King's Town Bank Directions Governing Anti-Money Laundering and Countering-Terrorism Financing

Article 1

The Directions are formulated in accordance with “Money Laundering Control Act,” “Terrorism Financing Prevention 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

The Bank formulated the internal control policy for anti-money laundering and countering-terrorism financing (AML/CTF) in accordance with Article 6 of the “Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated by the Financial Supervisory Commission.” The internal policy and any amendments thereafter shall become effective upon resolution at the board meeting. The content shall include the following information:

I. Policies and procedures for identifying, assessing, and managing money laundering and terrorism financing (ML/TF) risks established in accordance with the “Guidelines Governing Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program Development by the Banking Sector” (hereinafter referred to as “the Guidelines”).

II. An AML/CTF plan was established based on the Guidelines, the results of risk assessment, and the business scale to manage and mitigate the

identified risks, including enhanced control measures for higher-risk situations.

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

The identification, assessment, and management of the AM/TF risks, as mentioned in Subparagraph 1 of the preceding paragraph, shall cover at least the aspects of customers, geography, products and services, transactions, or payment channels, and shall be handled in accordance with the following provisions:

I. A risk assessment report shall be produced.

II. All risk factors shall be considered to determine the overall risk level and appropriate measures to reduce the risk.

III. A mechanism for updating risk assessment reports shall be established to ensure the risk information is up-to-date.

IV. The risk assessment report shall be sent to the Financial Supervisory Commission (hereinafter referred to as FSC) for reference when the report is completed or updated.

The AML/CTF plan, as mentioned in Subparagraph 2 of Paragraph 1, shall include the following policies, procedures, and control mechanisms:

I. Customer identity verification.

II. Checking of names of customers and trading counterparties.

III. Ongoing monitoring of accounts and transactions.

IV. Correspondent banking business.

V. Recordkeeping.

VI. Reporting of currency delivery above a certain amount.

VIII. Reporting of suspicious money laundering or terrorism financing transactions in accordance with the Counter-Terrorism Financing Act.

VIII. Appointment of AML/CTF Officers.

IX. Employee screening and hiring procedures.

X. Continuous employee training programs.

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

XII. Other matters required by the AML/CTF regulations and FSC.

The Bank shall establish a group-level AML/CTF plan, which shall be implemented across subsidiaries within the Group. The program shall include the policies, procedures, and control measures mentioned in the preceding paragraph as well as the following particulars without violating the information confidentiality regulations of the R.O.C. and host countries of the Bank's overseas subsidiaries:

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

II. With the aim of AML/CTF, the Bank may request subsidiaries to provide information on customers, accounts, and transactions based on the group-level AML/CTF plan when necessary, and such information shall include abnormal transactions or activity information and analysis thereof. When necessary, the said information may be obtained by subsidiaries through the Group management function.

III. Security protection of the use of exchanged information and its confidentiality, including security protection to prevent data leakage.

The Board of Directors of the Bank is ultimately responsible for ensuring the establishment and maintenance of appropriate and effective internal control of AML/CTF. The Board of Directors and senior management shall understand its ML/TF risks and the operation of the AML/CTF plan, as well as adopt measures to create a culture that focuses on AML/CTF.

Article 3

The terms referred to in the Directions are defined as follows:

I. "A certain amount" refers to NT$500,000 (or an equivalent amount in

foreign currencies).

II. “Cash transaction” refers to cash receipt or payment in a single transaction (including all transactions recorded on cash deposit or withdrawal vouchers for accounting purposes) or currency exchange transactions.

III. “Establishing business relationships” refers to the request from an individual for the Bank to provide financial service, and to establish a business relationship over a period of time, or when the individual contacts the Bank for the first time as a potential customer and request to establish a business relationship over a period of time.

IV. “Customers” refers to persons (including natural persons, legal persons, organizations, or trust) that establish a business relationship with the Bank or those that carry out occasional transactions approved by the Bank. Customers usually do not include a third party in a certain transaction. For example, in outward telegraphic transfer, the Bank does consider the beneficiary to be a customer.

V. “Occasional transactions” refers to transactions (including cash remittance, change of banknote) conducted by the public with a bank with which they do not have a business relationship.

VI. “Beneficial owner” refers to a natural person who has ultimate ownership or control over the customer, or a natural person who engages in transactions through persons acting on his/her behalf, including a natural person who has ultimate effective control over a legal entity or legal agreement.

VII. “Risk-based approach” refers to the approach adopted by the Bank to identify, assess, and understand the exposed risks of ML/TF, and take appropriate AML/CTF measures to effectively reduce such risks. With such an approach, the Bank shall 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 risks of ML/TF in the most appropriate and effective way.

VIII. “Transaction-related party” refers to any third party other than the Bank's customer involved in the transaction process. For example, the beneficiaries of outward remittances or the remitters of inward remittances.

Article 4

Customer identity verification measures shall be conducted in accordance with the following provisions:

I. The establishment of a business relationship or a transaction shall be denied if any of the following circumstances are identified:

(1) Where the customer is suspected of using an anonymous account, an account in a fictitious name, someone else's name, a shell entity, or a shell corporation.

(II) Where the customer refuses to provide documents relating to customer identity verification measures unless the customer's identity has been verified by a reliable and independent source.

(III) Where a proxy acts on behalf of the customer and there are difficulties in checking and verifying the veracity of the agency and identity-related information.

(IV) Where the customer uses forged or altered identification certificates.

(V) Where the customer presents only photocopies of identification documents. Nevertheless, it shall not apply to businesses that can be conducted using identity document copies or image files supplemented by other control measures in accordance with the regulations.

(VI) Where documents provided are suspicious, illegible, or the customer is unwilling to provide other supporting information or the documents provided cannot be verified.

(VII) Where the customer procrastinates in providing identification documents in an unusual manner.

(VIII) Where the customer is an individual, legal entity, or a group that is subject to designated sanctions by the Counter-Terrorism Financing Act, or terrorists or terrorist groups identified or investigated by foreign governments or international organizations. However, this shall not subject to payments made under Subparagraph 1 to 3 Paragraph 1 Article 6 of the Counter-Terrorism Financing Act.

(IX) Where other unusual circumstances exist in the process of establishing a business relationship and the customer fails to provide reasonable explanations.

II. Timing of customer identity verification:

(I) When establishing business relationships with clients.

