

## DISCLOSURE REQUIREMENTS FOR VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS

*Liudmila Lapițkaia*<sup>1</sup>  
*Alexandru Leahovcenco*<sup>2</sup>

**Abstract:** *The development of the digital economy has led to the emergence of such concepts as virtual assets, virtual asset service providers. Transactions with virtual assets are the most vulnerable from the point of view of information transparency. Therefore, the presentation and disclosure of such transactions is most important in terms of transparency and anti-money laundering.*

**Key words:** *virtual assets, virtual asset service providers.*

**JEL:** *M41, K24*

### INTRODUCTION

The concept of virtual assets has relatively recently entered our lives. However, experts in this field give different definitions of virtual assets. For example: a specialist in the field of commercial and tax law Andrew P. Grau in his article "What are virtual assets?," in the journal Estate planning alert gives the following definition: „*Virtual assets are electronic data stored on a computer or the internet. These assets include emails, digital photos, electronic bank statements, domain names, and online accounts. There is emotional, and sometimes financial, value in virtual assets. Online accounts are used to communicate, pay bills, access financial assets and conduct business. Often, when the account holder passes away, nobody has access to passwords, or worse, nobody knows the account exists. As a result, online accounts and other virtual assets are left untouched,*„[1].

The Financial Action Task Force on Money Laundering (FATF) gives the following definition that "virtual asset" refers to digital representations of value that can be digitally traded or transferred and can be used for payment or investment purposes, including digital representations of value that function as a medium of exchange, a unit of account, and/or a store of value. The FATF emphasises that virtual assets are distinct from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the money of a country that is designated as its legal tender[2].

Therefore, the virtual assets are, first of all cryptocurrency or virtual currency, which in short time has developed into a powerful payment method with ever growing global acceptance.

The lawful use of virtual currencies offers many benefits such as increased payment efficiency and lower transaction costs.

Along with that, other characteristics of virtual currencies, coupled with their global reach, present potential risks, such as:

- the anonymity provided in internet trade with virtual currencies,
- the limited in verification of participants in internet trade with virtual currencies,
- the lack of clarity regarding the responsibility for supervision and enforcement for these transactions that are segmented across several countries

<sup>1</sup> ASEM str.Banulescu-Bodoni 61,MD-2005, Chișinău, R. Moldova, tel.022 402757, liudmila@ase.md

<sup>2</sup> ASEM str.Banulescu-Bodoni 61,MD-2005, Chișinău, R. Moldova, tel.022 22-41-28

- the lack of a central oversight body.

In addition, FATF determines that virtual asset service provider means any natural or legal person who conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- ✓ exchange between virtual assets and fiat currencies;
- ✓ exchange between one or more forms of virtual assets;
- ✓ transfer of virtual assets;
- ✓ safekeeping and/or administration of virtual assets or instruments enabling
- ✓ control over virtual assets; and
- ✓ participation in and provision of financial services related to an issuer's offer
- ✓ and/or sale of a virtual asset [3],.

#### **MATERIAL AND METHOD**

Various studies show that money laundering offences involving virtual currencies to demonstrate how this payment method has already been abused for money laundering purposes.

In this context in June 2019, the Financial Action Task Force adopted an Interpretive Note to Recommendation 15 to apply the requirements in relation to virtual assets (VA) and virtual asset service providers (VASP), in particular with regard to the application of the risk-based approach to VA activities or operations and VASPs.

The Interpretive Note to Recommendation 15 establishes a number of requirements for VASPs and other obliged entities that engage in operations with virtual assets to observe the following principles

- Functional equivalence and objectives-based approach. First of all, this is connected with the formation and application of the regulatory framework, which in different jurisdictions should be based on the same principles and approaches,
- Technology-neutrality and future-proofing,
- Level-playing field. This principle is based on the fact that all jurisdictions should apply equal disclosure requirements for virtual assets or similar assets.

To mitigate the risks associated with covered virtual assets activities, virtual asset service provider for identifying, assessing, and determining the risks must consider the following elements:

- *transactions with virtual currency have higher risks than with fiat currency and the traditional financial system and with virtual-to-virtual transactions;*
- *type of VASP business models (centralised and decentralised);*
- *the specific types of virtual assets;*
- *the specific business model of the virtual asset service provider;*
- *possibility for virtual asset service provider to operate entirely online (platform-based exchanges) or in person (trading platforms that facilitate peer-to-peer exchanges or kiosk-based exchanges);*
- *using the Internet Protocol, such as anonymizers (The Onion Router) or invisible Internet Project (I2P), which may further obfuscate which inhibit a virtual asset service provider's ability to know its customers;*
- *the risks associated with a virtual asset service provider's connections to several jurisdictions;*
- *the scope of the virtual account, product, or service;*
- *the scope of the virtual assets payment channel (open- versus closed-loop systems or systems intended to facilitate micro-payments or government-to-person, etc.);*

- any measures that may potentially lower the provider's exposure to risk (limitations on transactions or account balance, etc.).

