Regulations Governing Anti-Money Laundering of Financial Institutions

Article 1 These Regulations are enacted pursuant to the front section of Paragraph 4, Article 7, Paragraph 3 of Article 8, Paragraph 3 of Article 9 and Paragraph 3 of Article 10 of the Money Laundering Control Act (referred to as the “Act” hereunder).

Article 2 Terms used in these Regulations are defined as follows:

1. “Financial institution” shall mean the following banking business, electronic payment institutions, electronic stored value card issuers, securities and futures businesses, and insurance enterprises:
   (1) "Banking business" includes banks, credit cooperatives, postal offices which also handle money transactions of deposit, transfer and withdrawal, bills finance companies, credit card companies and trust enterprises.
   (2) “Electronic payment institution” means an institution approved to engage in electronic payment business pursuant to the Act Governing Electronic Payment Institutions.
   (3) “Electronic stored value card issuer” means an institution approved to issue electronic stored value cards pursuant to the Act Governing Issuance of Electronic Stored Value Cards.
   (4) "Securities and futures business" includes securities firms, securities investment and trust enterprises, securities finance enterprises, securities investment consulting enterprises, securities central depository enterprises, futures commission merchants, leverage transaction merchants, futures trust enterprises, and managed futures enterprises.
   (5) “Insurance enterprise” includes insurance companies, reinsurance companies, insurance agent companies, insurance broker companies, and post offices engaging in simple life insurance business.
2. “A certain amount” shall mean NT$500,000 (including the foreign currency equivalent thereof).
3. “A certain quantity” shall mean 50 electronic stored value cards.
4. “Cash transaction” shall mean cash receipt or payment in a single transaction (including all transactions recorded on cash deposit or withdrawal vouchers for accounting purpose), or the transaction of currency exchange.
5. "E-payment account" shall mean an online account opened by users with an electronic payment institution to keep track of their funds transfer and funds deposit records. The term "users" mentioned above shall mean persons who register and open an electronic payment account ("e-payment account") with an electronic payment institution and use the services provided by the electronic payment

institution to make funds transfer or deposit stored value funds.

6. "Customer" shall mean the customers of banking business, securities and futures business and insurance enterprises, the users of e-payment accounts and the cardholders of electronic stored value card issuers.
7. "Beneficial owner" shall mean a natural person who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted, including those persons who exercise ultimate effective control over a legal person or arrangement.
8. "Risk-based approach" (RBA) shall mean financial institutions should identify, assess and understand the money laundering and terrorist financing (ML/TF) risks to which they are exposed and take anti-money laundering and countering terrorist financing (AML/CFT) measures commensurate to those risks in order to mitigate them. Based on the RBA, financial institutions should adopt enhanced control measures for higher risk situations, and adopt relatively simplified control measures for lower risk situations to allocate resources efficiently, and use the most appropriate and effective approach to mitigate the identified ML/TF risks.

Article 3 A financial institution shall comply with the following provisions in undertaking customer due diligence (CDD) measures：

1. A financial institution shall not accept anonymous accounts or accounts in fictitious names for establishing or maintaining business relationship.
2. A financial institution shall undertake CDD measures when:
   (1) establishing business relations with any customer;
   (2) carrying out occasional transactions with respect to:
      A. cash receipt or payment in a single transaction or electronic stored value cards above a certain quantity or multiple apparently related cash transactions that is above a certain amount when combined; or
      B. a cross-border wire transfer involving NTD 30,000 or more (including the foreign currency equivalent thereof);
   (3) there is a suspicion of money laundering or terrorist financing; or
   (4) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.
3. The time of establishing business relations with any customer mentioned under Item (1) of the preceding subparagraph is when accepting a customer's registration application in the case of an electronic payment institution, and when accepting a customer's registration of an electronic stored value card in the case of an electronic stored value card issuer.
4. The CDD measures to be taken by a financial institution are as follows:

(1) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information. In addition, a financial institution shall retain copies of the customer's identity documents or record the relevant information thereon.

(2) Verifying that any person purporting to act on behalf of the customer is so authorized, identifying and verifying the identity of that person using reliable, independent source documents, data or information. In addition, the financial institution shall retain copies of the person's identity documents or record the relevant information thereon.

(3) Taking reasonable measures to identify and verify the identity of the beneficial owner of a customer, including using reliable source data or information.