(II) When carrying out occasional transactions with respect to:

1. Cash transactions above a certain amount. The same shall apply for multiple cash transactions that are obviously related and the total is above a certain amount.
2. Cross-border remittances above NT$30,000 (or an equivalent amount in foreign currency).

(III) Suspicion of ML/TF.

(IV) Doubts about the veracity and adequacy of previously obtained information on a customer's identity.

III. Measures to be taken to verify a customer's identity:

(I) The customer's identity shall be identified and verified based on documents, materials, or information from reliable and independent sources, and a copy of the identity document shall be kept for record.

(II) For the business relationship or transaction established by an agent, the facts of the agency shall be verified, and the agent's identity shall be identified and verified according to the method in the preceding subparagraph, and a copy of the identity

document shall be kept for record.

(III) The customer's substantial beneficial owner shall be identified and his/her identity shall be verified with reasonable measures, including the use of materials, or information from reliable sources.

(IV) The customer identity verification measures shall include understanding the purpose and nature of the business relationship and obtaining relevant information depending on the situation.

IV. Under the preceding subparagraph, when the customer is an individual, at least the following information shall be obtained to identify the identity:

(I) Name.

(II) Date of birth.

(III) Household registration or residential address.

(IV) Official identification document number.

(V) Nationality.

(VI) Purpose of residence or transaction for foreigners (such as sightseeing and work).

V. For individual customers who are rated as high risk or with specific high-risk factors based on the Bank's ML/TF assessment, at least one of the following information shall be obtained when establishing a business relationship:

(I) Names or aliases used in the past: Names used in the past include names used before marriage and names used before name changes.

(II) Office address, P.O. Box address, email address (if any).

(III) Telephone or mobile phone number.

VI. Under subparagraph 3, when the customer is a party entrusted by a legal entity, group, or trustee of a trust, the Bank shall understand the nature of the customer's business or trust (including legal agreements that are similar to trust) and obtain at least the following information about the

customer or trust to identify and verify the customer's identity:

(I) Name, legal form, and proof of the existence of customer or trust.

(II) Charters of a legal entity, group, or trust, or similar documents of power. Provided, this shall not apply to the following circumstances:

1. The parties listed in Item 3 of Subparagraph 7, and not endorsed under Subparagraph 3 of Paragraph 1 of Article 6.
2. A group customer has been confirmed that it has not established a charter or similar documents of power.

(III) The information of senior management (including directors, supervisors, general manager, chief financial officer, representatives, managers, partners, persons authorized to sign and seal, natural persons equivalent to the aforementioned senior management personnel, or other personnel fall in the scope under the Bank's risk-based approach) in a legal person, an organization or a trustee:

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

(IV) Official identification number, such as tax ID number, tax serial number, or registration number.

(V) The registered office address of the legal entity, group, or trustee of a trust, and the address of its principal place of business.

(VI) The purpose of the correspondence for the legal entity, group, or trustee of a trust.

VII. Under the provision of Item 3 of Subparagraph 3, when the customer is a trustee of a legal entity, group, or trustee of a trust, the ownership and control structure of the customer or trust shall be understood, and the customer's beneficial owner shall be identified based on the following information, and reasonable measures shall be taken for verification.

(I) When the customer is a legal entity or group:

1. The identity (such as name, date of birth, nationality, and identification document number) of the natural person who has the ultimate controlling interest in a corporation. The term “controlling interest” shall refer to the directly or indirectly holding of more than 25% of the legal entity's shares or capital. The Bank may require the customer to provide a register of shareholders or other documents to assist in the identification.
2. If a natural person with a controlling interest is not identified in line with the preceding item, or when there are doubts as to whether the person with a controlling interest is the beneficial owner, the Bank shall identify the natural person who exercises control over the customer through other means. If necessary, the Bank may require a declaration from the customer to verify the beneficial owner's identity.
3. If no natural person with a controlling interest is identified under the preceding two items, the Bank shall identify the senior management personnel's identity.

(II) When the customer is a trustee: The identity of the settlor(s), the trustee(s), the trust supervisor, the beneficiaries, and any other person holding ultimate effective control over the trust, or the identity of persons in equivalent or similar positions.

(III) When the customer or the person with a controlling interest belongs to any of the following categories, the provision of identification and verification of the beneficial owner's identity set out in Item 3 of Subparagraph 3 does not apply, unless endorsed under Subparagraph 3 of Paragraph 1 of Article 6 or the fact that bearer shares have been issued:

1. An R.O.C government agency.

2. An enterprise owned by the R.O.C. government.
3. A foreign government agency.
4. An R.O.C. public company or its subsidiaries.
5. A company listed in other jurisdictions where it is required to disclose majority shareholders, and the subsidiaries of such company.
6. A financial institution supervised by the R.O.C. government, and investment vehicles managed by such institution.
7. A financial institution incorporated or established outside the R.O.C. that is subject to and supervised for compliance with the requirements for AML/CTF in line with the standards set by the Financial Action Task Force on Money Laundering (FATF), and investment vehicles managed by such institution. Relevant certifying documents of the said financial institution and its investment vehicles (such as public information regarding audit records, regulations, and articles with respect to anti-money laundering, inquiry history of negative information records, and statements of declaration) shall be kept by the Bank.
8. A fund administered by a R.O.C. government entity;
9. An employee stock ownership trust or an employee savings trust.

VIII. For the customer who has established a business relationship with the Bank, the method of verifying the customer's and beneficial owner's identities:

(I) Verification with documents:

1. Individuals:

(1)Verify identity or date of birth: Valid official identification photo documents, such as ID card, passport, residence permit, or driver's license. When there is a doubt about

the validity of the aforementioned documents, a notary's certification or an embassy's declaration shall be obtained. In addition, the Bank may verify the aforementioned information of the beneficial owner without the original copy or request the legal entity, or group and its representatives to declare the information on the beneficial owner according to the Bank's internal operating procedures. However, the part of the declaration information shall be able to be verified by other credible documents or sources of information, such as company registration documents or company annual reports.

(2) Address verification: The customer's bills, bank statements, or officially issued documents.

2. Legal entity, group, or trustee of a trust: Certified articles of incorporation, business license issued by the government, partnership agreement, trust instrument, certification of incumbency, etc. If the trustee of a trust is a trust managed by a financial institution listed in Paragraph 1 of Article 5 of the Money Laundering Control Act, relevant trust documents may be replaced by a written certificate issued by the financial institution; however, this does not apply to the financial institution that is located in the country or region that is endorsed under Subparagraph 3 of Paragraph 1 of Article 6.

