unit should urge the employee to attend relevant trainings if necessary.
5. In addition to internal on-the-job training, the trust enterprise may select employees to attend training provided by external training institutions.

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

Article 17

In case where customers meet one of the following descriptions, a trust enterprise's employees should decline their requests in a euphemistic manner and report to direct managers.

I. Insisting not to provide relevant data for identity verification when being told it is necessary according to regulatory requirements.
II. Any individuals or entities compel or attempt to compel trust enterprise employees not leave transaction records or complete reporting form.
III. Attempting to persuade employees not to collect data that is required to complete the transaction.
IV. Enquiring the possibility of avoiding being reported.
V. Eager to explain the source of fund is clean or the transaction is not for money laundering purpose.
VI. Insisting transactions must be completed immediately without a reasonable explanation.
VII. Descriptions provided by the customers apparently do no match the transactions.
VIII. Attempting to provide interest to employees to obtain the trust enterprise's services.

Article 18

Trust enterprises in the event that the FSC or authorized the entrusted institution investigation

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

Article 19

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

Guidelines for Trust Enterprises Regarding Assessment of Money Laundering and Terrorism Financing Risks and Adoption of Prevention Programs

I. These Guidelines are established in accordance with "Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated by the Financial Supervisory Commission" for the purpose of anti-money laundering and countering terrorism financing (AML/CFT) to cover how trust enterprise identify and assess money laundering and terrorist financing (ML/TF) risk in businesses and establish AML/CFT programs, etc., as a basis for implementation.

II. A trust enterprise's internal control system and its amendment should be approved by the Board of Directors. In addition, the internal control system should include relevant written policies and procedures for identifying, assessing and managing ML/TF risks, AML/CFT programs based on risk assessment results, and the periodic review of such policies, and procedures and programs.

The purpose of a risk-based approach is to help a trust enterprise develop prevention and mitigation measures that are commensurate with the ML/TF risks identified, determine the allocation of resources on AML/CFT, establish internal control system, and establish and implement policies, procedures and measures that are necessary in AML/CFT programs.

The trust business is diversified, such as money trust business, securities trust business, real estate trust business, and other ancillary businesses, etc. Therefore the ML/TF risks associated with each business are different. A trust enterprise should take such business diversity into account when assessing and mitigating ML/TF risks.

The examples provided in the Guidelines are not mandatory requirements. A trust enterprise's risk assessment mechanism should be commensurate with its business nature and scale. For a trust enterprise that is relatively small or has relatively simple businesses, a simple risk assessment is sufficient. For a trust enterprise that provides relatively complex products and services, has multiple branches (or subsidiaries) (referred to as the "branches" hereinafter) providing diversified products, or has diversified customer groups, however, is required to perform a relatively sophisticated risk assessment.

III. A trust enterprise should take appropriate measures to identify and assess its ML/TF risks, and determine specific risk categories based on the risk identified, in order to further control, mitigate or prevent such risks.

Such specific risk category should cover at least geographic areas, customers, and products, services, transactions or delivery channels, etc. A trust enterprise should further analyze each risk category to determine detailed risk factors.

(i) Geographic risk:

1. A trust enterprise should identify geographic areas that are exposed to higher ML/TF risks.

2. When building up a list of high-risk areas, a trust enterprise may determine appropriate risk factors based on the practices of branches and its needs.

(ii) Customer risk:

1. A trust enterprise should take an overall account of a customer's background, occupation, characteristics of social and economic activities, geographic areas, and an entity customer's organization type and structure, etc., to identify the customer's ML/TF risks.

2. When identifying a customer's risk and determine the customer's level of risk, a trust enterprise may perform risk assessment based on following risk factors:

(1) Geographic risk of the customer: Determine the level of risk of the customer's nationality and country of residence based on a list of areas that are exposed to ML/TF risks defined by the trust business.

(2) Occupation and industry risk of the customer: Determine the level of risk of the customer's occupation and industry based on a list of occupations and industries that are exposed to money laundering risks defined by the trust business. High-risk industries include, for example, cash-intensive businesses, or companies or trusts that tend to be used as personal asset-holding vehicles, etc.

(3) Individual customer's employer.

(4) The channel used by the customer to sign a contract and establish business relation.

(5) The transaction amount with which the customer first establishes business relation.

(6) Products or services that the customer applies.

(7) Whether the customer has other high ML/TF risk characteristics. For example, the customer fails to provide a reasonable explanation regarding the significant geographic distance between the customer and the branches; the customer has nominee shareholders or shares in bearer form; the extent of complexity in an entity customer's ownership structure, such as, whether the ownership structure is apparently unusual or excessively complex given the nature of the customer's business.

(iii) Product, service, transaction or delivery channel risk:

1. A trust enterprise should identify products, services, transactions or delivery channels that have higher ML/TF risk based on the nature of individual product, service, transaction, or delivery channel.

2. A trust enterprise should, before launching a new product, service or business (including new payment method, applying new technology on existing or new product or service), perform ML/TF risk assessment and establish relevant risk management measures to mitigate the risks identified.

