Content

Title：	Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises or Persons Providing Virtual Asset Services Ch
Date：	2024.11.26
Legislative：	1. Full text of 18 articles issued per 30 June 2021 Order No. Financial-Supervisory-Banking-Legal-11002720401 of the Financial Supervisory Commission, for enforcement from 1 July 2021 2. Name and full text of 18 articles amended and issued per 26 November 2024 Order No. Financial-Supervisory-Securities-Firms-11303860246 of the Financial Supervisory Commission; for enforcement from 30 November 2024, except for Article 7, which shall be enforced from a date to be separately specified by the FSC (Original name: Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises Handling Virtual Currency Platform or Transaction) (Errata amended per 17 February 2025 per Letter No. Financial-Supervisory-Securities-Firms-1140380639 of the Financial Supervisory Commission)
Content：	Article 1 These Regulations are adopted pursuant to Article 7, paragraph 3, Article 8, paragraph 4 (the fore part), Article 10, paragraph 3, Article 12, paragraph 3, and Article 13, paragraph 3 of the Money Laundering Control Act, applied mutatis mutandis under Article 5, paragraph 2 of that Act, and to Article 7, paragraph 5 of the Counter-Terrorism Financing Act. Article 2 Terms used in these Regulations are defined as follows: 1. "Enterprise or person providing virtual asset services" ("virtual asset service provider"; "VASP"): means an enterprise or person engaging within Taiwan in the activities listed below on behalf of others. A. Exchange between virtual assets and the New Taiwan dollar (NTD), foreign currency, or currency issued by Mainland China, Hong Kong, or Macao. B. Exchange between virtual assets. C. Transfer of virtual assets. D. Safekeeping or administration of virtual assets or providing instruments enabling control over virtual assets. E. Participation in and provision of financial services relating to the issuance or sale of virtual assets. 2. "Virtual asset": means a digital representation of value with the use of cryptography and distributed ledger technology or other similar technology that can be digitally stored, exchanged, or transferred, and can be used for payment or investment purposes. However, virtual assets do not include digital representations of NTD, foreign currency, currency issued by Mainland China, Hong Kong, or Macao, securities, and other financial assets issued in accordance with laws and regulations. 3. "Establish a business relationship": means the acceptance of a customer's application for registration or establishment of similar business transaction relationships. 4. "Occasional transaction": means a transaction involving any of the activities under subparagraph 1 with anyone with whom a business relationship has not been established. 5. "Beneficial owner" means the natural person(s) who ultimately owns or controls the customer, or the natural person(s) on whose behalf a transaction is conducted, including the natural person(s) who has ultimate

effective control over a juristic person or legal arrangement.
6. "Risk-based approach" (RBA): means the VASP shall identify, assess, and understand the money laundering and terrorist financing ("ML/TF") risks to which it is exposed and take appropriate anti-money laundering and countering of terrorist financing ("AML/CFT") measures commensurate with those risks in order to effectively mitigate them. Based on the RBA, the VASP shall take enhanced measures for higher risk situations, and may take relatively simplified measures for lower risk situations, to allocate resources efficiently and use the most appropriate and effective approach to mitigate the identified ML/TF risks.
The term "VASP" in subparagraph 1 of the preceding paragraph refers only to those that have completed registration in accordance with the Regulations Governing Anti-Money Laundering Registration of Enterprises or Persons Providing Virtual Asset Services.
When any of the financial institutions specified in Article 5, paragraph 1 of the Money Laundering Control Act engages in any of the activities specified in the items in paragraph 1 herein, it shall do so in accordance with the related AML regulations established by its respective central competent authority governing the target business and these Regulations shall not apply.

