



Finanšu izlūkošanas dienests

VIRTUAL CURRENCIES: MONEY LAUNDERING AND TERRORISM AND PROLIFERATION FINANCING RISK ASSESSMENT

Riga 2021



CONTENT

| | | |
|-------------|--|-----------|
| I. | ABBREVIATIONS AND TERMS | 2 |
| I. | INTRODUCTION | 3 |
| II. | SUMMARY | 3 |
| III. | REGULATORY FRAMEWORK | 6 |
| 1. | REGULATORY FRAMEWORK OF LATVIA | 6 |
| 2. | EU REGULATORY FRAMEWORK..... | 7 |
| 3. | FATF STANDARDS | 8 |
| 4. | CONCLUSIONS | 9 |
| IV. | GLOBAL TENDENCIES IN VIRTUAL CURRENCY SECTOR | 9 |
| 1. | INTRODUCTION OF FATF STANDARDS | 9 |
| 2. | INTERNATIONALLY IDENTIFIED VIRTUAL CURRENCY ML AND TF RISKS | 11 |
| V. | SITUATION IN LATVIA | 12 |
| 1. | IDENTIFICATION OF LOCAL AND FOREIGN VIRTUAL CURRENCY SERVICE PROVIDERS | 12 |
| 2. | REPORTING OF SUSPICIOUS TRANSACTIONS AND FINANCIAL INTELLIGENCE | 14 |
| 3. | INVESTIGATION | 15 |
| 4. | CASE LAW | 19 |
| VI. | TF AND PF RISKS OF VIRTUAL CURRENCIES | 21 |
| | ANNEX NO 1_VIRTUAL CURRENCY “RED FLAGS” OF ML/TF | 23 |
| 1. | RISK INDICATORS RELATED TO TRANSACTIONS AND TRANSACTION PATTERNS | 23 |
| 2. | RISK INDICATORS RELATED TO ANONYMITY | 24 |
| 3. | RISK INDICATORS RELATED TO SENDERS AND RECIPIENTS | 24 |
| 4. | RISK INDICATORS RELATED TO THE SOURCE AND GEOGRAPHY OF FUNDS OR WEALTH | 25 |

ABBREVIATIONS AND TERMS

| | |
|------------------------|---|
| UN | United Nations |
| EU | European Union |
| FATF | Financial Action Task Force |
| Fiat currency | National coins and banknotes identified as legal means of payment and electronic money accepted as means of exchange in the country of issue |
| FIU | Financial Intelligence Unit |
| FCMC | Financial and Capital Market Commission |
| MoF | Ministry of Finance |
| RoL | Republic of Latvia |
| Cabinet | Cabinet of Ministers |
| ML | Money laundering |
| AML/CFT Law | Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing |
| NRA | National ML/TF/PF Risk Assessment Report for 2017 –2019 |
| Action Plan | The Cabinet Order No 576 of 29 September 2020 “Regarding Action Plan for Prevention of Money Laundering and Terrorism and Proliferation Financing for 2020–2022”. |
| PF | Proliferation financing |
| Risk Assessment | Virtual Currencies: Money Laundering and Terrorism and Proliferation Financing Risk Assessment |
| TF | Terrorism financing |
| SRS | State Revenue Service |
| SRS TCPD | Tax and Customs Police Department of the State Revenue Service |
| SP | State Police |
| SP ECED | Economic Crime Enforcement Department of the Central Criminal Police Department of the State Police |

I. INTRODUCTION

1. New technologies, products, and related services have the potential to spur financial innovation and efficiency and improve financial inclusion, but they also create new opportunities for criminals and terrorists to launder their proceeds or finance their illicit activities.¹
2. A particularly important process is detecting and identifying the risks associated with the use of new technologies, which is also enshrined in the FATF standard² as well as in national policy planning documents.³ In recent years, a specific new technology — virtual currency — has gained special relevance. The issue of the use of virtual currencies continues to be relevant both at the international and national level.
3. The risk identification and assessment is carried out in order to promote the understanding of responsible public authorities, obliged entities under the AML/CFT Law and other stakeholders about the ML, TF and PF risks related to virtual currencies and virtual currency service providers. By identifying and assessing these risks, persons involved in the prevention of ML, TF and PF can adequately manage the relevant risks through a risk-based approach. Restricting the use of virtual currency is not the purpose of this Risk Assessment.
4. The Risk Assessment is developed by the FIU in cooperation with experts from the MoF, the SRS, the SP ECED and the FCMC.

