"Approved"
Central Bank of
the Republic of Azerbaijan
Decision № 11/1
24 February 2023

Regulation on transactions with virtual assets in the Republic of Azerbaijan

1. General provisions

1.1. This Regulation has been developed in accordance with the Laws of the Republic of Azerbaijan on Prevention of the Legalization of Criminally Obtained Property and the Financing of Terrorism and on Targeted Financial Sanctions, and determine requirements on the cases of taking measures on transactions with virtual assets and transmission of information in the operation chain.

1.2. Provision of services on of transactions with virtual assets in the Republic of Azerbaijan is provided by virtual asset service providers authorized by law.

1.3. Transactions where virtual asset service providers act as owners of their virtual assets and beneficiary are not subject to the requirements of Item 3.3 herein.

1.4. Irrespective other provisions of this Regulation, when virtual asset service providers identify that virtual asset owners and beneficiary are in the list of persons to be imposed financial sanctions during transactions with virtual assets, they should take measures in accordance with the Laws specified in Item 1.1 herein along with the measures specified in this Regulation.

2. Main definitions

2.1. Definitions used for the purposes of this Regulation bear the following meanings:

2.1.1. **virtual asset owner (VAO)** – a person who orders transactions with virtual assets;

2.1.2. **beneficiary** – a person in whose favor transactions with virtual assets are conducted;

2.1.3. **virtual asset (VA)** – a digital representation of the value available in the VAs circulation system that acts as a medium of exchange for payments or investments. The digital equivalent of national and foreign currencies, securities, as well as derivative financial instruments are not considered a virtual asset;

2.1.4. **virtual asset service provider (VASP)** – persons who organize exchange of VAs with currency resources, the national currency and other VAs; transfer or organization of transfer of the VA from the VA account or wallet used for its storage to another VA account or wallet; organize conduction of transactions (concluding transactions) with VAs or tools that allow controlling VAs or their storage; supply of financial services or involvement in supply of services on buy/sell/exchange/ initial placement or maintenance of VAs as an independent entrepreneurial activity;

2.1.5. **the issuer virtual asset service provider** – a person who accepts the order and sends the VA during transactions with VAs;

2.1.6. **beneficiary virtual asset service provider** – the person who accepts the VA and makes it available for the beneficiary;

2.1.7. **virtual asset account** – an account opened with the VASP for transactions with VAs;

2.1.8. **virtual asset wallet** – software or hardware under VAO's control for transactions with VAs;

2.1.9. **unhosted VA wallet** – a VA wallet not maintained, stored or managed by any VASP;

2.1.10. **VA wallet address** – a combination of letters and numbers to identify a VA wallet;

2.1.11. **unique reference number of the transaction** – a combination of letters, numbers and symbols unique for each transaction that makes it possible to trace the operation from the beginning to the end in the transaction chain carried out with VAs;

2.1.12. **information transmission technology** – a technology that enables the transfer of information about virtual assets and virtual asset owner and beneficiary between virtual asset service providers during transactions with virtual assets.

3. Responsibilities of the issuer virtual asset service provider

3.1. The issuer VASP should apply customer due diligence prior to the transactions with VAs in accordance with the requirements of the Law of the Republic of Azerbaijan on Prevention of the Legalization of Criminally Obtained Property and the Financing of Terrorism (hereinafter – the AML/CFT Law).

3.2. The issuer VASP provides availability of the following information during transactions with VAs:

3.2.1. The name of the VAO (1st, middle and last names of the individual; the name, organizational-legal form and TIN of the legal entity);

3.2.2. Personal identification information of the VAO (the date and place of birth, PIN, address or ID card number);

3.2.3. VAO's VA account number or VA wallet address;

3.2.4. a unique reference number of the operation;

3.2.5. the beneficiary's name (f1st, middle and last names of the individual; the name, organizational-legal form and TIN of the legal entity);

3.2.6. beneficiary's VA account number or VA wallet address.

3.3. Prior to the operation with the VA the issuer VASP should verify the information on the VAO specified in Items 3.2.1 and 3.2.2 herein and provide other due diligence measures specified in the legislation in accordance with Article 4.17 of the AML/CFT Law.

3.4. The issuer VASP should transmit the information specified in Item 3.2 herein during transactions with VAs to the beneficiary VASP in the operation chain with VAs.

3.5. The requirements of Item 3.2 herein apply to the cases where the VAO and the beneficiary are the same person.

3.6. Prior to transactions with VAs the issuer VASP should find out whether transaction is conducted to another VASP or to the unhosted VA wallet.