Article 3
A VASP shall comply with the following provisions when undertaking customer due diligence (CDD) measures:
1. The VASP shall not accept anonymous accounts or accounts in fictitious names for establishing or maintaining business relationships.
2. The VASP shall undertake CDD measures when:
A. Establishing a business relationship with any customer.
B. Carrying out an occasional transaction equal to or above NTD$30,000 or the equivalent, or multiple occasional transactions that are obviously related with a sum total equal to or above NTD$30,000 or the equivalent.
C. There is a suspicion of money laundering or terrorist financing.
D. The VASP has doubts about the veracity or adequacy of previously obtained customer identification data.
3. CDD measures shall be taken as follows:
A. Identifying the customer and verifying the customer's identity using reliable, independent source documents, data or information.
B. Verifying that any person purporting to act on behalf of the customer is so authorized, and identifying and verifying the identity of that person using the methods specified in the preceding item.
C. Identifying the beneficial owner of a customer and taking reasonable measures to verify the identity of the beneficial owner, including using data or information from a reliable source.
D. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship when undertaking CDD measures.
4. When the customer specified in the preceding subparagraph is a natural person, the VASP shall obtain at least the following information on the customer to identify and verify the customer's identity:
A. Name.
B. Official identity document number.
C. Date of birth.
D. Nationality.
E. Household registration or residence address.
5. When the customer specified in subparagraph 3 is a juristic person, an organization, or a trustee of a trust, the VASP shall understand the business nature of the customer or trust (including a legal arrangement similar to a trust) and obtain at least the following information to identify the customer or the trust and verify its identity:
A. Name, legal form, and proof of existence of the customer or trust.
B. The articles of incorporation/association or similar power documents that regulate and bind the juristic person or trust, except in any of the following circumstances:
a. Those listed under subparagraph 7, item C hereof without the situations specified in the proviso of subparagraph 3 of Article 6 herein.
b. A customer that is an organization that is verified as not having

articles of incorporation/association or similar power document.
C. Names of the relevant persons having a senior management position in the customer.
D. The address of the registered office of the customer and the address of its principal place of business.
6. When the customer is a juristic person, the VASP shall understand whether the customer is able to issue bearer shares and apply appropriate measures for customers who have issued bearer shares to ensure the information on their beneficial owners is kept up to date.
7. When the customer specified in item C of subparagraph 3 is a juristic person, an organization, or a trustee of a trust, the VASP shall 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:
A. When the customer is a juristic person or organization:
a. The identity of the natural person(s) who ultimately has a controlling interest in the juristic person. A controlling interest means holding directly and/or indirectly 25 percent or more of the juristic person's shares or capital; the VASP may ask the customer to provide its list of shareholders or other documents to assist in the identification of persons holding a controlling interest.
b. To the extent that no natural person with controlling interest is identified under the preceding sub-item or that there is doubt as to whether the person(s) with the controlling 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, the VASP shall identify the natural person who holds the position of senior managing official.
B. For a customer that is a trustee of a trust: 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 positions.
C. Unless otherwise provided for in the proviso of subparagraph 3 of Article 6 or where the customer has issued bearer shares, the VASP is not subject to the requirements of identifying and verifying the identity of beneficial owner(s) of a customer set out under item C of subparagraph 3 hereof if the customer or the person having a controlling interest in the customer is:
a. an ROC government agency;
b. an enterprise owned by the ROC government;
c. a foreign government agency;
d. an ROC public company or its subsidiary;
e. a company listed on a stock exchange outside the ROC that is subject to regulatory disclosure requirements of its principal shareholders, or a subsidiary of such a company;
f. a financial institution supervised by the ROC government or an investment vehicle managed by such an institution;
g. a financial institution established outside the ROC that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the Financial Action Task Force (FATF), or an investment vehicle managed by such an institution;
h. a fund administered by an ROC government agency;
i. an employee stock ownership trust or an employee savings trust.
8. The VASP shall perform CDD measures by itself. However, if it is otherwise permitted by law or regulation to rely on third parties to perform the identification and verification of the identities of customers, agents, and beneficial owners or the purpose and nature of the business relationship, such a VASP relying on a third party shall still bear the ultimate responsibility for CDD measures and comply with the following provisions:
A. The VASP shall be able to immediately obtain the necessary CDD information.
B. The VASP shall 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 by the VASP without delay.
C. The VASP shall ensure 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.
D. The VASP shall make sure that the jurisdiction where the third party it relies on is located has AML/CFT regulations in place consistent with the standards set out by the FATF.
9. The VASP shall not establish a business relationship with a customer or conduct occasional transactions with a value equal to or above than NTD$30,000 or the equivalent before completing the CDD measures.
10. If the VASP is unable to complete the required CDD process on a customer, it shall consider filing a suspicious transaction report on money laundering or terrorist financing (STR) in relation to the customer.
11. If the VASP 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.