(II) Where necessary, the verification can be performed with undocumented information such as:

1. Communication with the customer via telephone or mail after the account is opened.
2. Information provided by other financial institutions.

3. Cross-referencing information provided by the customer with public information from other reliable sources or paid databases.

IX. For customers of the Bank who are rated as high risk or with specific high-risk factors based on the Bank's ML/TF assessment shall be verified in an enhanced manner, for example:

(I) Obtain a reply letter which is sent to the address provided by the customer and is personally signed by the customer, legal entity, or group, or make telephone inquiries.

(II) Obtain the supporting documents for the source of personal wealth and funds.

(III) Obtain the supporting documents regarding the source and flows of funds of a legal entity, group, or trustee of a trust. For example, the list of major suppliers and the list of major customers.

(IV) On-site visits.

(V) Obtain transaction history at previous banks and check the transactions with the banks.

X. Before completing the customer identity verification, no business relationship or occasional transaction may not be established with the customer. However, the Bank may first obtain information on the identity of the customer and any beneficial owner, establish a business relationship, and then complete the verification, provided that:

(I) ML/TF risks are effectively managed, including adopting risk management procedures with respect to the conditions under which a customer may utilize the business relationship to complete a transaction prior to verification.

(II) It shall be essential not to interrupt the normal conduct of business with the customer.

(III) Verification of the identities of the customer and the beneficial owner will be completed as soon as reasonably practicable. The

Company shall terminate the business relationship and inform the customer prior to the termination if verification fails to be completed within a reasonable period.

XI. If the Bank allows a customer to establish a business relationship before customer identity verification is completed, relevant risk control measures shall be adopted, including:

(I) The Bank shall determine a deadline for completion of customer identity verification.

(II) Before the completion of identity verification, the supervisory officer of the business units shall examine the transactions with the customers, and report to the senior-level managerial officers regarding the progress of the verification procedure on a regular basis.

(III) The Bank shall restrict the number and types of the customer's transactions before the completion of verification.

(IV) The customer shall be prohibited from outward transfers to a third party before the completion of verification, unless:

1. There are no suspected ML/TF activities.
2. The customer is classified as low ML/TF risk level.
3. The Bank shall obtain approval from high-level management at a level of approval authorization determined by internal risk considerations.
4. The name of the beneficiary is not on the ML/TF name list.

(V) The preceding item shall not be applicable if there is doubt regarding the veracity and adequacy of previously obtained information on a customer's or the beneficial owner’s identity.

(VI) The term “reasonable period” stated in Item 3 of the preceding subparagraph shall be determined accordingly based on the risk-based approach. Examples are as follows:

1. The verification process of the customers’ identity shall be

completed no later than 30 working days after the establishment of the business relationship.

2. If the verification process is uncompleted after 30 days from the establishment of the business relationship, the Bank shall terminate the business relationship with the customer, and prevent any further transaction (except when it is feasible to return the funds to their original source).
3. If the verification process is uncompleted after 120 days from the establishment of the business relationship, the Bank shall terminate the business relationship with the customer.

XII. When the customer is a legal entity, the articles of incorporation shall be reviewed, or the customer shall be required to submit a declaration to examine if it can issue bearer shares. In order to ensure the renewal of its beneficial owner, the following measures shall be taken for a customer who has issued bearer shares:

(I) The Bank shall request customers to require its bearer shareholders with controlling interest in the legal entity to register his/her identity with the customer and request the customer to notify the Bank of any changes to the identity of the bearer shareholders with controlling interest.

(II) The Bank shall request the customer to provide the Bank with updated information on its beneficial owners after each shareholders' meeting and provide information on shareholders who hold a certain percentage of bearer shares. However, the customer shall promptly notify the Bank when the customer learns of any changes in the identity of a shareholder who has controlling interests in the legal person based on other reasons.

XIII. The Bank shall utilize appropriate risk management mechanisms to check whether a customer or the customer's beneficial owner or executive is a politically exposed person who is, or has been, entrusted with a prominent

function by a foreign government or an international organization is verified when carrying out the customer' identity verification.

(I) If the customer or its beneficial owner is a politically exposed person currently in a foreign government, the customer shall be directly regarded as a high-risk customer, and the enhanced measures of customer identity verification under Subparagraph 1 of Paragraph 1 of Article 6 shall be adopted.

(II) If the customer or its beneficial owner is a politically exposed person currently in the domestic government or an international organization, the Bank shall assess the risk when establishing a business relationship with the customer, and conduct an annual review thereafter. In the case of higher-risk business relationships, the Bank shall adopt the enhanced measures of customer identity verification under Subparagraph 1 of Paragraph 1 of Article 6.

(III) If a member of the customer's senior management is a politically exposed person currently in the/a domestic/foreign government or an international organization, the Bank shall consider the influence of the senior management member on the customer and decide whether to adopt the enhanced customer identity verification measures under Subparagraph 1 of Paragraph 1 of Article 6 for the customer.

(IV) For non-current politically exposed persons in domestic, foreign government, or international organizations, the Bank shall assess the impact of relevant risk factors and determine whether the risk-based approach applies to the provisions of the preceding three items.

(V) The preceding four items also apply to politically exposed persons' family members and close associates. The scope of the aforementioned family members and close associates shall be determined in accordance with the latter part of the provisions of

Paragraph 4 of Article 7 of the Money Laundering Control Act.

(VI) For the parties listed in Subitems 1 to 3 and Subitem 8 of Item 3 of Subparagraph 7, they shall not be subject to the provisions of Items 1 to 5 of this Subparagraph if their beneficial owners and senior management personnel are politically exposed persons.

XIV. Other points to follow for customer identity verification:

(I) When the Bank establishes a business relationship with a customer or conducts an occasional financial transaction above a certain amount with a customer or there is any doubt about the customer's information that is insufficient to confirm the identity, the customer's identity shall be confirmed and recorded based on the documents issued by the government or other identification documents.

(II) The Bank shall adopt enhanced customer identity verification for discretionary accounts and transactions handled by professional intermediaries.

(III) The Bank shall strengthen inspections on customers who are served by the personal wealth management department of the Bank.

(IV) The Bank shall strengthen inspections on clients blacklisted by other banks for financial dealings.

(V) When conducting non-face-to-face identity verification, the Bank shall utilize procedures that have the same effectiveness as the verification process conducted face-to-face, and shall adopt adequate and sufficient measures to mitigate risks.