(4) Enquiring information on the purpose and intended nature of the business relationship and obtaining relevant information in view of the situation when undertaking CDD measures.

5. When the customer is a legal person, an organization or a trustee, a financial institution shall, in accordance with the preceding subparagraph, understand the business nature of the customer or trust (including trust-like legal arrangements) and obtain at least the following information to identify the customer or the trust and verify its identity:

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

(2) The charter or similar power documents that regulate and bind the legal person or trust, except for any of the following circumstances:

A. Customers/entities listed under Item (3) of Subparagraph 7 hereof and insurance products listed under Item (4) of Subparagraph 7 hereof are free of the situation described in the proviso of Subparagraph 3, Paragraph 1 of Article 6 herein.

B. Customers/entities engaging in electronic stored value card registration business.

C. The customer who is an organization acknowledges that it does not have a charter or similar power document.

(3) Names of relevant persons having a senior management position in the customer.

(4) The address of the registered office of the customer, and if different, the address of its principal place of business.

6. When the customer is a legal person, a financial institution shall understand whether the customer is able to issue bearer shares and apply appropriate measures for customers who have issued bearer shares to ensure their beneficial owners are kept up-to-date.

7. When the customer is a legal person, an organization or a trustee, a financial institution shall, in accordance with Item (3) of Subparagraph 4 hereof, understand the ownership and control structure of the customer or the trust, and obtain the following information to identify the beneficial owners of the customer and take reasonable measures to verify the identity of such persons:
   (1) For legal persons and organizations:
      A. The identity of the natural person(s) who ultimately has a controlling ownership interest in the legal person. A controlling ownership interest refers to owning directly and/or indirectly more than 25 percent of the legal person's shares or capital; a financial institution may ask the customer to provide its list of shareholders or other documents to assist in the identification of persons holding controlling ownership interest.
      B. To the extent where no natural person exerting control through ownership interests is identified or that there is doubt as to whether the person(s) with the controlling ownership interest are the beneficial owner(s), the identity of the natural person(s) (if any) exercising control of the customer through other means.
      C. Where no natural person is identified under Sub-item A or B above, a financial institution shall identify the identity of a natural person who holds the position of senior managing official.
   (2) For trustees: the identity of the settlor(s), the trustee(s), the trust supervisor, the beneficiaries, and any other natural person(s) exercising ultimate effective control over the trust, or the identity of person(s) in equivalent or similar position.
   (3) Unless otherwise provided for in the proviso of Subparagraph 3, Paragraph 1 of Article 6 herein or where the customer has issued bearer shares, a financial institution is not subject to the requirements of identifying and verifying the identity of beneficial owner(s) of a customer set out under Item (3) of Subparagraph 4 hereof, provided the customer or the person having a controlling ownership interest in the customer is
      A. a R.O.C government entity;
      B. an enterprise owned by the R.O.C government;
      C. a foreign government entity;
      D. a public company and its subsidiaries;
      E. an entity listed on a stock exchange outside of R.O.C. that is subject to regulatory disclosure requirements of its principal shareholders, and the subsidiaries of such entity;
      F. a financial institution supervised by the R.O.C. government, and an

investment vehicles managed by such institution;

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

H. a fund administered by a R.O.C. government entity; or

I. an employee stock ownership trust or an employee savings trust.

(4) Except for situations provided for in the proviso of Subparagraph 3, Paragraph 1 of Article 6 herein, a financial institution is not subject to the requirements of identifying and verifying the identity of beneficial owner(s) of a customer set out under Item (3) of Subparagraph 4 hereof when the customer purchases property insurance, accident insurance, health insurance or an insurance product that does not require policy value reserve.

8. An insurance enterprise shall adopt the following measures when the beneficiary(ies) on a life insurance policy, investment-linked insurance policy or annuity insurance policy have been identified or designated:

(1) Obtaining the name and identification document number or registration (incorporation) date of the designated beneficiary; and

(2) For beneficiary(ies) that are designated by contract characteristics or by other means, obtaining sufficient information concerning the beneficiary to satisfy the insurance enterprise that it will be able to establish the identity of the beneficiary at the time of the payout.

(3) Verifying the identity of the beneficiary(ies) at the time of the payout.

