Regulations and guidelines 4/2019

Virtual currency providers

J. No
FIVA 12/01.00/2019

Issued
14/06/2019

Valid from
01/07/2019

Further information from
Digitalisation and
Analysis/Digitalisation and Banking
Services

FINANCIAL SUPERVISORY AUTHORITY
tel. +358 9 183 51
firstname.surname@fiva.fi
fin-fsa.fi

FIN-FSA
FINANCIAL SUPERVISORY AUTHORITY

Legal nature of regulations and guidelines

Regulations

Financial Supervisory Authority (FIN-FSA) regulations are presented under the heading ‘Regulation’ in the FIN-FSA's regulations and guidelines. FIN-FSA regulations are binding legal requirements that must be complied with.

The FIN-FSA issues regulations only by virtue of and within the limits of legal provisions that entitle it to do so.

Guidelines

FIN-FSA interpretations of the contents of laws and other binding provisions are presented under the heading ‘Guideline’ in the FIN-FSA's regulations and guidelines.

Also recommendations and other operating guidelines that are not binding are presented under this heading, as are the FIN-FSA’s recommendations on compliance with international guidelines and recommendations.

The formulation of the guideline shows when it constitutes an interpretation and when it constitutes a recommendation or other operating guideline. A more detailed description of the formulation of guidelines and the legal nature of regulations and guidelines is provided on the FIN-FSA website.

fin-fsa.fi > Regulation > Legal framework of FIN-FSA regulations and guidelines

Contents

1 Scope of application and definitions

1.1 Scope of application

These regulations and guidelines are applicable to the following other financial market participants as referred to in section 5 of the Act on the Financial Supervisory Authority (878/2008):

- virtual currency providers as referred to in section 2 of the Act on Virtual Currency Providers (572/2019).

1.2 Definitions

For the purposes of these regulations and guidelines, the following definitions apply:

- *Supervised entity* refers to all supervised entities falling within the scope of section 1.1 of these regulations and guidelines.
- *Application* refers to a registration application as mentioned in section 5 of the Act on Virtual Currency Providers.
- *Virtual currency* refers to a virtual currency defined in section 2, subsection 1, paragraph 1 of the Act on Virtual Currency Providers (572/2019).
- *Virtual currency provider* refers to participants defined in section 2, subsection 1, paragraph 2 of the Act on Virtual Currency Providers (572/2019).
- *Service related to virtual currency* refers to services mentioned in section 2, subsection 1, paragraph 6 of the Act on Virtual Currency Providers (572/2019).
- *Money laundering* refers to activities mentioned in chapter 32, sections 6–10 of the Criminal Code of Finland (39/1889).
- *Terrorist financing* refers to activities mentioned in chapter 34 a, sections 5 and 5 a of the Criminal Code of Finland (39/1889).
- *Obliged entity* refers to virtual currency provider mentioned in chapter 1, section 2, subsection 1, paragraph 8 a of the Anti-Money Laundering Act.

2 Legal framework and international recommendations

2.1 Legislation

The following statutes relate to the matters addressed in these regulations and guidelines:

- Act on Virtual Currency Providers (572/2019).
- Act on Preventing Money Laundering and Terrorist Financing (444/2017, hereinafter the Anti-Money Laundering Act or AMLA)
- Act on the Financial Supervisory Authority (878/2008, hereinafter the Act on the FIN-FSA)
- Act on the Financial Intelligence Unit (445/2017).

2.2 European Union Directives

The following European Union Directives are related to the matters addressed in these regulations and guidelines:

- Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (hereinafter 'the 4th AML Directive')
- Directive (EU) 2018/843 of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (hereinafter 'the 5th AML Directive').

2.3 The FIN-FSA's authority to issue regulations

The FIN-FSA's authority to issue binding regulations is based on the following legal provisions:

- section 11, subsection 2 of the Act on Virtual Currency Providers
- section 11, subsection 4 of the Act on Virtual Currency Providers
- section 13, subsection 4 of the Act on Virtual Currency Providers.

2.4 International recommendations

The following recommendations and guidance by the Financial Action Task Force (FATF) are related to the matters addressed in these regulations and guidelines:

- International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - The FATF Recommendations (published 16 February 2012)
- FATF Guidance for a Risk-Based Approach to Virtual Currencies (published June 2015).

3 Objectives

(1) These regulations and guidelines comprise the FIN-FSA's regulations, guidelines, recommendations and interpretations on the holding of client assets and on compliance with regulations on customer due diligence and on the prevention and uncovering of money laundering and terrorist financing.

