

Chinese National Futures Association

Guidelines for Anti-Money Laundering and Countering Terrorism Financing for Futures Commission Merchants (Template)

Passed in the 11th Joint Session of 3th-term Directors and Supervisors' Meeting on April 27, 2012.

Approved by Financial Supervisory Commission per letter Jin-Guan-Zheng-Fa-Zi-1010020800 dated May 10, 2012.

Passed in the 2nd Joint Session of 4th-term Directors and Supervisors' Meeting on October 18, 2013.

Approved by Financial Supervisory Commission per letter Jin-Guan-Zheng-Chi-Zi-1020044489 dated November 12, 2013.

Passed in the 6th Joint Session of 4th-term Directors and Supervisors' Meeting on April 11, 2014.

Approved by Financial Supervisory Commission per letter Jin-Guan-Zheng-Fa-Zi-1030015225 dated June 17, 2014.

Approved by Financial Supervisory Commission per letter Jin-Guan-Zheng-Fa-Zi-1040024657 dated July 8, 2015.

Article 1

These Guidelines are formulated in accordance with Article 6 of the *Money Laundering Control Act* and the *Directions Governing Anti-Money Laundering and Countering Terrorism Financing of Securities and Futures Sector*.

Article 2

A futures commission merchant (FCM) shall conduct customer due diligence (CDD) and keep records on all business relations and transactions with its customers in accordance with these Guidelines as well as relevant provisions in *Money Laundering Control Act* and *Regulations Governing Cash Transaction Reports (CTR) and Suspicious Transaction Reports (STR) by Financial Institutions*.

Article 3

A FCM shall comply with the following provisions in undertaking CDD measures:

- A. Things to note when accepting customer request to open an account (including natural person and non natural person accounts):
 1. Check two identification documents and save photocopy of customer's national identification (ID) card or document evidencing the legal person status, and ask the customer to specify in the application form their reasons or purposes for opening an account. Where the customer is an individual, check the customer's national ID card and another viable form of identification, such as national health insurance card, passport, driver's license, student ID, household registration transcript, or other

viable ID documents. Where the customer is not an individual, ask the customer to present document evidencing its legal person status, and in addition, the meeting minutes of its board of directors, articles of incorporation or financial statements before the account opening application may be accepted. In addition, the second identification document shall have identifying power.

2. A FCM shall not keep anonymous accounts, accounts in fictitious names, dummy accounts, or accounts opened via a bogus business entity or bogus corporate entity.
 3. Request to open an account shall be politely declined if forged or altered identification documents are used, or if all identification documents presented are photocopies.
 4. Request to open an account shall be politely declined if suspicious or illegible documents or data are provided, or the applicant refuses to provide other supporting data or the documents provided cannot be verified.
 5. Request to open an account shall be politely declined if the customer unreasonably stalls the provision of additional identification documents.
 6. Request to open an account shall be politely declined if there are other irregular circumstances for which the customer fails to provide a reasonable explanation.
 7. When accepting an application to open an account, ascertain whether the customer is well-known political figure in a foreign country. If so, appropriate management measures shall be taken and regularly reviewed. If assessment indicates suspicious signs of money laundering, save the transaction records and support documents and report to the Investigation Bureau, Ministry of Justice.
- B. A FCM shall undertake customer due diligence (CDD) measures when:
1. establishing business relations with a customer;
 2. having doubts about the veracity or adequacy of previously obtained customer identification data;
 3. the address or workplace of the customer is far from the place where the FCM is located and no reasonable explanation is provided therefor or the transaction situation appears to be unusual;
 4. the account which has not been used for transactions for more than one year is suddenly used for carrying out block trades (a trade where each transaction covers more than 100 contracts and the margin or premium involved therein exceeds NT\$10,000,000 and the aggregated transactions within three trading days cover more than 300 contracts and the margin or premium involved therein exceed NT\$30,000,000) involving domestic or foreign futures, options or futures options, or for depositing thereinto or withdrawing therefrom large amount of margin or

premium, which is then quickly transferred out of the account;