9. A financial institution shall not establish business relationship or conduct occasional transactions with a customer before completing the CDD process. However, a financial institution may first obtain information on the identity of the customer and its beneficial owner(s) and complete the verification after the establishment of business relationship, provided that:

(1) The 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;

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

(3) Verification of the identities of the customer and its beneficial owner(s) will be completed as soon as reasonably practicable after the establishment of business relationship. A financial institution shall advise its customer in advance that the business relationship will be terminated if verification cannot be completed as

soon as reasonably practicable.

10. Where a financial institution is unable to complete the required CDD process on a customer, it should consider filing a suspicious transaction report on money laundering or terrorist financing (STR) in relation to the customer.
11. If a financial institution forms a suspicion of money laundering or terrorist financing and reasonably believes that performing the CDD process will tip-off the customer, it is permitted not to pursue that process and file an STR instead.
12. The CDD process for e-payment accounts shall follow relevant provisions in the Regulations Governing Identity Verification Mechanism and Transaction Limits for Users of Electronic Payment Processing Institutions, to which the provisions of Subparagraphs (4) ~ (7) hereof do not apply.
13. The provisions of Item (3) of Subparagraph 4 and Subparagraph 6 hereof do not apply to electronic stored value card registration operation.

Article 4　If there exists any of the following situations in the CDD process, a financial institution should decline to establish business relationship or carry out any transaction with the customer:

1. The customer is suspected of opening an anonymous account or using a fake name, a nominee, a shell firm, or a shell corporation or entity to open an account, purchase insurance or register an electronic stored value card;
2. The customer refuses to provide the required documents for identifying and verifying its identity;
3. Whereas any person acts on behalf of a customer to open an account, register an electronic stored value card, register an e-payment account, apply for insurance, file an insurance claim, request change of insurance contract or conduct a transaction, it is difficult to check and verify the fact of authorization and identity-related information;
4. The customer uses forged or altered identification documents;
5. The customer only provides photocopies of the identification documents; the preceding provision does not apply to businesses where a photocopy or image file of the identification document supplemented with other control measures are acceptable;
6. Documents provided by the customer are suspicious or unclear so that the documents cannot be authenticated, or the customer refuses to provide other supporting documents;
7. The customer procrastinates in providing identification documents in an unusual manner;
8. The customer is an individual, a legal person or an organization sanctioned under

the Terrorism Financing Prevention Act, or a terrorist or terrorist group identified or investigated by a foreign government or an international anti-money laundering organization, except for payments made under Subparagraphs 2 ~ 4, Paragraph 1, Article 6 of the Terrorism Financing Prevention Act; or

9. Other unusual circumstances exist in the process of establishing business relationship or conducting transaction and the customer fails to provide reasonable explanations.

Article 5 The CDD measures of a financial institution shall include ongoing customer due diligence and observe the following provisions:

1. A financial institution shall apply CDD requirements to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained. The aforementioned appropriate times include at least:
   (1) When the customer opens another new account, registers another new electronic stored value card, registers another new e-payment account, increases the amount insured irregularly or enters new business relationships with the financial institution;
   (2) When it is time for periodic review of the customer scheduled on the basis of materiality and risk; and
   (3) When it becomes known that there is a material change to customer's identity and background information.
2. A financial institution shall conduct ongoing due diligence on the business relationship to scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, its business and risk profile, including, where necessary, the source of funds.
3. A financial institution shall periodically review the existing records to ensure that documents, data or information of the customer and its beneficial owner(s) collected under the CDD process are kept up-to-date and relevant, particularly for higher risk categories of customers, whose reviews shall be conducted at least once every year.
4. A financial institution can rely on existing customer records to undertake identification and verification. Therefore, a financial institution is allowed to carry out transactions without repeatedly identifying and verifying the identity of an existing customer. However, a financial institution shall conduct CDD measures again in accordance with Article 3 herein if it has doubts about the veracity or

adequacy of the records, such as, where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile.