(2) The objective of these regulations and guidelines is to provide guidance for market entry, to enhance the registration process and to provide guidance for market operation. The regulations and guidelines highlight which additional matters aside from the requirements laid down in legislation the FIN-FSA will pay particular attention to when assessing whether a natural or legal person submitting a registration application meets the requirements for providing virtual currency services. The requirements for registration must be fulfilled throughout the activity of the sole proprietorship or entity.

(3) The objective of the regulations and guidelines is to clarify the position of virtual currencies as client assets and to regulate and guide the safeguarding and proper holding of virtual currencies classified as client assets.

(4) It is the FIN-FSA's task to supervise that supervised entities' procedures for customer due diligence and risk management comply with statutory requirements. The supervised entity, and if the supervised entity is a legal person, may be subject to an administrative sanction prescribed in chapter 8 of the AMLA for failure to comply with its obligations under said Act.

4 Safeguarding and holding of client assets

(5) Client assets of a virtual currency provider may include virtual currencies and assets.

(6) For the purposes of this chapter and chapters 4.1 and 4.2, the term ‘assets’ shall refer to cash, monetary value stored on an account, and electronic money.

(7) The obligation to safeguard client assets has been prescribed in order to compensate for, inter alia, no capital requirements for own funds being imposed on virtual currency providers.

(8) For the purposes of this chapter and chapters 4.1, 4.2, and 4.3, the term ‘risk assessment’ shall refer to a risk assessment concerning the safeguarding and holding of client assets.

(9) The objective of the regulations and guidelines presented in this chapter is to achieve the following:

- the supervised entity shall safeguard all assets and virtual currencies received for purposes of virtual currency exchange
- the supervised entity shall hold all assets received for purposes of virtual currency exchange in a manner that prevents them from being commingled with the assets of another service user, service provider or its own assets
- the virtual currencies of each client must be reliably distinguishable from virtual currencies belonging to other clients and from the virtual currency provider’s own virtual currencies
- the supervised entity shall monitor for malfunctions and errors in the safeguarding and holding of client assets and the damage caused thereby.

4.1 Regulations and guidelines concerning the holding and safeguarding of all client assets

(10) For the purposes of this chapter and chapter 4.3, the term ‘information system’ shall refer to information systems used for receiving, holding, and transferring virtual currencies belonging to client assets.

(11) For the purposes of this chapter and chapter 4.3, the term ‘control’ shall refer to procedures in order to ensure that operational goals are reached. Controls include all measures taken to prevent, detect and mitigate disruptions, shortcomings, faults and misuse. Examples of controls include reconciliation tasks, the four-eye principle, and comparison of counterparties' confirmations with the supervised entity’s own contract documentation.

(12) By virtue of section 11, subsection 4 of the Act on Virtual Currency Providers, the FIN-FSA may issue more detailed regulations on the holding and safeguarding of client assets.

REGULATION (paragraphs 13 – 17)

(13) Supervised entities shall draw up a risk assessment of the holding and safeguarding of client assets.

(14) The risk assessment shall comprise the necessary reviews on the principles for client asset safeguarding and holding in the event of cessation of business or transfer of business. The risk

assessment shall also include a plan for the restoration of client assets in aforementioned situations.

(15) Supervised entities shall determine a recovery time objective (RTO) for processes relating to the exchange and holding of client assets, i.e. a maximum acceptable interruption time that would not disrupt business activities. Alternative modes of operation and recovery procedures shall be set up for these processes in case of disruptions. Special attention shall be paid to the restoration of information that is crucial for the resumption of business activities.

(16) Supervised entities shall keep records of their own assets and client assets. Supervised entities shall ensure the integrity, availability and confidentiality of the accounting data. Information systems shall be equipped with built-in controls allowing reconciliation of accounting data and stored assets.

(17) Supervised entities shall define key processes relating to the safeguarding and holding of client assets. Supervised entities shall have sufficient controls to ensure proper safeguarding of client assets and to reduce the level of personal risk associated with processing to an acceptable level.

GUIDELINE (paragraphs 18 – 19)

(18) In outsourcing activities, supervised entities shall take into account that by virtue of section 24 subsection 2 of the Act on the FIN-FSA, the FIN-FSA shall, confidentiality provisions notwithstanding, have the right to obtain necessary information for supervisory purposes at the place of business of a company that acts as the supervised entity's representative or a company that, by order of the supervised entity, performs tasks pertaining to the accounting, information system or risk management or other internal control of the supervised entity.