FATF sets the following items and disclosures to be disclosed for transactions with virtual assets.

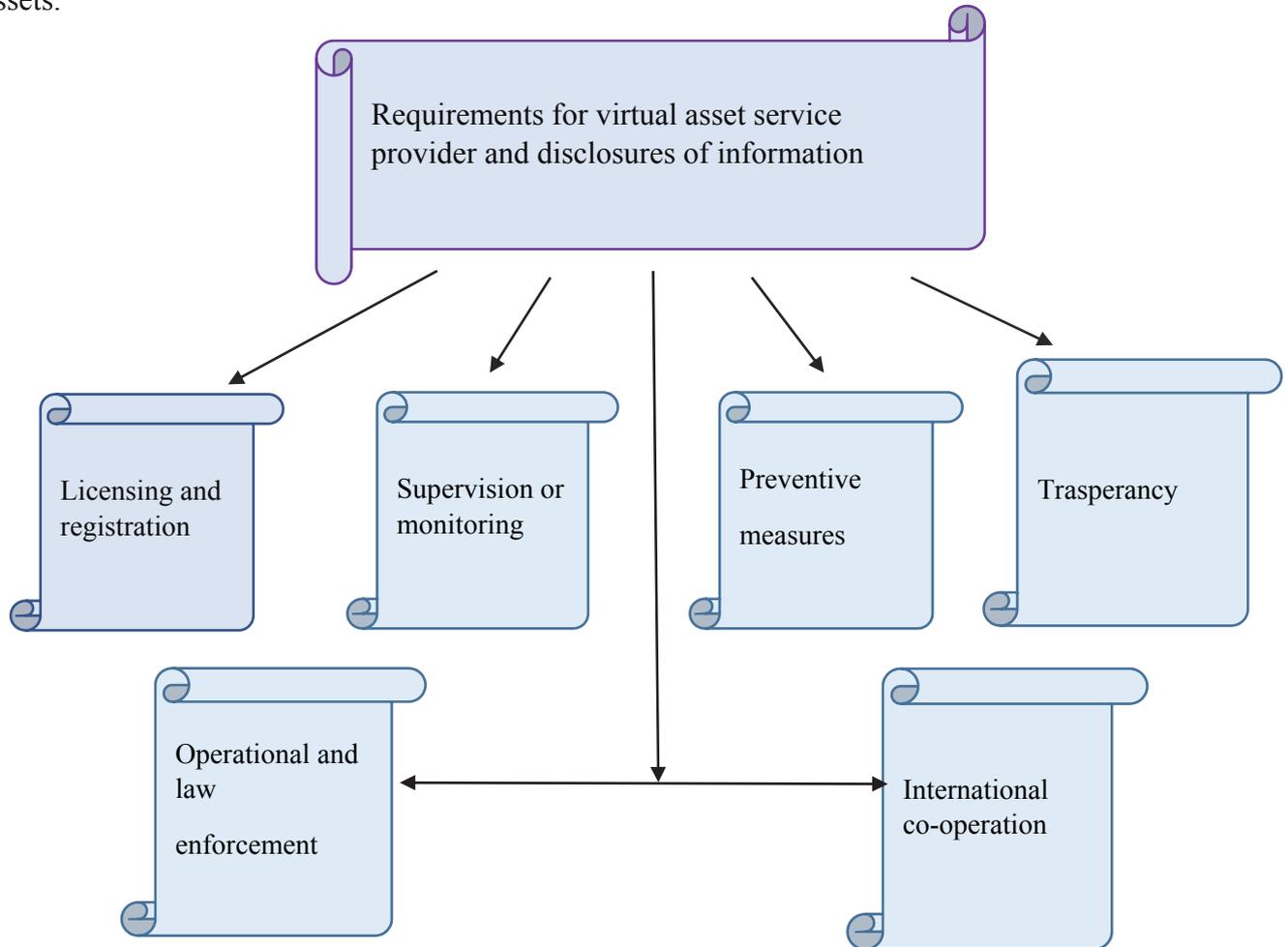


Fig. 1 Requirements for virtual asset service provider and disclosures of information

Source: developed by the authors according to Interpretive Note to Recommendation 15 elaborated by FATF

Licensing of providers who provide services for transactions with virtual assets should be carried out by the state authorities, which must identify persons operating without a license, using such tools as: web-scraping and open-source information to identify online advertising or possible solicitations for business by an unregistered or unlicensed entity; information from industry circles (including by establishing channels for receiving public feedback) regarding the presence of certain businesses that may be unlicensed or unregistered.

Supervision or monitoring is an important point since these operations do not fall within a single jurisdiction, they have the cross-border nature of VASPs' activities so that international cooperation between relevant supervisors is also of specific importance.