(VI) When a business relationship is established through the Internet, the verification shall be conducted in accordance with relevant operational procedures established by The Bankers Association and approved by the competent authority.

(VII) Where a customer entrusts or authorizes another party to

establish a business relationship, or where the Bank discovers suspicion about a customer after the establishment of a business relationship, the Bank shall verify the customer's identity by telephone, mail, or on-site visits.

(VIII) If a business relationship is established by mail, the customer's identity shall be verified by a registered mail after the establishment of a business relationship is completed.

(IX) Provided that it is not in violation of the relevant regulations, if a customer’s source of funds is known for a fact to be, or is assumed to be, from corruption or embezzlement, the Bank shall not accept a business relationship or should terminate the said relationship with the customer.

(X) If the Bank cannot complete related procedures for the verification of customer identity, it shall consider reporting suspicious ML/TF transactions related to the customer.

(XI) If a customer or a transaction is suspected of being involved in ML/TF and it is reasonably believed that performing the customer identity verification may lead to the leakage of customer information, the Bank may choose not to continue with the verification procedures but file a suspicious ML/TF report instead.

(XII) The establishment of other business relations shall be processed in accordance with the internal operation guidelines of the Bank.

XV. If any of the following circumstances occur, they shall be handled in accordance with the stipulations in the contracts:

(I) Pursuant to Item 8 of subparagraph 1, the Bank may refuse to conduct business with the customer or terminate the business relationship at its sole discretion.

(II) For customers who are unwilling to comply with the identity verification, refuse to provide information on beneficial owners

or persons who exercise controlling interest over the customer, or unwilling to explain the nature and purpose of the transaction and sources of the funds, the Bank may temporarily suspend the transaction or temporarily or permanently terminate the business relationships with the customer.

XVI. The Bank shall file a suspicious ML/TF transaction report in accordance with Article 10 of the Money Laundering Control Act if the Bank establishes a business relationship or conducts a transaction with any counterparty specified in Item 8 of Subparagraph 1. If the counterparty is an individual, legal entity, or group who is subject to sanctions by the Counter-Terrorism Financing Act, the Bank shall engage in any acts set out in Paragraph 1 of Article 7 of the Counter-Terrorism Financing Act, from the day it becomes aware of such circumstance, and the Bank shall file a report such matter in accordance with the provisions set out in the Counter-Terrorism Financing Act. (related forms may be downloaded from the website of the Investigation Bureau, Ministry of Justice) If any circumstance specified in Subparagraphs 3 and 4, Paragraph 1, Article 6 of the Counter-Terrorism Financing Act already exist before the aforesaid counterparty was designated for sanctions, the Bank shall apply to the Investigation Bureau for permission in accordance with the related provisions of the Counter-Terrorism Financing Act.

Article 5

The Bank's customer identity verification measures shall include an ongoing review of the customer's identity and shall be conducted in accordance with the following provisions:

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

II. The Bank shall regularly review the adequacy of the information obtained by identifying customers and their substantial beneficial owner and ensure that such information is up-to-date. High-risk customers shall be reviewed at least once a year. For other customers, the frequency of review shall be determined based on the risk-based approach.

III. The customer identity verification may be conducted based on the record information provided by the customers in past verifications. Thus, the Bank is not required to identify and verify the customer’s identity at every transaction. However, if the Bank has doubts about the veracity or adequacy of the customer’s information, or has found the customer to have involved in suspected ML/TF activities, or if the operations of the customer’s transactions or accounts differ significantly from the norm of the nature of the business relationship with the customer, the Bank shall confirm the customer’s identity again in accordance with Article 4.

Article 6

The extend of customer identity verification measures and ongoing review mechanism set out in Subparagraph 3 of Article 4, and the preceding Article shall be determined based on the risk-based approach and shall include:

I. For high-risk circumstances, the Bank shall apply enhanced customer identity verification measures and ongoing review measures by adopting additionally at least the following enhanced measures:

(I) Before establishing or adding new business relationships, the Bank shall seek approval from the senior management personnel with the appropriate level of approval authorization based on the Bank's internal risk considerations.

(II) The Bank shall take reasonable measures to understand a customer's wealth and source of funds. The source of funds refers to the actual source from which a specific fund is generated (e.g. salary, investment income, purchase, and sale of real estate).

(III) The bank shall enhance ongoing monitoring of business relationships.

II. For customers from high ML/TF risk countries or regions, the Bank shall adopt enhanced measures which are consistent with the risks identified.

III. For low-risk circumstances, the Bank may adopt simplified customer identity verification measures, which are consistent with the low-risk factors. However, the simplified customer identity verification measures cannot be applied to customers who exhibit any of the following circumstances:

(I) Where the customer is from a high-risk country or region that does not take effective AML/CTF measures, including but not limited to countries or regions which fail to comply with the suggestions of international anti-money laundering organizations as published by the international anti-money laundering organizations via the Financial Supervisory Commission, and countries or regions that are materially defective in AML/CTF.

(II) Where the Company suspects that the customer or the transaction is ML or FT-related.

The simplified measures may be adopted by the Bank under the following circumstances:

I. Reducing the frequency of updating customer identification information.

II. Reducing the level of ongoing monitoring measures and adopt a reasonable threshold as a basis to review the transaction.

III. If the purpose and nature can be determined based on the type of transaction or existing business relationship, the Bank may not require to collect specific information or to implement special measures to learn about the purpose and nature of the business relationship.

The Bank shall conduct assessments on the identity of existing customers base on the level of materiality and risks, and carry out reviews on the existing relationship, taking into consideration the timing and the adequacy of

information obtained in the previous review.

Article 7

The Bank shall perform the customer identity verification by itself. However, if it is otherwise provided in laws and statutes or FSC regulations that the Bank may retain third parties to perform the identity verification of the customers, agents, and beneficial owners or the purpose and intended nature of the business relationship, the Bank shall bear the ultimate liability for the verification of customer identity and comply with the following provisions:

I. The Bank shall have access to the information required for verification of customer identity.

II. The Bank shall adopt measures that meet the Bank's needs and ensure that the entrusted third party will not delay in providing necessary customer identity information or other relevant documents to verify the customer's identity, as required by the Bank.

III. The Bank shall ensure that the entrusted third party is regulated, supervised, or monitored, adopts appropriate relevant measures to verify the customer's identity, and retains the records accordingly.