3.7. The issuer VASP should determine the risk rate of the operation with the unhosted VA wallet and effective monitoring measures in line with those risks.

3.8. The issuer VASP should strive to minimize risks by imposing additional restrictions or prohibitions in line with the identified risk rate with respect to the operation with the unhosted VA wallet.

4. Responsibilities of the beneficiary virtual asset service provider

4.1. Prior to the operation with the VA the beneficiary VASP should apply due diligence measures in accordance with the requirements of the AML/CFT Law and verify integrity of the information specified in Item 3.2 herein.

4.2. The beneficiary VASP should verify the information specified in sub-item 3.2.5 herein during the operation with the VA in accordance with Article 4.17 of the AML/CFT Law and provide other customer due diligence measures specified in the legislation, as well as verify the accuracy of information specified in sub-item 3.2.6 herein.

4.3. In case the beneficiary VASP finds out that the information obtained from the VASP in the operation chain is incomplete, it should apply a risk-based approach by documenting the decision to be taken and its reasons and depending on the frequency of such cases or the level of business relations with the VASP it is in business relation with it should:

4.3.1. request the issuer VASP to provide integrity of information on the VAS and the beneficiary w/o executing the operation;

4.3.2. refuse to conduct the operation.

4.4. The beneficiary VASP should revise its business relations with the issuer VASP it is in business relations with in the cases specified in Item 4.3 herein and either suspend or terminate business relations in accordance with the risk appetite level.

5. Information transmission technology

5.1. When the information specified in Item 3.2 herein is transmitted from one VASP to another one during transactions with VAs, channels and information transmission technologies that do not meet requirements of the legislation and this Regulation, and impede execution of obligations by VASPs should be avoided. Prior to the execution of the operation with VAs the VASP should ensure availability of secure network channels.

5.2. Information transmission technologies used by the VASP should provide:

5.2.1. identification of the beneficiary VASP by the issuer VASP during the operation with VAs;

5.2.2. transmission of the information specified in Item 3.2 herein by the issuer VASP to the beneficiary VASP in no time fully and completely during the operation with VAs;

5.2.3. efficient and consistent execution of large-volume transactions by the issuer VASP to multiple destinations;

5.2.4. that the issuer VASP uses and transmits the information in accordance with the requirements of a secure and legally protected privacy regime, as well as maintains its integrity and availability to facilitate registration;

5.2.5. creation of connection channels between the VASP and other VASPs to:

5.2.5.1. verify the information specified in sub-items 6.1.1-6/1/2 herein on another VASP with whom a business relation is built;

5.2.5.2. request information from another VASP to find out whether any operation is related to any high-risk or prohibited activity.

6. Establishing business relations between virtual asset service providers

6.1. When establishing business relations with other VASPs the VASP should:

6.1.1. obtain necessary information to understand the nature of activities of the VASP with whom business relations are built;

6.1.2. obtain information on the reputation, the quality of its supervision, whether was involved in investigation of crimes on legalization of criminally obtained property and the financing of terrorism of the VASP with whom business relations are built from open sources;

6.1.3. assess internal AML/CFT system of the VASP with whom business relation is built;

6.1.4. get consent of the management on building a new business relation.

6.2. The VASP should take into account high risk of business relations with VASPs operating in foreign countries (territories) where the legal regulation of transactions with VAs is either weak or non-existent and apply enhanced due diligence measures.

6.3. Additional risk management measures (set limits on and monitor transactions, and intensify compliance measures) may be imposed when building business relations with VASPs located in the countries (territories) where the system of prevention of the legalization of criminally obtained property, the financing of terrorism and proliferation and the financing of proliferation of weapons of mass destruction is weak in relation to transactions with VAs.

6.4. The VASP should regularly assess the internal control system on AML/CFT of the counter party while business relations continue and find out whether this system is covered with an independent audit review. In the event the VASP finds out that the counterparty fails to meet these requirements, it should terminate business relations.

7. Final provisions

7.1. If provided for in their internal rules and procedures the VASPs may determine additional requirements on transactions with VAs.

7.2. During transactions with VAs the VASP should comply with the requirements arising from the Laws of the Republic of Azerbaijan on Prevention of the Legalization of Criminally Obtained Property and the Financing of Terrorism and on the Targeted Financial Sanctions and have internal rules and procedures, preventive measures, including electronic monitoring systems in place on the regulation of such transactions, and business relations with foreign financial institutions and VASPs.