Article 6　A financial institution shall determine the extent of applying CDD and ongoing due diligence measures under Subparagraph 4 of Article 3 and the preceding article using a risk-based approach (RBA):

1. For higher risk circumstances, a financial institution shall perform enhanced CDD or ongoing due diligence measures by adopting additionally at least the following enhanced measures:
   (1) Obtaining the approval of senior management before establishing or entering a new business relationship;
   (2) Taking reasonable measures to understand the sources of wealth and the source of funds of the customer; in case the source of funds is deposits, understand further the source of deposits; and
   (3) Conducting enhanced ongoing monitoring of business relationship.
2. For customers from high ML/TF risk countries or regions, a financial institution shall conduct enhanced CDD measures consistent with the risks identified.
3. For lower risk circumstances, a financial institution may apply simplified CDD measures, which shall be commensurate with the lower risk factors. However simplified CDD measures are not allowed in any of the following circumstances:
   (1) Where the customers are from or in countries and jurisdictions known to have inadequate AML/CFT regimes, including but not limited to those which designated by international organizations on AML/CFT as countries or regions with serious deficiencies in their AML/CFT regime , and other countries or regions that do not or insufficiently comply with the recommendations of international organizations on AML/CFT as forwarded by the Financial Supervisory Commission (FSC); or
   (2) Where there is a suspicion of money laundering or terrorist financing in relation to the customer or the transaction.

The provisions of Items (1) and (2) of Subparagraph 1 of the preceding paragraph do not apply to electronic stored value card registration operation.

An insurance enterprise should consider the beneficiary of a life insurance policy as a relevant risk factor in determining whether to apply enhanced CDD measures. If the insurance enterprise determines that a beneficiary who is a legal person or a trustee presents a higher risk, the enhanced CDD measures should include reasonable measures to identify and verify the identity of the actual beneficiary before making

benefit payout.

Article 7 A financial institution should perform its own CDD operation. However if it is otherwise permitted by law or the FSC that a financial institution may reply on third parties to perform the identification and verification of the identities of customers, agents and beneficial owners or the purpose and intended nature of the business relationship, the financial institution relying on the third party shall still bear the ultimate responsibility for CDD measures and comply with the following provisions:

1. A financial institution relying on a third party should be able to immediately obtain the necessary CDD information.
2. A financial institution should take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.
3. A financial institution shall make sure that the third party it relies on is regulated, supervised or monitored, and has appropriate measures in place for compliance with CDD and record-keeping requirements.
4. A financial institution shall make sure that the jurisdiction at where the third party it relies on is based has AML/CFT regulations in place that are consistent with the standards set out by the FATF.

Article 8 Financial institutions shall observe the following provisions in watch list filtering:

1. A financial institution shall establish policies and procedures for watch list filtering, using a risk-based approach, to detect, match and filter whether customers, or the senior managerial officers, beneficial owners or trading counterparties of customers are individuals, legal persons or organizations sanctioned under the Terrorism Financing Prevention Act or terrorists or terrorist groups identified or investigated by a foreign government or an international anti-money laundering organization.
2. The policies and procedures for watch list filtering shall include at least matching and filtering logics, implementation procedures and evaluation standards, and shall be documented.
3. A financial institution shall document its name and account filtering operations and maintain the records for a time period in accordance with Article 12 herein.

Article 9 Financial institutions shall observe the following provisions for ongoing monitoring of accounts or transactions:

1. A financial institution shall use a database to consolidate basic information and

transaction information on all customers for inquiries by the head office and branches for AML/CFT purpose so as to strengthen the institution's capability of account and transaction monitoring. A financial institution shall also establish internal control procedures for requests and inquiries as to customer information made by various units and shall exercise care to ensure the confidentiality of the information.

2. A financial institution shall establish policies and procedures for account and transaction monitoring using a risk-based approach and utilize information system to assist in the detection of suspicious ML/TF transactions.
3. A financial institution shall review its policies and procedures for account and transaction monitoring based on AML/CFT regulations, nature of customers, business size and complexity, ML/TF trends and related information gathered from internal and external sources, and its risk assessment results, and update those policies and procedures periodically.
4. The policies and procedures for account and transaction monitoring of a financial institution shall include at least complete ML/TF monitoring indicators, and carrying out the setting of parameters, threshold amounts, alerts and monitoring operations, the procedures for examining the monitored cases and reporting standards, and shall be documented.
5. Complete ML/TF monitoring indicators mentioned in the preceding subparagraph shall, based on the business nature of the financial institution, include the suspicious indicators published by the trade associations and the additional ones developed by the financial institution in reference to its ML/TF risk assessment or daily transaction information. With regard to transfer of funds between e-payment accounts, a financial institution should, when carrying out the monitoring, take into consideration all information received on both accounts to determine whether to file a suspicious ML/TF transaction report.
6. A financial institution shall document its ongoing account and transaction monitoring operation and maintain the records in accordance with Article 12 herein.