3. Examples of individual product, service, transaction, or delivery channel risk factors are as follows:

(1) The extent of associating with cash.

(2) The channel to establish business relation or process transaction, including whether it allows non-face-to-face transactions, and whether it is a new payment method such as electronic banking.

(3) Whether it allows high amount of money or value transfer.

(4) Anonymous transactions.

(5) Payment received from unknown or un-associated third parties.

IV. A trust enterprise should establish multiple levels of customer risk and rules to determine the level of customer risk.

Customer risk should have at least two levels, "high-risk" and "general risk", as bases to determine the extent of customer due diligence and ongoing monitoring. For a trust enterprise that adopts only two risk levels, the trust business should not take simplified measures to a customer rated as "general risk" because "general risk" is still higher than "low risk" provided in Paragraph V and VII of the Guidelines.

A trust enterprise should not disclose a customer's level of risk to the customer or any person that is unrelated to AML/CFT obligations.

V. A trust enterprise should directly treat foreign political exposed persons, terrorists or terrorist groups that are sanctioned, identified or investigated by foreign governments or international AML organizations, and designated individuals or entities sanctioned under Counter-Terrorism Financing Act as high-risk customers. In addition, a trust enterprise may determine the types of customers that should be directly treated as high-risk customers based on its business type and relevant risk factors.

A trust enterprise may, based on the results of an overall written risk analysis, define the types of customers that can be treated as low-risk customers. The results of the written risk analysis should be sufficient to explain that such types of customers are commensurate with lower risk factors.

VI. With respect to a new customer to establish business relation with a trust enterprise, a trust enterprise should determine the customer's level of risk when establishing business relation.

With respect to an existing customer with a specific level of risk, a trust enterprise should re-assess customer risk in accordance with its risk assessment policies and procedures.

Although a trust enterprise performs customer risk assessment when establishing business relation with a customer, for certain customers, the overall risk profile become clear after the customers use accounts to transact. Therefore, a trust enterprise should conduct due diligence to existing customers on the basis of materiality and risk, and, at appropriate times, review the existing business relationships and adjust the level of risk after taking into account the time and information sufficiency of last due diligence. Such appropriate times should at least include:

(i) When the customer's supplement contract has a significant impact or is establishing a new business relation.

(ii) Time to conduct periodic review determined on the basis of the customer's materiality and risk.

(iii) When a trust enterprise knows a material change occurs in the customer's identification and background information.

(iv) When the trust business reports a suspicious ML/TF transaction or other events that may result in substantial change in customer risk profile occur.

A trust enterprise should review periodically the sufficiency of the information for identifying customers and beneficial owners, and ensure the update of such information. Especially, high-risk customers should be reviewed at least annually by the trust business.

VII. A trust enterprise should establish control measures according to the risks identified to mitigate or prevent such money laundering risk. A trust enterprise should determine appropriate control measures according to a customer's level of risk.

With respect to such control measures, a trust enterprise should take different measures to a high-risk customer and a customer with a specific high-risk factor to effectively manage and mitigate identified risks. Following are examples:

(i) Conduct enhanced due diligence, such as:

1. Obtaining relevant information on the purpose of having a contract signed and its purpose: the expected use of the account (for example, the amount, purpose and frequency of expected transactions)

2. Obtaining information on an individual customer's source of wealth, source and destination of funds, and types and quantities of assets, etc. If the source of funds is deposit, a trust enterprise should further understand the source of such deposit.

3. Obtaining an entity customer's further business information: understand the customer's latest financial situation, commercial activities and business relationship information to establish the source of assets, source of funds and destination of funds.

4. Obtaining information on the reason for intended or performed transactions.

5. Conducting site visit or phone interview, according to customer type, to validate a customer's operation situation.

(ii) Obtain the approval of senior management, defined by the trust business considering

internal risks, before first establishing a business relation or establishing a new business relation.

(iii) Increase the frequency of customer due diligence.

(iv) Conduct enhanced ongoing monitoring of the business relationship.

Except in the situation described in Subparagraph 1 of Paragraph 3 of Article 6 of the Template, a trust enterprise may take simplified measures in a lower risk situation in accordance with its risk prevention policies and procedures. Such simplified measures should be commensurate with the lower-risk factors. Examples of simplified measures that may be applied include:

(i) Reducing the frequency of updates of customer identification information.

(ii) Reducing the degree of ongoing monitoring and scrutinizing transactions based on a reasonable monetary threshold.

(iii) Exempting from collecting specific information or conducting specific measures as to the purpose and nature of business relations if a trust enterprise may infer this from the type of transactions or business relations.

VIII. A trust enterprise should establish a mechanism of periodic enterprise-wide ML/TF risk assessment and generate a risk assessment report to enable senior management to timely and effectively understand the trust business's overall ML/TF risks, determine necessary mechanisms to be established, and develop appropriate mitigation measures.

A trust enterprise should establish a mechanism of periodic enterprise-wide ML/TF risks assessment based on following risk factors:

(i) The nature, scale, diversity and complexity of businesses.

(ii) Target markets.

(iii) Volumes and sizes of trust business transactions: considering the usual transaction activities of the trust business and characteristics of its customers.