(19) The FIN-FSA recommends that the aforementioned clause granting the FIN-FSA access to information and right of inspection is included in outsourcing contracts.

4.2 Holding of assets classified as client assets

(20) A virtual currency provider shall deposit assets on an account in the central bank, a deposit bank or in a credit institution authorised in another State and entitled to receive deposits or in low-risk and liquid securities or other investment targets if the assets have not been transferred on the business day following the day of receipt of the assets.

(21) By virtue of section 11, subsection 2 of the Act on Virtual Currency Providers, the FIN-FSA shall issue regulations on when a security or other investment target may be deemed low-risk and liquid.

REGULATION (paragraphs 22 – 23)

(22) Assets may, with the express consent of the client, be invested in units of a money market fund registered in an EEA Member State that meets the preconditions of Directive 2009/65/EC (UCITS Directive) or Directive 2011/61/EU (AIFM Directive) or is otherwise subject to supervision and fulfils the requirements of Article 2 of Regulation (EU) No 1071/2013 of the European Central Bank concerning the balance sheet of the monetary financial institutions sector.

(23) If assets are invested in investment targets referred to in paragraph 22, the virtual currency provider shall especially consider the need to diversify the client assets and comply with due diligence (sufficient professional skill, care and prudence) in choosing the money-market fund that will keep the assets in custody and assess, on a regular basis, compliance with the requirements relating to the holding of client assets.

GUIDELINE (paragraph 24)

(24) The FIN-FSA recommends that if a virtual currency provider deposits assets on an account in the central bank, a deposit bank or in a credit institution authorised in another State and entitled to receive deposits, the virtual currency provider deposits assets received for purposes of virtual currency exchange from the users of the service related to virtual currency or other provider of services related to virtual currency in the following targets:

- a corporate account or a corresponding short-term account in the central bank, or
- a sight deposit account in a Finnish deposit bank, or
- a sight deposit account in a credit institution authorised in another State and entitled to receive deposits.

4.3 Holding and safeguarding of virtual currencies classified as client assets

(25) Due to the nature of virtual currencies, holding and safeguarding of virtual currencies classified as client assets usually means reliable holding and safeguarding of private encryption keys.

(26) All regulations and guidelines in this chapter also apply, as applicable, to other than information system-based mechanisms for the safeguarding and holding of virtual currencies classified as client assets.

(27) By virtue of section 11, subsection 4 of the Act on Virtual Currency Providers, the FIN-FSA may issue more detailed regulations on the holding and safeguarding of client assets.

REGULATION (paragraphs 28 – 35)

(28) The amount of virtual currencies classified as client assets stored in a system connected to a public communications network must not exceed an amount the loss of which the supervised entity, based on the risk assessment, is able to cover.

(29) All data, services, information systems and data communications relating to the handling of client assets received for purposes of virtual currency exchange shall be secured and the availability of the services ensured through administrative, technical and other measures. The supervised entity shall ensure a level of information security for its information systems that is adequate with respect to the nature and size of its operations, the severity of security threats and the general level of technical development.

(30) The supervised entity shall have the expertise, organisation and internal control required to record, transfer, process and file information relating to the processing of virtual currencies. If these functions are outsourced, the supervised entity shall ensure the provider of outsourced services complies with the principles laid down in this chapter.

(31) Access to information systems shall be monitored. Non-repudiation of events processed in information systems and identification and authentication of intercommunicating parties must be dealt with appropriately. The information systems must also provide a full audit trail of all events.

(32) The major risks involved in information systems and their risk management methods shall be documented, and necessary controls for managing the risks shall be built.

(33) Recovery plans shall be drawn up for information systems describing how each information system can be reactivated in the event of a disruption.

(34) Backup copies of information systems and possible standby computer facilities shall be located so far from the ordinary data processing centre that data and backup copies cannot be destroyed at the same time.

(35) Private encryption keys used to safeguard virtual currencies classified as client assets shall be stored in an adequately secure manner.

GUIDELINE (paragraphs 36 – 38)

(36) The FIN-FSA recommends that the amount of virtual currencies classified as client assets stored in a system connected to a public communications network should not exceed an amount the loss of which supervised entity, based on the risk assessment, is able to cover through its own funds, an insurance policy or other corresponding means.

(37) A system connected to a public communications network refers to, for example, ‘hot wallet’ storage.