Article 10 When conducting CDD measures, a financial institution should use self-established database or information obtained from external sources to determine whether a customer and its beneficial owner or senior managerial officer is a person who is or has been entrusted with a prominent function by a domestic government, a foreign government or an international organization (referred to as politically exposed persons (PEPs) hereunder):

1. For a customer or the beneficial owner determined to be a current PEP of a foreign

government, a financial institution shall treat the customer directly as a high-risk customer, and adopt enhanced CDD measures under Subparagraph 1, Paragraph 1 of Article 6 herein.

2. For a customer or the beneficial owner determined to be a current PEP of a R.O.C. government or an international organization, a financial institution shall assess the PEP's risks when establishing business relationship with the person and conduct annual review thereafter. In case of higher risk business relationship with such customers, the financial institution shall adopt enhanced CDD measures under Subparagraph 1, Paragraph 1 of Article 6 herein.
3. For a senior managerial officer of a customer determined to be a current PEP of a R.O.C. government, a foreign government or an international organization, a financial institution shall determine whether to apply the enhanced CDD measures under Subparagraph 1, Paragraph 1 of Article 6 herein by considering the level of influence the officer has on the customer.
4. For a PEP who is no longer entrusted with a prominent public function by a R.O.C. government, a foreign government or an international organization, a financial institution shall assess the level of influence that the individual could still exercise by considering relevant risk factors and determine whether to apply the provisions of the preceding three subparagraphs based on the RBA.
5. The preceding four subparagraphs apply to family members and close associates of PEPs. The scope of family members and close associates mentioned above will be determined in a manner stipulated in the latter section of Paragraph 4, Article 7 of the Act.

Provisions of the preceding paragraph do not apply when the beneficial owner or senior managerial officer of a customer specified under sub-items (A) ~ (C) and (H) of Item (3), Subparagraph 7 of Article 3 herein is a PEP.

Insurance companies and post offices engaging in simple life insurance business should take reasonable measures to identify and verify whether the beneficiary of a life insurance policy, investment-linked insurance policy or annuity insurance policy and the beneficial owner of the beneficiary are PEPs referred to in the preceding paragraph before paying out benefit or cash surrender value. In case high risk circumstances are discovered, an insurance enterprise should, prior to paying out policy proceeds to PEPs, inform senior management, conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a suspicious ML/TF transaction report.

Article 11 Insurance agent companies that solicit insurance policies on behalf of insurance companies in accordance with Article 8 of the Insurance Act and insurance

broker companies that negotiates an insurance policy or provides related services on the basis of the interests of the insured in accordance with Article 9 of the Insurance Act may be exempted from the provisions of ongoing customer due diligence provided in Article 5 and Article 6 herein, the policies and procedures for watch listing filtering provided in Article 8 herein, ongoing monitoring of transactions provided in Article 9 herein and provisions on PEPs in the preceding Article. However if an insurance agent company undertakes underwriting and claim settlement business on behalf of an insurance company, the insurance agent company shall comply with the provisions of these Regulations on insurance company with respect to its policies, procedures and controls for its agency business.

Article 12 A financial institution shall keep records on all business relations and transactions with its customers in hard copy or electronical form and in accordance with the following provisions:

1. A financial institution shall maintain all necessary records on transactions, both domestic and international, for at least five years or a longer period as otherwise required by law.
2. A financial institution shall keep all the following information for at least five years or a longer period as otherwise required by law after the business relationship is ended, or after the date of the occasional transaction:
   (1) All records obtained through CDD measures, such as copies or records of official identification documents like passports, identity cards, driving licenses or similar documents.
   (2) Account files (including e-payment accounts and the accounts of electronic stored value card holders) or contract files.
   (3) Business correspondence, including inquiries to establish the background and purpose of complex, unusual large transactions and the results of any analysis undertaken.
3. Transaction records maintained by a financial institution must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.
4. A financial institution shall ensure that transaction records and CDD information will be available swiftly to the competent authorities when such requests are made with appropriate authority.