IV. The Bank shall ensure that the regulations on AML/CTF in the location of the entrusted third party are consistent with the standards set by the Financial Action Task Force on Money Laundering (FATF).

Article 8

The Bank’s regulations regarding the checking of names of customers and trading counterparties shall comply with the following provisions:

I. Based on a risk-based approach, the Bank shall establish name check and verification policies and procedures for customers and transaction-related parties to detect, match, and screen customers, their high-level management personnel, beneficial owners, or transaction-related parties to check if they belong to the categories of individuals, legal entities, or groups that are subject to designated sanctions by the Counter-Terrorism

Financing Act, or terrorists or terrorist groups identified or investigated by foreign governments or international organizations. If so, such matter shall be handled in accordance with Subparagraph 15 of Article 4.

II. The name check and verification policies and procedures for customers and transaction-related parties shall include at least matching and filtering logic, operating procedures, and evaluation standards, and these matters shall be documented.

III. The implementation of the name check and verification shall be recorded and preserved in accordance with the time period specified in Article 15.

IV. This check and verification mechanism shall be tested and the scope for testing shall include:

(I) Whether the sanctions list and thresholds are established based on a risk-based approach.

(II) The completeness and correctness of data input in the corresponding fields.

(III) Matching and filtering logics.

(IV) Model verification.

(V) The completeness and correctness of data output.

V. Confirming if the test results can appropriately reflect the risks and make revise the mechanism accordingly.

Article 9

The Bank's ongoing monitoring of accounts and transactions shall be handled in accordance with the following provisions:

I. The Bank shall use the information system to gradually integrate basic information and transaction information on all customers for the head office and branches to consult for the purpose of AML/CTF to strengthen its account and transaction monitoring capabilities. The Bank shall also establish internal control procedures for requests and inquiries as to customer information made by various departments and shall exercise care

to ensure the confidentiality of the information.

II. The account and transaction monitoring policies and procedures shall be established based on a risk-based approach, and an information system shall be employed to assist in the discovery of suspicious ML/TF transactions.

III. The account and transaction monitoring policies and procedures shall be reviewed and updated regularly in accordance with laws and regulations on AML/CTF, nature of customers, business scale and complexity, money laundering and terrorism financing-related trends and information obtained from internal and external sources, and the Bank's internal risk assessment results.

IV. The account and transaction monitoring policies and procedures shall include at least a complete monitoring model, parameter settings, monetary threshold amounts, alerts and monitoring operation procedures, inspection procedures, and reporting standards. These matters shall be documented.

V. The preceding mechanism shall be tested, and the scope for testing includes:

(I) Internal control process: Examination of the roles and responsibilities of personnel or units related to the account and transaction monitoring mechanism.

(II) The completeness and correctness of data input in the corresponding fields.

(III) Detection scenario logics.

(IV) Model verification.

(V) Data output.

VI. When the Bank has discovered or has reasonable grounds to suspect that the customer, the customer's funds, assets, or intention to conduct or have conducted transactions related to ML/TF, regardless of the monetary amount or value or completion of the transaction, the Bank shall further

review the customer's identity.

VII. The red flags for suspicious ML/TF transactions listed in the Appendix are developed by the Bank that should be watch-listed based on its own asset scale, geographical distribution, business characteristics, the natures and transaction attributes of its customer groups, and its internal risk assessment of ML/TF or information regarding normal transaction activities.

VIII. The reasonableness of the watch-listed red flag transactions mentioned in the preceding Subparagraph shall be determined on a case-by-case basis (the determination of reasonableness includes: whether there are transactions that are incommensurate with the customer's identity, income level, or business scale, irrelevant to the nature of the customer's own business, inconsistent with the customer's business model, have no reasonable economic purpose, explanation, or usage, or have unclear or inadequate explanations for the source of funds). The review for such determination for ML/TF red flag transactions shall be completed as fast as possible, and documented for records. When a transaction is examined and determined not to be a transaction suspected of ML/TF, the reasons for the exclusion shall be recorded and analyzed. For any transaction suspected of ML/TF, the Bank shall file a report with the Investigation Bureau, Ministry of Justice within 2 business days after the matter is approved by the designated supervisory officers of the Bank. The same shall apply to uncompleted transactions.

IX. The Bank shall identify suspicious ML/TF transactions based on the risk-based approach, and establish a relevant information system to assist the monitoring of such transactions. For transactions that are not included in the information system, the Bank shall provide other methods to assist employees in the determination of ML/TF transactions. The information system may not completely replace the employee's judgment. Thus, it is necessary to enhance employee training, so that the employees are able to

identify suspicious ML/TF transactions.

Suspicious ML/TF reports:

I. When an abnormal transaction is identified, the personnel in charge shall report to their supervisory officers at once.

II. The Bank shall ensure that supervisor officers promptly determine suspicious ML/TF transactions and file a report. If a transaction is determined to be reported, the original personnel in charge shall fill out a report form (the format shall be downloaded from the website of the Investigation Bureau, Ministry of Justice) immediately.

III. The report shall be submitted to the designated unit after approval.

IV. The report shall be filed with the Investigation Bureau, Ministry of Justice after approval by the designated supervisory officers.

V. Major and urgent suspected ML/TF transactions shall be reported to the Investigation Bureau, Ministry of Justice by fax immediately, and supplemented by written reports thereafter. However, if the Bank receives an acknowledgment receipt from the Investigation Bureau, Ministry of Justice by fax (the format shall be downloaded from the website of Investigation Bureau, Ministry of Justice), no supplement written reports are required. The Bank shall keep the fax containing the acknowledgment receipt for records.

Confidentiality of reported information:

I. The suspected ML/TF reports shall be kept confidential by personnel of all levels. The Bank shall provide training or instructional materials to prevent information leakage during interactions between employees and customers and in the course of daily operations.

II. All documents related to the report shall be treated as confidential documents. Shall there be leakage, such matter shall be dealt with relevant regulation.

III. Personnel from the Anti-Money Laundering Unit, Compliance Department, and audit units may have access to instant transaction records of the

customers when performing their AML/CTF duties. However, they shall abide by the confidential requirements.

The execution of account examination and ongoing monitoring shall be recorded and preserved in accordance with the time period specified in Article 15.