Article 4
If any of the following situations exists in the CDD process, the VASP shall decline to establish a business relationship or carry out any transaction with the customer:
1. The customer is suspected of opening an anonymous account or using a fictitious name, a nominee, a shell business, or a shell juristic person/organization to establish a business relationship.
2. The customer refuses to provide the required documents for identifying and verifying its identity.
3. Any person acts on behalf of a customer to establish a business relationship or conduct a transaction, and it is difficult to check and verify the fact of the authorization and identity-related information.
4. The customer uses forged or altered identification documents.
5. Documents provided by the customer are suspicious or unclear, and the customer refuses to provide other supporting documents or documents provided by the customer cannot be verified.
6. The customer procrastinates in providing identification documents in an unusual manner.
7. The customer is an individual, a juristic person or an organization sanctioned under the Counter-Terrorism Financing Act, or a terrorist or terrorist group identified or investigated by a foreign government or an international organization, except for payments made under Article 6, paragraph 1, subparagraphs 1 to 3 of the Counter-Terrorism Financing Act.
8. Other unusual circumstances exist in the process of establishing a business relationship or conducting a transaction and the customer fails to provide reasonable explanations.

Article 5
The CDD measures of the VASP shall include ongoing customer due diligence and comply with the following provisions:
1. The VASP shall apply CDD requirements to existing customers on the basis of materiality and risk and 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 shall include at least:
A. When the customer enters any new business relationship with the VASP.
B. When it is time for periodic review of the customer scheduled on the basis of materiality and risk.
C. When it becomes known that there is a material change to a customer's identity and background information.
2. The VASP 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 and its business and risk profile, including, when necessary, the source of funds.
3. The VASP shall periodically review the existing customer records to ensure that the information of the customer and its beneficial owner(s)

collected under the CDD process are adequate and kept up-to-date, particularly for high-risk customers, whose reviews shall be conducted at least once every year.
4. The VASP may rely on existing customer records to undertake identification and verification without the need to repeatedly identify and verify the identity of an existing customer when carrying out transactions. However, the VASP shall conduct CDD measures again in accordance with Article 3 when it has doubts about the veracity or adequacy of the records, where there is a suspicion of ML/TF in relation to that customer, or where there is a material change in the way that the customer's transaction is conducted or the customer's account is operated, which is not consistent with the customer's business profile.

Article 6
The VASP shall determine the extent of application of CDD and ongoing due diligence measures under Article 3, subparagraph 3 and the preceding article based on a risk-based approach (RBA):
1. For higher risk circumstances, the VASP shall perform enhanced CDD or ongoing due diligence measures, including adopting at least the following additional enhanced measures:
A. Obtaining the approval of senior management of the VASP before establishing or entering a new business relationship.
B. Taking reasonable measures to understand the sources of wealth and the source of funds of the customer. The aforementioned source of funds refers to the substantial source from which the funds generate.
C. Conducting enhanced ongoing monitoring of the business relationship.
2. For customers from high ML/TF risk countries or regions, the VASP shall conduct enhanced CDD measures commensurate with the risks identified.
3. For lower risk circumstances, the VASP 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:
A. The customers are from or in countries or regions known to have inadequate AML/CFT regimes, including but not limited to those which are 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.
B. There is a suspicion of ML/TF in relation to the customer or the transaction.