Article 13 Financial institutions shall comply with the following provisions with respect to cash transactions above a certain amount:

1. Verify the identity of the customer and keep relevant transaction records.

2. Conduct CDD measures in accordance with the following provisions:
   (1) Check the identity (ID) document or passport provided by the customer and record the customer's name, date of birth, address, telephone, account number, amount of transaction, and ID number. Notwithstanding the foregoing, in case that the customer is confirmed to be exactly the accountholder, it should be clearly noted in the transaction record rather than undertaking a repeated ID verification.
   (2) If the transaction is conducted by an agent, check the identity of the agent by checking his or her ID document or passport and record the name, date of birth, address, and telephone of the agent, account number, amount of transaction, and ID number.
   (3) For occasional transactions, verify the identity of the customer in accordance with Paragraph 4 of Article 3 herein.
3. Except for situations specified in Article 14 herein, report the transaction to the Investigation Bureau, Ministry of Justice (referred to as "Investigation Bureau" hereunder) in a format prescribed by the Investigation Bureau via electronic media in five (5) business days after the completion of transaction. If a financial institution is unable to file a report via electronic media with a legitimate reason, the institution may file a written report after obtaining the consent of the Investigation Bureau.
4. Keep the data reported to the Investigation Bureau and relevant transaction records in accordance with Article 12 herein.

Article 14 A financial institution is not required to file a report on any of the following cash transactions above a certain amount with the Investigation Bureau, provided the financial institution verifies the identity of the customer and keeps the transaction records thereof:

1. Deposits into the accounts opened by government agencies, state-run enterprises, institutions acting with governmental power (within the scope of mandate), public and private schools, public enterprises and government funds established where relevant regulations or contractual relationships so provide.
2. Receivables and payables collected and made by a financial institution on behalf of government treasuries.
3. Transactions and fund arrangements between financial institutions. Notwithstanding the foregoing, payables to another financial institution's customer paid through an inter-bank deposit account, such as a customer cashing the check issued by another financial institution, shall be handled as required, provided the cash transaction of the same customer exceeds a certain amount.

4. Funds paid by a lottery merchant for purchasing lottery tickets.
5. Payments collected on behalf of a third party (excluding payments deposited in designated stock subscription accounts and credit card payments collected) where the payment notice expressly bears the name and ID Card number of the counterparty (including the code which enables tracking of counterparty's identity), and type and amount of transaction. Nevertheless, the duplicate copy of the payment notice shall be kept as the transaction record.

In case of non-individual accounts such as those opened by department stores, megastores, supermarket chains, gas stations, hospitals, transportation businesses and hotels and restaurants which must deposit cash amounting to over a certain amount constantly or routinely in line with business needs, a financial institution may, after verifying the actual business needs, submit the name list to the Investigation Bureau for recordation. Verification and reporting of transactions on a case-by-case basis may be waived for such an account unless the Investigation Bureau responds to the contrary within ten (10) days from the receipt of the name list. A financial institution shall examine the counterparties to the transactions exempted from reporting on a case-by-case basis at least once every year, and report to the Investigation Bureau for recordation if a counterparty no longer has business dealing as mentioned in this paragraph with it.

Article 15 Financial institutions shall file suspicious ML/TF transaction reports in accordance with following provisions:

1. For transactions related to the monitoring patterns under Subparagraph 5 of Article 9 herein or other situations that are deemed as suspicious ML/TF activities, a financial institution shall file a suspicious transaction report (STR) with the Investigation Bureau, regardless of the amount of transaction and regardless whether the transaction was completed or not.
2. Within ten (10) business days upon discovery of a suspicious ML/TF transaction, a financial institution shall promptly file a STR with the Investigation Bureau in a format prescribed by the Bureau after the report has been approved by the responsible chief compliance officer at the institution.
3. For obviously significant suspicious ML/TF transactions of urgent nature, a financial institution should file a report as soon as possible to the Investigation Bureau by fax or other available means and follow it up with a written report. The financial institution is not required to submit a follow-up written report, provided the Investigation Bureau has acknowledged the receipt of report by sending a reply by fax. In such event, the financial institution shall retain the faxed reply.
4. The formats of STR and faxed reply mentioned in the preceding two subparagraphs

shall be prescribed by the Investigation Bureau.

5. The data reported to the Investigation Bureau and relevant transaction records shall be kept in accordance with Article 12 herein.

Article 16 These Regulations shall enter into force on June 28, 2017.