Article 10

The Bank’s report on the properties or property interest and locations of designated sanctioned individuals or entities pursuant to Article 7 of the “Counter-Terrorism Financing Act” shall be handled in accordance with the following provisions:

I. Upon knowing any ML/TF transactions, the designated unit shall submit the report to the designated supervisory officers mentioned in the preceding Article for approval in the format downloaded from the website of the Investigation Bureau, Ministry of Justice. Then, the report shall be filed with the Investigation Bureau, Ministry of Justice within 2 business days after the approval.

II. Major and urgent matters shall be reported to the Investigation Bureau, Ministry of Justice by fax or other feasible means immediately, in the format required by the Investigation Bureau, Ministry of Justice (the format can be downloaded from the website of the Investigation Bureau, Ministry of Justice) and supplemented by written reports thereafter. However, if the Bank receives an acknowledgment receipt in the template format from the Investigation Bureau, Ministry of Justice by fax, no supplement written reports are required. The Bank shall keep the fax containing the acknowledgment receipt for records.

III. The Bank shall prepare an annual report in the format prescribed by the Investigation Bureau, Ministry of Justice (the format may be downloaded from the website of Investigation Bureau, Ministry of Justice) with December 31 being the settlement record date. The report shall state all properties or property interests of designated sanctioned individuals, legal

persons or groups managed or held in accordance with Article 7 of the Counter-Terrorism Financing Act, and be submitted to the Investigation Bureau, Ministry of Justice before March 31 of the following year for reference.

The report records, transaction records, and annual reports shall be kept for five years in the original manner.

Article 11

For cross-border correspondent banking and other similar businesses, certain policies and procedures shall be established, which shall include:

I. Collecting sufficient public information to fully understand the nature of the correspondent institution's business and judging its reputation and management quality, including compliance with regulations on AML/CTF, and whether it has been investigated or subject to any administrative penalty for ML/TF.

II. Assessing whether the correspondent institution has appropriate control policies and effective implementation regarding AML/CTF.

III. Obtaining approval from the senior management personnel with the appropriate level of approval authorization based on the Bank's internal risk considerations, before establishing a correspondent relationship with the correspondent institution.

IV. Documenting the respective AML/CTF responsibilities of each institution;

V. Where a correspondent relationship involves “payable-through accounts”, it is necessary to ensure that the correspondent bank has performed the customer identity verification measures on customers who have direct access to the cross-border correspondent bank accounts. When necessary, the Bank is able to provide information regarding the customers’ identity upon the request of the cross-border correspondent banks.

VI. The Bank shall not establish a correspondent relationship with shell banks nor any financial institution that permits any shell bank to use its accounts.

VII. For any correspondent banks that are unable to provide the aforementioned public information upon requests, the Bank may refuse to open an account, suspend transactions, report a suspected ML/TF transaction, or terminate the business relationship.

VIII. When the correspondent bank is one of the Bank's foreign branch (or subsidiary), the aforementioned provisions shall also apply.

Article 12

The Bank shall conduct the ML/TF risk assessment before launching new products or services or conducting a new type of business (including new payment mechanisms, using new technologies in existing or new products or business), and establish corresponding risk management measures to mitigate the identified risks.

Article 13

The Bank’s regulations regarding remittance:

I. The Bank 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.”

II. The domestic New Taiwan Dollar outward remittance business shall be handled in accordance with the following provisions:

(I) Providing the necessary and correct information of the remitter and the necessary information of the beneficiary by any of the means below:

1. The information of the remitter and beneficiary shall accompany the remittance transaction.
2. The information on the remitter's and the beneficiary's account numbers or a transaction code that can be tracked shall be accompanying the remittance transaction, and the

remitter's and beneficiary's information shall be provided within three business days upon receipt of the request from the receiving financial institution or the competent authority. However, law enforcement authorities should be able to compel immediate production of such information and the Bank shall respond accordingly.

3. For single transactions of less than NT$ 30,000, the Bank may not verify the correctness of the information of emitters unless in situations of suspected ML/TF transactions.

(II) Retaining the following information on the remitters and beneficiaries in accordance with Article 12 of the Regulations Governing Anti-Money Laundering of Financial Institutions:

1. Information of the remitter shall include: name, account number (if unavailable, a transaction code for tracking shall be provided), and any one of the information below:
   (1) Identity card number.
   (2) Address of the remitter.
   (3) Birthdate and birthplace.
2. Information of the beneficiary shall include name, and account number (if unavailable, a transaction code for tracking shall be provided).

III. When the Bank fails to comply with the provisions of the preceding two subparagraphs, it shall not perform the remittance business.

IV. The domestic New Taiwan Dollar inward remittance business shall be handled in accordance with the following provisions:

(I) Risk-based policies and procedures for determining when to execute, reject, or suspend a remittance lacking the information specified under Subparagraph 2, Paragraph 2 hereof, and the appropriate follow-up actions.

(II) Retaining the information obtained on the remitters and

beneficiaries in accordance with Article 12 of the Regulations Governing Anti-Money Laundering of Financial Institutions:

Article 14

The Bank shall handle cash transactions above a certain amount in accordance with the following provisions:

I. The customer's identity shall be verified and the relevant records shall be kept.

II. Customer identity verification measures shall be conducted in accordance with the following provisions:

(I) The customer's identity is verified by identification documents or passport provided by the customer, and the name, date of birth, address, telephone number, transaction account number, transaction amount, and identification documents shall be recorded. In case that the customer is confirmed to be the account holder, it should be clearly noted in the transaction record without undertaking the identity verification.

(II) If the transaction is conducted by an agent, the agent's identity shall be verified by identification documents or passport provided by the customer, and the name, date of birth, address, telephone number, transaction account number, transaction amount, and identification documents shall be recorded.

(III) If the transaction is an occasional transaction, the customer's identity shall be verified in accordance with the provisions of Subparagraph 3 of Article 4.

III. Unless specified in Items 2 and 3 of this Article, a report shall be filed with the Investigation Bureau, Ministry of Justice through electronic media (the format may be downloaded from the website of the Investigation Bureau, Ministry of Justice) within 5 business days after the completion of the transaction. The Bank may file such a report in writing (the format may be

downloaded from the website of the Investigation Bureau, Ministry of Justice) provided it is unable to file the report via electronic media with good causes and has acquired the approval of the Investigation Bureau, Ministry of Justice.

IV. The relevant records and documents filed with the Investigation Bureau shall be handled in accordance with the provisions of Article 15.

The following cash transactions above a certain amount are exempt from reporting to the Investigation Bureau, Ministry of Justice. However, the Bank shall still be required to verify the identity of customers and keep relevant records:

I. Deposits into the accounts opened by government agencies, state-owned enterprises, institutions acting with governmental power (within the scope of mandate), public and private schools, public enterprises, and government funds established under laws.