Article 7
If the VASP serves as the originating party of a virtual asset transfer, it shall comply with the following provisions:
1. The VASP shall obtain required and accurate information on the customer transferring the virtual assets ("the originator") and required information on the customer receiving the virtual assets ("the beneficiary"), and shall maintain previously acquired information in accordance with Article 10, and submit the information mentioned above immediately and securely to the enterprise serving as the beneficiary party. Law enforcement authorities should be able to compel immediate production of such information and the VASP shall cooperate accordingly.
2. The required information of the aforementioned originator and beneficiary specified in the preceding subparagraph includes:
A. Information of the originator shall include the name of the originator, information on the wallet used for transferring the virtual assets, and one of the following items of information of the originator:
a. Official identity document number.
b. Address.
c. Date and place of birth.
B. Information of the beneficiary shall include the name of the beneficiary and information on the wallet used for receiving the virtual assets.
3. When the VASP fails to conduct the transfer in accordance with the two preceding subparagraphs, it is not allowed to execute the virtual asset transfer.
If the VASP serves as the beneficiary party of virtual asset transfers, it

shall comply with the following provisions:
1. Take reasonable measures to identify virtual asset transfers that lack the required information specified in subparagraph 2 of the preceding paragraph.
2. Have risk-based policies and procedures for determining when to execute, reject, or suspend a virtual asset transfer lacking the required information specified in subparagraph 2 of the preceding paragraph, and the appropriate follow-up action.
3. Maintain the information on the originator and beneficiary in accordance with Article 10.
When the VASP transfers virtual assets, it shall verify that the transaction counterparty (originating party or beneficiary party) is subject to and supervised for compliance with AML/CFT requirements consistent with the standards set by the Financial Action Task Force on Money Laundering (FATF).

Article 8
The VASP shall establish policies and procedures for watch list filtering of names and titles/accounts of customers and transaction counterparties, based on a risk-based approach, to detect, match, and filter whether customers, their beneficial owners, or parties connected to the transactions are individuals, juristic persons, or organizations sanctioned under the Counter-Terrorism Financing Act or terrorists or terrorist groups identified or investigated by a foreign government or an international organization.
The VASP shall document its name and title/account filtering operations and maintain the records for a time period in accordance with Article 10.

Article 9
When conducting CDD measures, the VASP shall put in place risk management systems to determine whether a customer or its beneficial owner is a person who is or has been entrusted with a prominent function by a domestic government, a foreign government, or an international organization ("politically exposed person"; "PEP"):
1. For a customer or a beneficial owner thereof determined to be a current PEP of a foreign government, the VASP shall directly deem the customer to be a high-risk customer and adopt enhanced CDD measures under the items of subparagraph 1 of Article 6.
2. For a customer or the beneficial owner thereof determined to be a current PEP of the domestic government or an international organization, the VASP shall assess the PEP's risks when establishing a business relationship with the PEP and conduct annual review thereafter. In cases of a higher risk business relationship with such customers, the VASP shall adopt enhanced CDD measures under the items of subparagraph 1 of Article 6.
3. For a PEP who is no longer entrusted with a prominent public function by the domestic government, a foreign government, or an international organization, the VASP shall assess the influence that the individual could still exercise by considering relevant risk factors and determine whether to apply the provisions of the two preceding subparagraphs based on the RBA.
4. The three preceding subparagraphs shall also apply to family members and close associates of PEPs.
The scope of PEPs, their family members, and close associates mentioned in the preceding paragraph will be determined by the standards provided in the latter part of paragraph 4 of Article 8 of the Money Laundering Control Act.
The provisions of paragraph 1 do not apply when a beneficial owner of any of those specified in Article 3, subparagraph 7, item C, sub-items a to c and h is a PEP.

Article 10
The VASP shall keep records and evidence of all business relations and transactions with its customers in hard copy or electronic form and in accordance with the following provisions:
1. The VASP shall maintain all necessary records on domestic and international transactions for at least 5 years or a longer period as

otherwise required by law.
2. The VASP 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 occasional transaction is concluded:
A. All records obtained through CDD measures, such as copies or records of passports, identity cards, driving licenses or other similar official identification documents.
B. Contract document files.
C. Business correspondence, including information obtained from inquiries regarding the background and purpose of complex, unusual large transactions and any analysis undertaken.
3. The transaction records maintained shall be sufficient to reconstruct individual transactions so as to provide evidence for determination of illegal activity.
4. The VASP shall ensure that transaction records and CDD and related information will be available swiftly to the competent authorities when such requests are made with appropriate authority.