Preventive measures oblige that virtual asset service providers should design CDD processes to meet the FATF Standards and national legal requirements. Initial CDD comprises identifying the customer and, where applicable, the customer's beneficial owner and verifying the customer's identity on a risk basis and on the basis of reliable and independent information, data, or

documentation to at least the extent required by the applicable legal or regulatory framework. The CDD process also includes understanding the purpose and intended nature of the business relationship, where relevant, and obtaining further information in higher risk situations.

Transparency and beneficial ownership of legal persons and arrangements means that as any natural or legal person that conducts as a business the activities or operations specified in the VASP definition should take measures to prevent the misuse of legal persons and arrangements for money laundering and terrorist financing.

Operational and law Enforcement means that competent authorities should be able to obtain access to all necessary documents and information, including powers to use compulsory measures for the production of records, held by VASPs. They should have effective mechanisms in place to identify whether natural or legal persons such as VASPs hold or control virtual assets accounts or wallets and mechanisms for ensuring that competent authorities have a process to identify assets, including VAs, without prior notification to the owner.

Transactions with virtual assets accounts must be effectively regulated, supervised, and enforced relating to the VASP sector requires a global approach and a level regulatory framework across jurisdictions. Authorities from different countries should have in place the tools necessary to cooperate with one another, provide mutual legal assistance; help identify, freeze, seize, and confiscate the proceeds and instrumentalities of crime that may take the form of VAs as well as other traditional assets associated with VASP activities and provide effective extradition assistance in the context of virtual assets-related crimes or illicit actors who engage in illicit activities among other international capabilities.

## **RESULTS AND DISCUSSIONS**

Virtual asset service providers and other entities in virtual assets transfers should consider how they might impact existing commercially available technology to comply with the established requirements. Examples of existing technologies that providers could consider as a basis for enabling the identification of beneficiaries of virtual assets transfers:

- private and public keys, which are formed in pairs for each subject involved in a transmission and encrypt and decrypt information during the initial part of the transmission so that only the sender and recipient can decrypt and grasp the information, wherein the public key is available to everyone while the private key is known only to the creator of the keys;
- transport layer security/secure sockets layer (TLS/SSL) connections, which make utilize of public and private keys among parties when establishing a connection and secure almost all on the transference Internet, including emails, logins, and financial operations, ensuring that all data that passes between a web server and a browser keeps private and secure;
- digital certificates administered by certificate authorities that use such standard to verify that a public key belongs to the user, computer, or service identity in the certificate and which are used worldwide across public and private sectors;
- specific attribute certificates, which can encode attributes (such as name, date of birth, address, and unique identifier number) and are administered by attribute certificate authorities;
- API technology, which provides tools for creating software applications and specifies how software components should interact.

Studying the experience of disclosing information providers in different countries, you can consider the example of Norway and the United States. In accordance with Norwegian act to Virtual Currency custodianship services is meant the services of private cryptographic keys on behalf of customers, for purposes of transferring, storing or trading in virtual currency. But virtual currency

means a digital expression of value, which is not issued by a central bank or a government authority, which is not necessarily attached to a legally established currency and does not possess a legal status of currency or money but which is accepted as a means of exchange, and which can be transferred, stored or traded electronically.

Virtual asset service provider required to presents the required information to Financial Supervisory Authority which may supervise compliance with the Anti-Money Laundering Act.

U.S. law enforcement uses financial intelligence information from Financial Crimes Enforcement Network FinCEN to conduct investigations involving digital assets.

## CONCLUSIONS

Financial Action Task Force in it's adopted Interpretive Note stated that if virtual companies are engaged in the transfer of funds, they must be required to obtain and store the necessary and accurate information on the sender, as well as the necessary information on the recipient of these funds, and that this information must be provided to the second organization ("provider"), if any. Moreover, these second recipient organizations may also be required by FATF countries to obtain and maintain the necessary (and for some reason not necessarily accurate) information about the source of the transferred funds, as well as the necessary and accurate information about the recipient.

Necessary or required information in the case of each translation means:

- *Name of the sender (the person who is the client of the provider),*
- *The account number of this person, if it is from this account that the transfer is carried out – that is, a virtual wallet,*
- *Physical address of the sender, or national identification number, or customer identification number (but not the transaction),*
- *The name of the recipient,*
- *Beneficiary's account number, if it is transferred to it – i.e. virtual wallet.*

Given the high risks of illegal use of virtual assets, including for the financing of terrorist activities, FATF in a public statement this month gave its members 12 months to implement the recommendations in practice.

Experts in the field of blockchain note, however, that it will be difficult (if not impossible) to implement FATF instructions in practice, that it will damage the privacy of customers.

## REFERENCES

1. Andrew P. Grau. What Are Virtual Assets? [http://www.hrmml.com/library/files/client\\_alert\\_virtual\\_assets.pdf](http://www.hrmml.com/library/files/client_alert_virtual_assets.pdf)
2. FATF <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html>
3. Guidance for a risk-based approach to virtual assets and virtual asset service providers <https://static.coindesk.com/wp-content/uploads/2019/06/Embargo-Virtual-Asset-Guidance.pdf>