5. immediately after opening an account, the account is used for carrying out block trades (a trade where each transaction covers more than 100 contracts and the margin or premium involved therein exceeds NT\$10,000,000 and the aggregated transactions within three trading days cover more than 300 contracts and the margin or premium involved therein exceed NT\$30,000,000) involving domestic or foreign futures, options or futures options, or for depositing thereinto or withdrawing therefrom large amount of margin or premium, which is then quickly transferred out of the account, that the transactions do not appear to be commensurate with the customer's status, income or credit information;
6. an account jointly opened by employees of a company or members of a specific group to carry out frequent large-sum and frequent transactions involving futures, options or futures options;
7. more than three accounts which are not opened under the customer's own name are used to carry out separate, large-sum transactions and the funds are quickly transferred out from those accounts or the situation appears to be irregular;
8. margins or premiums for futures trade are remitted from a country or region that is designated by international organizations on anti-money laundering and countering the terrorism financing (AML/CFT) as a country or region with serious deficiencies in its AML/CFT regime, or from other countries or regions that do not or insufficiently comply with the recommendations of international organizations on AML/CFT as forwarded by the competent authority in charge of the industry and such remittance does not appear to be commensurate with the customer's status and income;
9. there is a suspicion of money laundering or terrorism financing, or carrying out any transactions from a country or region with high money laundering and terrorism financing risk;
10. individuals implicated in special or major cases reported in the media such as TV, newspaper, magazine or the Internet are carrying out transactions at the FCM;
11. the bank account which the customer requests to release the money to is located in any of the countries or economic bodies identified as non-cooperative by the Financial Action Task Force (FATF) (please see <http://www.fatf-fafi.org>);
12. the one who opens an account, carries out transactions, settles futures trading or the account's agent or ultimate beneficiary is a terrorist or terrorist group as forwarded by the competent authority in charge of the industry based on information provided by foreign governments, or a terrorist organization identified or investigated by an

international organization against money laundering; or where the fund for the transaction is suspected to be linked or it is reasonable to suspect that the transaction is linked with a terrorist activity, terrorist organization or terrorism financing; or

13. there are other obviously irregular trading activities or other suspicious circumstances as identified by the FCM's associated persons, regardless of the trading amount or whether the transaction is completed or not.

C. The CDD measures to be taken by a FCM are as follows:

1. Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information. In addition, a FCM 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 where the customer opens an account or conducts a transaction through an agent. In addition, the FCM 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
4. Inquiring information on the purpose and intended nature of the business relationship when undertaking CDD measures.
5. For suspicious customers discovered after opening account, examining and verify the accuracy of the customer information by phone, in writing or via onsite visitation.

D. According to Item 3 of the preceding Subparagraph, a FCM shall obtain the following information to identify the beneficial owners of a customer when the customer is a legal person or a trustee:

1. For legal persons:

- (1) The identity of the natural persons who ultimately have a controlling ownership interest in a legal person. A controlling ownership interest refers to owning more than 25 percents of a company's shares or capital.
- (2) To the extent that there is doubt under (1) above as to whether the person(s) with the controlling ownership interest are the beneficial owner(s) or where no natural person exerting control through ownership interests is identified, the identity of the natural persons (if any) exercising control of the customer through other means.
- (3) Where no natural person is identified under (1) or (2) above, a FCM shall identify and take reasonable measures to verify the identity of relevant natural person who

holds the position of senior managing official.

2. For trustees: the identity of settlor(s), trustee, trust supervisor, beneficiaries, and any other person exercising ultimate effective control over the trust.
3. Unless otherwise provided for in the proviso of Article 4 herein, a FCM is not required to inquire if there exists any beneficial owner in relation to a customer that is:
 - (1) a R.O.C government entity;
 - (2) an enterprise owned by the R.O.C government;
 - (3) a foreign government entity;
 - (4) a public company and its subsidiaries;
 - (5) 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;
 - (6) a financial institution supervised by the R.O.C. government, and an investment vehicles managed by such institution;
 - (7) 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 FATF, and an investment vehicle managed by such institution;or
 - (8) Public Service Pension Fund, Labor Insurance, Labor Pension Fund, or Postal Savings of R.O.C.
4. For customers who refuse to cooperate in CDD, refuse to provide information on the actual beneficiary or who exercise control of the customer, or disincline to provide explanation on the nature and purpose of their transactions or sources of funds, a FCM may suspend the customer from trading or suspend or terminate business relationship with the customer.