Article 11
The VASP shall report cash transactions with an amount equal to or above NTD$500,000 (including its equivalent in foreign currencies and currencies issued by Mainland China, Hong Kong, or Macao) to the Investigation Bureau, Ministry of Justice within 5 business days after the transaction.
The data reported to the Investigation Bureau, Ministry of Justice under the preceding paragraph and related records and evidence shall be kept in accordance with the preceding article.

Article 12
The VASP shall comply with the following provisions for ongoing monitoring of customer transactions:
1. The VASP shall establish policies and procedures for transaction monitoring based on a risk-based approach and may utilize information systems to assist in the detection of suspicious ML/TF transactions. It shall review its policies and procedures for transaction monitoring on a regular basis.
2. The policies and procedures for transaction monitoring in the preceding subparagraph shall include at least complete monitoring indicators, parameter setting, threshold amounts, alerts and operation procedures of monitoring, review procedures for monitored cases, and reporting standards, and shall be documented in writing.
3. The VASP shall document its implementation of transaction monitoring and maintain the records for a time period in accordance with Article 10.
The VASP shall file suspected ML/TF transaction reports in accordance with following provisions:
1. For a transaction that exhibits the monitoring indicators or other irregularities set out under subparagraph 2 of the preceding paragraph, the VASP shall complete the review process as quickly as possible to determine whether the transaction is suspected of involving ML/TF activity, and shall retain records.
2. If the review has resulted in a determination that a transaction is suspected of involving ML or TF activity, regardless of the amount of the transaction, the VASP shall promptly file an STR with the Investigation Bureau, Ministry of Justice in a format prescribed by the Bureau after the report has been approved by the responsible compliance officer of the VASP. The report shall be filed within 2 business days following such approval. The same shall apply to attempted transactions.
3. For obviously significant suspected ML/TF transactions of an urgent nature, the VASP shall immediately file a report to the Investigation Bureau, Ministry of Justice by fax or other feasible means as soon as possible.
4. The VASP shall keep the data reported to the Investigation Bureau, Ministry of Justice and related records and evidence in accordance with Article 10.

Article 13
When a VASP files a report under Article 7, paragraph 3 of the Counter-

Terrorism Financing Act, it shall comply with the following provisions:
1. After learning of the case, the VASP shall submit the report for approval by the responsible compliance officer, and then promptly file the report with the Investigation Bureau, Ministry of Justice in the format and manner prescribed by the Bureau. The report shall be filed within 2 business days following such approval.
2. In the event of an obviously significant and urgent case, the VASP shall immediately file a report to the Investigation Bureau, Ministry of Justice by fax or other feasible means as soon as possible.
Records of reports mentioned in the preceding paragraph and related records and evidence shall be maintained in accordance with Article 10.

Article 14
The VASP shall take appropriate measures to identify, assess, and understand its ML/TF risks. The measures shall at least cover the customers, countries, or geographic areas, products, services, transactions, or delivery channels and be handled in accordance with the following provisions:
1. A risk assessment report shall be prepared every year and submitted by letter to the Financial Supervisory Commission by the end of March of the following year for recordation.
2. The risk assessment shall consider all risk factors to determine the level of overall risk, and appropriate measures to mitigate the risks.
3. The VASP shall ensure that the risk assessment report is regularly updated.