(38) The FIN-FSA recommends that the supervised entity check at least the following items to ensure adequate information security before launching and offering a service:

- When building information systems, backup arrangements should be taken into account in order to prepare for disruptions and outages in activities and systems by setting up alternative modes of operation or systems. Backup arrangements typically involve the use of duplex components in data processing and data communications as well as backup copying.
- System-specific information security tests and reviews should be made and ongoing monitoring and reporting of security levels and possible disruptions of information systems should be put in place. A security review is a systematic examination of the security level of a system, service or activity to ensure that the targeted security level is achieved.
- Systems should be tested on a regular basis and particularly after system changes. Detected security shortcomings should be remedied immediately.
- Systems and their necessary data connections should be protected against, for example, denial-of-service attacks. Systems should be equipped with access control mechanisms, and the supervised entity should ensure that appropriate management of authorisations is in place.
- External networks should be separated from the supervised entity's internal network by means of security measures.

5 Customer due diligence and risk management systems

(39) According to section 13, subsection 1 of the Act on Virtual Currency Providers, a virtual currency provider is required to know its customers. A virtual currency provider shall identify the beneficial owner of a customer and the person acting on behalf of said customer as well as, where necessary, verify their identity.

(40) According to section 13, subsection 2 of the Act on Virtual Currency Providers, a virtual currency provider shall have in place adequate risk management systems by which it can assess the risks arising from customers to its operations.

(41) Customer due diligence is also covered by the AMLA.

(42) By virtue of section 13, subsection 4 of the Act on Virtual Currency Providers, the FIN-FSA may issue further provisions on the procedures to be complied with in customer due diligence referred to in subsection 1 and on risk management referred to in subsection 2.

(43) Virtual currency providers are obliged entities as referred to in the AMLA, and as such required to (list not exhaustive)

- prepare a risk assessment on money laundering and terrorist financing (AMLA chapter 2, section 3)
- know their customers (AMLA chapter 3)
- file reports on suspicious transactions or suspected financing of terrorism with the Financial Intelligence Unit (AMLA chapter 4, section 1), and
- organise training and protection of employees and draw up operating guidelines in order to ensure compliance with the provisions of said Act (AMLA chapter 9, section 1)

(44) Customers shall be identified and their identity verified when establishing a regular customer relationship. Non-regular (occasional) customers shall be identified and their identity verified when carrying out a single transaction which individually or as the sum of interrelated transactions amounts to at least EUR 10,000 (AMLA chapter 3, section 2, subsection 1).

(45) Customer due diligence is also covered by FIN-FSA Standard 2.4, *Customer due diligence – Prevention of money laundering, terrorist financing and market abuse*. The standard comprises various definitions, including who shall be considered as an obliged entity's regular customer and non-regular (occasional) customer.

GUIDELINE (paragraphs 46 – 51)

(46) The FIN-FSA recommends that virtual currency providers use an information system-based analysis program in order to perform customer due diligence and to monitor customer activities if, based on the risk assessment, the nature and scope of the business so requires. Virtual currency providers should also use the data obtained from the analysis program to assess the risks customers pose to their operations.

(47) The obligation to perform enhanced customer due diligence in non-face-to-face identification is prescribed in chapter 3, section 11 of the AMLA.

(48) The FIN-FSA recommends that as the reliable source for providing additional documents or information in order to verify the identity of a customer as prescribed in chapter 3, section 11 of the AMLA, virtual currency providers use, for example, official registers such as population information systems.

(49) The FIN-FSA recommends that supervised entities should have measures in place to check information a customer has given via non-face-to-face identification.

(50) The FIN-FSA recommends that if a provider of services related to virtual currency allows customers to transfer virtual currencies to or from the service with the assistance of features whose evident purpose is to obscure the origin of virtual currencies, this should be taken into account in the risk assessment on money laundering and financing of terrorism. An example of such a feature is a mixer. According to chapter 3, section 4, subsection 3 of the AMLA, the origin of funds relating to a transaction shall be traced where necessary.

(51) The FIN-FSA recommends that if a provider of services related to virtual currency as part of its service offers features like those mentioned above, whose evident purpose is to obscure the origin of virtual currencies, this should be taken into account in the risk assessment on money laundering and financing of terrorism.

6 Transitional provisions and entry into force

(52) Providers who have been practicing activities requiring registration under the Act on Virtual Currency Providers prior to the entry into force of the Act may continue their operations in Finland without registration until 1 November 2019. The regulation is applicable to such providers as from 1 November 2019.

(53) The AMLA is applicable to obliged entities as from 1 December 2019.