E. Ongoing monitoring on accounts and transactions:

1. A FCM or futures business shall conduct ongoing due diligence on the business relationship and scrutiny of 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, their business and risk profile, including, where necessary, the source of funds.
2. A FCM shall periodically review the adequacy of customer identification information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date
3. A FCM is entitled to rely on the identification and verification steps that it has already

undertaken, therefore a securities or futures business is allowed not to repeatedly identify and verify the identity of each customer every time that a customer conducts a transaction unless it has doubts about the veracity of that information. Examples of situations that might lead a securities or futures business to have such doubts could be 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..

- F. A FCM shall apply CDD measures to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

Article 4

A FCM shall determine the extent of applying CDD and ongoing monitoring measures under Subparagraphs (3) and (5) of the preceding article using a risk-based approach (RBA). The enhanced CDD and ongoing monitoring measures shall be applied to those circumstances with higher risk while simplified CDD measures are allowed where a lower risk has been identified. However, simplified CDD measures are not allowed in the following circumstances:

- A. Where the customers are from or in countries and jurisdictions known to have inadequate AML/CFT regimes, including but not limited to those which designated by international organizations on AML/CFT as countries or regions with serious deficiencies in their AML/CFT regime, and other countries or regions that do not or insufficiently comply with the recommendations of international organizations on AML/CFT as forwarded by the Financial Supervisory Commission (FSC); or
- B. Where a FCM suspects that money laundering or terrorism financing is involved.

Article 5

A FCM shall keep records on all business relations and transactions with its customers in accordance with the following provisions:

- A. A FCM shall maintain, for at least five years, all necessary records on transactions, both domestic and international.
- B. A FCM shall keep all the following information for at least five years after the business relationship is ended, or after the date of the occasional transaction:
 - 1. All records obtained through CDD measures, such as photocopies or records of

official identification documents like passport, national ID card, driver's license, or similar documents.

2. Account files.
3. Business correspondence, including inquiries made to establish the background and purpose of complex, unusual large transactions and the results of any analysis undertaken.

Article 6

Risk control mechanism and internal control system:

- A. The risk control mechanism or internal control system established shall contain the following items and the types and extent of control measures adopted should be commensurate with the money laundering and terrorism financing risks and business scale.
 1. In case the transaction exceeds a certain threshold or there is any doubt about the customer but the information provided is insufficient for identifying the client's status, the client's identity shall be verified using other documents issued by the government or other identification documents and put on record.
 2. For discretionary accounts and individuals or groups posing high risks to the goodwill of the FCM, special efforts shall be made to strengthen the verification of customer identity.
 3. Special attention should be paid to non-resident customers to find out the reason for which such customers choose to open an account abroad.
 4. Strengthening the examination of customers who have been in default.
 5. To the extent that no relevant laws are violated, if it is learned or has to be assumed that the sources of customer funds come from embezzlement or abuse of public assets, the FCM shall not accept or terminate the business relationship with the customer.
 6. Utilizing the information system step by step to help identify suspicious transactions.
 7. Strengthening control over high-risk accounts.
 8. If a customer has any of the following situations, the associated person shall politely decline to provide service and report directly to their supervisor:
 - (1) The customer attempts to persuade the associated person not to fill out the information which is required for completing a transaction.
 - (2) The customer inquires the possibility of avoiding declaration of the transaction.
 - (3) The customer is eager to explain that the source of his/her funds is legal or he/she is not trying to launder money.

- (4) The customer's description is obviously not consistent with the transaction itself.
 - (5) The customer attempts to offer benefit to the associated person in order to obtain services from the FCM.
9. Internal process for reporting suspicious transactions and procedure for reporting to the designated authority:
- (1) The internal reporting process shall be as follows: The associated person who discovers any suspicious transaction shall report directly to the department chief, who in turn will forward the report which he/she believes to have merit to the deputy general manager and general manager with a notice to the chief auditor and a report to the chairman of the board to complete the internal reporting process. If any person in the internal reporting process may have an interest in the matter, the associated person may skip reporting to the level of such person and directly report to the manager at a higher level.
 - (2) After completing the internal reporting process, a report on suspicious transaction shall be immediately made to the Investigation Bureau, Ministry of Justice in accordance with regulations set forth in Subparagraph 1 or 2, Article 8 of the *Regulations Governing Cash Transaction Reports (CTR) and Suspicious Transaction Reports (STR) by Financial Institutions*.
 - (3) If a FCM has filed reports with the Investigation Bureau, Ministry of Justice, the FCM shall, within 15 days after the end of each fiscal year, compile the types, signs and items of suspicious money laundering transactions (as provided in Subparagraph 2 of Article 3 herein) and case count reported in the previous year and report the information to the competent authority in charge of the industry for record and send a copy of the same to Taiwan Futures Exchange and the Chinese National Futures Association.
10. Maintaining confidentiality to prevent the reported information and news from being disclosed.
- B. Establishing policies and procedures for identifying, assessing and managing money laundering and terrorism financing risks in accordance with the Guidance on Assessment of Money Laundering and Terrorism Financing Risks and Formulation of Related Control Programs by Futures Commission Merchants (Appendix), and an AML/CFT program based on said Guidance and the result of risk assessment.
1. A FCM shall periodically review its internal control measures to determine whether the measures are adequate to prevent money laundering and review these Guidelines periodically every year to determine if revision is necessary.