Article 15
A VASP shall establish internal audit and internal control systems for AML/CFT operations based on the Money Laundering Control Act, Counter-Terrorism Financing Act, these Regulations, Regulations Governing Anti-Money Laundering Registration of Enterprises or Persons Providing Virtual Asset Services, and the self-regulatory rules of the Taiwan Virtual Asset Service Provider Association, and based on its ML/TF risks and business size. The system and any subsequent amendments thereto shall be approved by the board of directors. The content of the systems shall include the following matters:
1. AML/CFT operations and control procedures.
2. Appointing an AML/CFT compliance officer at the management level for coordinating and supervising AML/CFT operations.
3. Establishing screening procedures to ensure high standards when hiring employees, and ongoing employee training programs, including examining whether the prospective employee has character integrity and the professional knowledge required to perform their duties, and regularly organizing or participating in on-the-job training for AML/CFT operations.
4. Preparing and periodically updating the ML/TF risk assessment report.
5. An independent audit function to test the effectiveness of the AML/CFT system.
6. Other matters required by AML/CFT regulations and the FSC.
The policies, controls, and procedures established in the systems in the preceding paragraph shall be approved by the senior management, to enable the VASP to manage and mitigate ML/TF risks, including those that have been identified either by the country or the VASP itself. The VASP shall monitor the implementation of those controls and enhance them if necessary. Where higher risks are identified, it shall take enhanced measures to manage and mitigate the risks.
The AML/CFT compliance officer specified in paragraph 1, subparagraph 2 shall meet one of the following qualification requirements within 3 months after appointment, and the VASP shall establish relevant control mechanisms to ensure compliance with the provisions hereof:
1. Having served as a legal compliance officer or AML/CFT compliance officer, appointed in accordance with laws and regulations, on a full-time basis for at least 3 years.
2. Having attended at least 24 hours of courses offered by institutions recognized by the FSC, passed the exams, and received completion certificates therefor.
3. Having received an AML/CFT professional certificate issued by an

international or domestic institution recognized by the FSC.
The VASP shall implement on-the-job training in accordance with paragraph 1, subparagraph 3 of the following provisions:
1. The AML/CFT compliance officer specified in paragraph 1, subparagraph 2 shall annually attend at least 12 hours of training on AML/CFT. The training shall cover at least newly amended laws and regulations, trends, and typologies of ML/TF risks. If the person has obtained an AML/CFT professional certificate issued by an international or domestic institution recognized by the FSC in a current year, the certificate may be applied against the training hours for the year.
2. The VASP shall annually arrange appropriate hours and contents of orientation and on-the-job training on AML/CFT for its directors, supervisors, president, legal compliance officers, internal auditors, and business personnel in view of the nature of its business, to familiarize them with their AML/CFT duties and equip them with the professional knowhow to perform their duties.
The VASP shall arrange sufficient and competent legal compliance personnel.
With respect to the audit functions specified in paragraph 1, subparagraph 5, the VASP shall conduct an independent audit on the following matters and submit audit opinions:
1. Whether the ML/TF risk assessment and the AML/CFT policies, controls, and procedures meet the regulatory requirements and are implemented.
2. The effectiveness of the AML/CFT policies, controls, and procedures.

Article 16
The VASP shall conduct ML/TF risk identification and assessments before launching new products or services or conducting new types of business. It shall also establish corresponding risk management measures to mitigate identified risks.

Article 17
With respect to the VASP's implementation of AML/CFT, the FSC may, at any time, appoint a designee or entrust an appropriate institution to conduct an audit using the risk-based approach, using audit methods including on-site audit and off-site audit. When necessary, it may designate or require the VASP to engage professional and technical personnel to conduct an audit of the VASP's implementation of AML/CFT and submit a report to the FSC. The expenses shall be borne by the audited entity.
When the FSC conducts an audit under the preceding paragraph, it may order the VASP to provide AML/CFT-related books, documents, electronic data files, or other relevant materials. The aforementioned materials, whether stored in hard copy, electronic files, email, or any other form, shall be provided, and the VASP shall not circumvent, reject, or obstruct the audit for any reason.

Article 18
These Regulations shall enter into force from 30 November 2024, except for Article 7, which shall enter into force from a date to be separately specified by the FSC.

Files： 33Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises or Persons Providing Virtual Asset Services(113.11.26).txt