II. Receivables and payables collected and made by a financial institution on behalf of government treasuries.

III. Transactions and funding arrangements between financial institutions. Notwithstanding the foregoing, payables to another bank’s customer paid through a vostro deposit account, such as cashing a check issued by another bank or the same customer's cash transactions exceeding a certain amount, shall be handled as required.

IV. Lottery ticket purchases by lottery merchants.

V. Payments collected on behalf of a third party (excluding payments deposited in designated stock subscription accounts and credit card payments) where the payment notice expressly bears the name and identification documents number of the counterparty (including the code which enables the tracking of counterparty’s identity), as well as type and amount of transaction. Nevertheless, duplicate copies of the payment notices shall be retained as transaction records.

For non-individual accounts such as those opened by the department stores,

hypermarkets, supermarket chains, gas stations, medical institutions, the transportation industry, and the hotel industry, which have regular or routine deposits reaching a certain amount due to the business nature, the Bank may, after confirming their actual business needs, submit the name list to the Investigation Bureau, Ministry of Justice for review. Such transactions may be exempt from case-by-case verification if the Investigation Bureau does not respond with dissenting opinions within 10 days. The Bank shall review the transaction counter-party at least once a year, and shall report to the Investigation Bureau for review if the Bank has no longer business dealing with the counterparties.

For the transaction set out in the preceding two paragraphs, if any suspicious ML/TF transactions are discovered, they shall still be handled in accordance with Article 10 of the Money Laundering Control Act and Article 7 of the Counter-Terrorism Financing Act.

Article 15

The Company shall keep records of correspondence and transactions with customers in hard copies or the electronic form, and in accordance with the following provisions:

I. The Bank shall retain all necessary records on domestic and foreign transactions for at least 5 years unless a longer period of time is required by laws and regulations. The aforementioned necessary records include:

(I) Name, account number, or identification number of each party conducting the transaction.

(II) Date of transaction.

(III) Type and amount of currency.

(IV) Methods of depositing or withdrawing funds, such as cash, checks, etc.

(V) Destination of funds.

(VI) Method of instruction or authorization.

II. For large currency transactions exceeding a certain amount, verification records, and report records of the transactions shall be retained in their original form for a minimum of 5 years.

III. For suspected ML/TF transaction reports, report records shall be retained in their original form for a minimum of 5 years.

IV. The Bank shall keep the following information for at least 5 years after the end of the business relationship or after the completion of an occasional transaction unless a longer period of time is required by laws and regulations:

(I) All records obtained through the customer identity verification measures, such as passport, identification card, driver’s license, and copies of similar official documents or records.

(II) Account or contract document files.

(III) Business correspondence, including information on the background and purpose obtained from inquiries to complex, unusual large transactions and the results of any analysis undertaken.

V. Transaction records retained shall be sufficient for the reconstruction of a single transaction so as to serve, if necessary, as evidence for the prosecution of criminal activity.

VI. The Bank shall ensure that information on transaction records and customer identity verification can be made available swiftly to the competent authorities when such requests are made with appropriate authorization.

Article 16

The Bank shall allocate sufficient AML/CTF personnel and resources based on the scale and risks. The Board of Directors shall appoint a senior manager to be the designated supervisory officer who is granted full authority in the coordination and supervision of AML/CTF matters. Moreover, the Board of

Directors shall ensure that the personnel and managers do not hold concurrent posts which might involve a conflict of interest with their AML/CTF duties. Also, a designated AML/CTF unit shall be established under the Compliance Department. The unit shall not concurrently conduct business other than AML/CTF matters.

The designated unit or designated supervisory officers in the preceding paragraph is in charge of the following tasks:

I. Supervising the identification and evaluation of ML/TF, as well as planning and implementing policies and procedures.
II. Coordinating the supervision of overall identification, evaluation, and execution of AML/CTF.
III. Supervising risks related to AML/CTF.
IV. Promoting plans regarding AML/CTF.
V. Coordinating the supervision on the implementation of the AML/CTF plan.
VI. Confirming the compliance of AML/CTF plans to laws and regulations including the templates or self-discipline rules issued by the Bank Association and approved by the FSC.
VII. Supervising the reporting on suspicious transactions and the properties or property interests and locations of designated individuals or entities sanctioned under the Terrorism Financing Prevention Act to the Investigation Bureau, Ministry of Justice.

Regarding Item 1, the designated supervisory officer shall report to the Board of Directors and the Audit Committee at least once every six months. If any major violation of the laws is identified, the designated supervisory officer shall report to the Board and Audit Committee immediately.

Article 17

The business units of the Bank shall appoint a senior officer to act as the supervisor to take charge of supervising AML/CTF-related matters and self-inspections conducted by the business unit.

The Bank’s audit units shall conduct the audit on the following items in accordance with regulations and issue audit opinions:

I. Whether ML/TF risk assessment and AML/CTF plans are in compliance with laws and regulations and implemented thoroughly.

II. The effectiveness of AML/CTF plans.

The duties of the Bank’s internal audit unit:

I. Conducting routine audits in accordance with the internal regulations as instituted for internal control, and tests on the effectiveness of the AML/CTF plans and the quality of risk management of the Bank, the Bank's segments, and branches (or subsidiaries).

II. The auditing method shall cover an independent transaction test, including screening relevant transactions for high-risk products, customers, and geographical areas identified by the Bank to verify that the AML/CTF-related regulations have been effectively implemented.

III. Where negligence during the implementation of a management measure is discovered, such matters shall be to the designated supervisory officers regularly and serve as reference material for employee on-the-job training.

IV. Where concealments of major violations of the laws were discovered, such matters shall be properly handled by the competent units of the head office.

The Bank's President shall supervise each unit to carefully assess and review the implementation of the AML/CTF internal control system. A declaration shall be submitted jointly by the Chairman, President, Chief Auditor, and AML/CTF Officer to the Board of Directors for approval. The content of the said declaration shall be disclosed on the Bank's website and published on a website designated by the FSC within three months after the end of each fiscal year.

Article 18

The Bank shall establish a high-quality and appropriate staff selection procedure and appointment process, including reviewing whether employees have an honest personality and the professional knowledge required to perform their duties.