2. A FCM shall establish an appropriate process for prudently selecting/recruiting employees, including examining the integrity of character of prospective employees and the professional knowledge required to perform their duties, especially for employees who will be responsible for performing prevention of money laundering and countering terrorism financing. In addition, attention should be paid to any potential conflict of interest between employees and their duties of preventing money laundering and countering terrorism financing.
 3. The FCM's business department shall conduct regular on-the-job training on money laundering prevention every year or arrange for employees to attend relevant training courses or workshops to enhance their judgment and enable them to fully understand money laundering characteristics and patterns of suspicious transactions.
 4. A deputy general manager (or an officer at comparable position) who has attended the training classes in connection with money laundering prevention shall be appointed to act as the designated compliance officer (the newly appointed officer shall attend such training courses within six months of appointment) and a unit shall be designated to take charge of the coordination and supervision of risk management concerning anti-money laundering and countering terrorism financing.
 5. A FCM should reward employees who have contributed to crime busting by the law enforcement due to their reporting of suspicious money laundering activities, and reward associated persons who have performed well in attending relevant overseas seminars on money laundering prevention or have collected and researched laws and regulations of foreign countries which provide valuable information to the FCM in its money laundering prevention activities.
- C. A standard operating procedure to comply with the AML/CFT regulations, which shall be included in the self-inspection and internal audit system. The internal audit unit's responsibilities in connection with this task are as follows:
1. A FCM shall incorporate the Guidelines for Anti-Money Laundering and Countering Terrorism Financing into its internal control system, and the internal audit unit shall conduct regular audits according to the internal control measures and established audit guidelines, the test the effectiveness of its AML/CFT program as well as the risk management quality of company operations, departments and branches.
 2. If the internal auditors find any deficiencies in the anti-money laundering operations performed by any unit, they shall report the matter regularly to the designated compliance officer or an officer holding comparable position and offer improvement suggestions for reference in on-the-job training of associated persons.

3. If an internal auditor intentionally conceals any material violation discovered, the responsible unit shall take appropriate actions to address the matter.
 4. The internal audit unit may conduct random checks on block trades and look into the legality of such trades.
- D. To the extent that the laws and regulations of host countries or jurisdictions so permit, a FCM shall ensure that its foreign branches and subsidiaries comply with the AML/CFT measures as stringent as those in Taiwan. In the event the minimum requirements in the countries at where the head office and the branch office are located differ, the branch office shall choose the higher standard of the two jurisdictions as the basis for compliance. If there is any doubt as to which standard is higher, the determination of the competent authority of the country at where the parent company is located shall prevail. If the same standard as that adopted by the head office cannot be adopted because it is prohibited by the foreign laws and regulations, the head office shall adopt suitable additional measures to manage money laundering and terrorism financing risks and report the situation to the competent authority in charge of the industry.
- E. Branches or subsidiaries of foreign financial groups in Taiwan shall establish policies and procedures for identifying, assessing and managing money laundering and terrorism financing risks in accordance with the Guidance on Assessment of Money Laundering and Terrorism Financing Risks and Formulating Related Control Programs by Futures Commission Merchants (Appendix). However if those policies and procedures have been established by the parent company, which are not less than the requirements in Taiwan and do not violate Taiwan's laws and regulations, the branch or subsidiary may adopt the policies and procedures of the parent company.

Article 7

These Guidelines shall be implemented after being approved by the Board of Directors (or the responsible department authorized by delegation) and shall be submitted to the competent authority in charge of the industry for record. The same shall apply to the modification of the Guidelines thereof.