(iv) Management data and reports related to high risk: such as the number and proportion of high-risk customers; the amount, volume or proportion of high-risk products, services or transactions; the amount or proportion of customer's nationality, place of registration or

operation, or transactions that involve high-risk areas.

(v) Businesses and products, including the channels and manners that a trust enterprise uses to provides customers businesses and products, and the way to conduct customer due diligence, such as the extent of using information system and whether relying on third parties to perform due diligence.

(vi) The examination results of internal auditors and supervisory authorities.

When a trust enterprise performs the enterprise-wide ML/TF risk assessment described in last paragraph, in addition to taking into account such risk factors, it is suggested to supplement the assessment with other information obtained from internal or external sources, such as:

(i) Management reports provided by the trust business's management (such as head of business unit, relationship managers, etc.)

(ii) Relevant AML/CFT reports published by international anti-money laundering organizations and other countries.

(iii) Information of ML/TF risk released by the Competent Authorities.

A trust enterprise's enterprise-wide ML/TF risk assessment results should be used as a basis to develop AML/CFT programs. A trust enterprise should allocate appropriate headcounts and resources based on such results and take effective countermeasures to prevent or mitigate risks.

If a material change occurs to a trust enterprise, such as a material incident, material development in management and operation, or relevant new threats, a trust enterprise should re-perform the assessment.

A trust enterprise should file a risk assessment report to the Financial Supervisory Commission when it is completed or updated.

Annex: Red Flags for Transactions Suspected to Involve Money Laundering or Terrorism Financing

1. Products / Services – Trust account
   (1) The aggregation of cash deposited in and out of a trust account, or the aggregation of cash withdrawn from an account, reaches a specific amount within a certain period.
   (2) The aggregation of cash deposited in and out of a customer's trust account, or the aggregation of cash withdrawn from a customer's account, reaches a specific amount within a certain period.
   (3) The transaction of cash deposited or withdrawn by a customer for an amount slightly below the currency reporting threshold and each transaction of cash deposited or withdrawn reaches a specific amount within a certain period.
   (4) A customer's account suddenly has funds entrusted that cumulatively reach a specific amount.
   (5) An inactive trust account suddenly has deposits that accumulatively reach a specific amount and are transferred rapidly.
   (6) Multiple deposit transactions are made into the trust account for up to a certain amount or for a certain number of transactions, and then they are promptly transferred with the account closed immediately.
   (7) A customer frequently transfers funds that accumulatively reach a specific amount between related trust accounts.
   (8) A customer frequently requests to have transactions processed in the form of cash.
   (9) A customer frequently deposits cash on behalf of another person or a trust account frequently has cash deposited by a third party to the extent that such transactions cumulatively reach a specific amount.
   (10) A customer requests to have evidence issued for several transactions with cash at one time that cumulatively reaches a specific amount.
   (11) The funds remitted from or to high ML/TF risk jurisdictions accumulatively reach a specific amount. The high ML/TF risk jurisdictions described in the Template include but are not limited to the jurisdictions, published by international anti-money laundering organizations and notified by Financial Supervisory Commission ("FSC"), that have serious deficiencies in AML/CFT, and other jurisdictions that fail to comply with or completely comply with the recommendations of such organizations.

2. Products / Services – Trust structure
   (1) Customers do not have a compelling reason, purpose, or motivation to have a trust

account setup.

(2) The trust structure of the customer or the arrangement of the related transactions by the customer has caused doubts about the trust's purpose and intention.

3. Unusual Transaction Activity / Behavior – Transaction Behavior

(1) The trust conducted by an individual involved in a special and material case that is instantly reported on television, in the press, on the internet, or other media is apparently unusual.

(2) Customers purchase trust products in cash on separate occasions in a short period of time and then return them in a lump sum or purchase trust products collectively and then return them on separate occasions in a manner that is inconsistent with their identity, financial status, and business operations.

(3) Customers who come from high-risk countries or regions where money laundering or terrorism financing risk is high purchase trust products in cash frequently in a short period of time.

(4) Trust funds are used for some unusual business transactions or other financial activities.

(5) Customers, after signing a trust contract, have it terminated immediately within a short period of time and without legitimate reasons.

(6) Other obviously abnormal trading behaviors.

4. Unusual Transaction Activity / Behavior – Customer identification information

(1) A customer has faced the circumstances specified in the “Template for Guidelines Governing Anti-Money Laundering and Countering Terrorism Financing of Trust Enterprises” or others situations that have resulted in the incompletion of the customer identification process.

(2) A large number of customers share the same address, occupants of an address change frequently, or the address is not the actual residence address.

(3) The customers or their trust related parties try to evade contact.

(4) The trust condition or transaction has an illegal purpose or is inconsistent with the known customer wealth source, the purpose of establishing the trust account, and the intended content.

5. Terrorism Financing

Related parties of a transaction are terrorists or terrorist groups designated by foreign governments and notified by FSC, or terrorist groups identified or investigated by an international organization; or the fund for a transaction seems to, or is reasonably suspected to,

have a connection with terrorism activities, groups, or terrorism financing.