The Bank's AML/CTF Officers, AML/CTF personnel, and supervisors of domestic business units shall meet one of the following qualifications within three months after the appointment. The Bank shall also establish relevant control mechanisms to ensure the compliance:

I. Have served as designated compliance officers or AML/CFT personnel for more than three years.

II. Have attended at least 24 hours of courses held by the FSC-accredited institutions, passed the examinations, and obtained the certificates of completion. However, those who have met the requirements of compliance personnel shall be deemed to have the qualifications specified under this item after participating in at least 12 hours of training on AML/CTF.

III. Have obtained domestic or international AML/CTF professional certificates issued by the FSC-accredited institutions.

Every year, AML/CTF Officers, AML/CTF personnel, and supervisory officer of the business units shall at least attend 12 hours of AML/CTF training held by the internal/external training institutions approved by the designated supervisory officers set forth in Item 1 of Article 16. The AML/CTF training shall cover the latest updates to the laws, and trends and patterns of AML/CTF risks. III. Those who have obtained domestic or international AML/CTF professional certificates issued by the FSC-accredited institutions may be exempt from the course hour requirement of that year.

The Bank shall arrange education and training on AML/CTF with appropriate content and number of hours every year for its Directors, Independent Directors, President, compliance personnel, internal auditors, and business personnel shall, according to the nature of their duties, facilitate their understanding of their AML/CTF duties, and equip them with the required professional skills for their duties.

Employees who exhibit any of the following conditions shall have their work inspected, with the help of the audit unit, if necessary.

I. Leading an extravagant lifestyle that is not commensurate with the income

levels.

II. Having leaves scheduled, but cancel leaves without reason.

III. Unable to reasonably explain the large transactions in and out of their accounts.

Employees shall be rewarded for their AML/CTF contributions specified as follows:

I. Employees who have discovered cases allegedly involved in AML/CTF, and have filed a report to the competent authority in accordance with relevant AML regulations, leading to the prevention or resolving of crimes by the police and prosecution authorities.

II. Employees who have participated in relevant domestic or international business seminars on AML/CTF with outstanding performances or who have successfully gathered valuable legal research information on foreign countries for the Bank's AML/CTF activities.

Pre-employment and on-the-job training shall be handled in the following ways:

I. Pre-employment training: A certain hours of training courses on the AML regulations. CTF regulations and the legal responsibilities of financial services personnel shall be provided for the Bank's new recruits so that they can understand relevant requirements and their responsibilities.

II. On-the-job training:

(I) Initial law awareness training: After the implementation of or amendments to the Money Laundering Control Act and the Counter-Terrorism Financing Act, the Bank shall, as soon as possible, organize law awareness training, familiarize them with the Money Laundering Control Act, and the Counter-Terrorism Financing Act, and explain the Bank's relevant corresponding measures. The relevant matters are planned by the designated unit before handed over to the staff training unit for implementation.

(II) Regular on-the-job training:

1. The staff training unit shall organize relative training courses for the employees to enhance the employees' capability in judgment, ensure the functions of the AML/CTF measures, and prevent the employees' violation of laws. Courses of the training may be arranged in other suitable training courses.
2. The training courses may be lectured by internal lecturers or by experts and scholars when necessary.
3. The training courses shall include relevant laws and regulations, and also case studies to allow employees to understand the characteristics and types of ML/TF to detect "suspicious ML/TF transactions."
4. The designated unit shall routinely review employees' participation and urge those who have not attended any training course to participate in relevant training.
5. In addition to internal on-the-job training, the Bank may select and send relevant employees to take training courses organized by external training agencies.

III. Topical lectures: The Bank shall organize lectures on selected topics so that the employees can better understand AML laws and regulations. Scholars and experts may be invited to give such lectures.

Article 19

Other matters to be noted:

I. The Bank's employees shall decline to provide services to the customers if the customers exhibit any of the following circumstances, and report to the supervisory officers directly.

(I) Where the customer insists on not providing relevant information when being notified that he/she is to provide such information to prove his/her identity as required by law.

(II) Where any individual or group uses force or intends to use force

to prevent the Bank's employee from documenting the transaction records or filing the report form.

(III) Where the customer attempts to persuade the Bank's employee to forgo the completion of mandatory transaction information.

(IV) Where the customer inquiries about the possibility of avoiding the filing of the report.

(V) Where the customer anxiously explains the legality of the sources of funds or that there is no money laundering activity involved.

(VI) Where the customer insists that the transaction be completed immediately without reasonable explanations.

(VII) Where the customer's description is obviously not consistent with the transaction itself.

(VIII) Where the client attempts to provide benefits to the Bank's employee in exchange for services of the Bank.

II. If the Bank conducts other businesses concurrently, the department conducting other businesses shall also be subject to the Directions Governing Money Laundering and Countering-Terrorism Financing which is related to its business. For example, the Trust Department of the Bank shall comply with the Directions Governing Anti-Money Laundering and Countering-Terrorism Financing for Trust Enterprise.

Article 20

When the FSC or the entrusted institution conducts the inspection on the Bank in accordance with Article 10 of the "Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated by the Financial Supervisory Commission", the Bank shall provide relevant books, documents, electronic files, or other relevant materials. The aforementioned materials, whether stored in hard copy, electronic files, e-mails, shall be provided

for inspection, and the Bank shall not circumvent, reject, or obstruct the inspection for any reason.

Article 21

The amendments to these guidelines shall also be implemented after approval by the Board of Directors. But authorization for amendments to the appendices is granted solely to be approved by the general manager.

The Directions were enacted on April 22, 1997.
Amended on October 15, 1997.
Amended on November 23, 1999.
Amended on March 7, 2002.
Amended on August 6, 2003.
Amended on November 14, 2003.
Amended on August 12, 2004.
Amended on August 17, 2005.
Amended on December 23, 2005.
Amended on June 1, 2006.
Amended on December 14, 2006.
Amended on March 8, 2007.
Amended on March 8, 2007.
Amended on May 9, 2007.
Amended on December 10, 2007.
Amended on the 48th board meeting of the 11th board on July 31, 2009.
Amended on the 60th board meeting of the 11th board on January 15, 2010.
Amended on May 14, 2013.
Amended on September 27, 2013.
Amended on December 16, 2013.
Amended on December 8, 2014.
Amended on November 23, 2015.
Amended on April 25, 2016.
Amended on October 16, 2017.
Amended on August 20, 2018.
Amended on August 20, 2018.
Amended on October 12, 2020.
Amended on October 31, 2023.