II. SUMMARY

5. Virtual currencies and virtual currency service providers can be used at all ML stages: placement, layering, and integration.⁴ In addition, virtual currencies and virtual currency service providers can be used to launder the proceeds of any crime, including those identified in the NRA as posing the most significant national ML threat : tax evasion and corruption, illegal circulation of excise goods and drugs, including smuggling, as well as criminal offences against property, in particular fraud committed on a large scale.⁵
6. At the international level, however, virtual currencies are mainly used to commit the following criminal offences: drug trafficking, sale of firearms, fraud, tax evasion, violation of sanctions, computer crimes (e.g. cyberattacks involving theft or encrypted ransomware), child exploitation, human trafficking and TF.
7. Internationally, there is a tendency for the most detected ML and TF cases related to virtual currencies to take place in the virtual currency environment from the outset, but less frequently the use of virtual currencies in ML is detected when proceeds of crime are obtained in the fiat currency. In this respect, Latvia's practice is significantly different, as the vast

¹ Updated guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. October 2021. Available at: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>.

² FATF Recommendation 15 “New Technologies” provides for that countries and financial institutions should identify and assess the ML and TF risks that may arise in relation to (1) the development of new products and new business practices, including new delivery mechanisms, and (2) the use of new or developing technologies for both new and pre-existing products.

³ Outcome indicator 2 of action 1.2 in the Action Plan envisages the development of an assessment of new technologies (including emerging threats) and the related ML, TF and PF risks once a year.

⁴ ML as a set of specific activities is a single process that can be divided into three basic stages: (1) placement, (2) layering, and (3) integration. In the layering stage or structuring stage, the proceeds of crime, by simulating various transactions, are: a) moved and structured with the aim of distancing them from the source of the funds; and (b) gives the impression that a civil transaction is taking place. See more in the methodological material “Money Laundering Typologies and Features”. Available at: https://www.fid.gov.lv/uploads/files/2021/FID_Tipologiju%20materials_II_red.pdf.

⁵ National ML/TF/PF Risk Assessment Report for 2017 –2019 (summary), p. 9 Available at: https://www.fid.gov.lv/uploads/files/Dokumenti/Riska%20zi%C5%86ojumi/Nacion%C4%81%C4%81%20NIL_LTPF%20risku%20nov%C4%93rt%C4%93juma%20zi%C5%86ojuma%20kopsavilkums.pdf.

majority of suspicious transaction reports received by the FIU suspect ML using virtual currencies, where the proceeds are obtained, for example, as a result of fraud with fiat currency.

8. This difference between Latvia and international practice can be explained precisely by the fact that the FIU does not receive suspicious transaction reports from virtual currency service providers that could directly report criminal offences occurring exclusively in the virtual currency environment (this is explained, among other things, by a small number of market operators). These observations indicate that Latvia has a high level of latency (unregistered criminal offences) for criminal offences that occur only in the virtual currency environment (including those criminal offences that pose the highest ML threat in Latvia according to the NRA).
9. From the point of view of virtual currency service providers, in Latvia the highest ML/TF/PF risks are caused by:
 - 9.1. Latvian residents — unregistered virtual currency service providers — who deliberately do not comply with the requirements for the prevention of ML/TF/PF;
 - 9.2. Virtual currency service providers with weak or non-existent ML/TF/PF prevention requirements registered in countries with weak or non-existent ML/TF/PF prevention requirements for virtual currency service providers.
10. It can be concluded that in Latvia, as well as internationally, in the context of virtual currency ML and TF risks, the main tendencies are (1) virtual currency service providers with weak or non-existent ML/TF/PF prevention requirements, as well as (2) methods and tools that enhance anonymity. If a customer of the obliged entity under the AML/CFT Law uses virtual currencies with methods and tools that enhance anonymity without logical explanation, it may serve as a ML/TF/PF risk indicator. The same applies to the use of virtual currency service providers with weak or non-existent ML/TF/PF prevention requirements (for a more detailed list of ML/TF/PF risk indicators, see Annex 1).
11. The partial non-compliance with the FATF standards identified in the Latvian regulatory framework in the previous years has been prevented and, compared to other countries of the world, the vulnerabilities of virtual currency service providers registered in Latvia are significantly lower, as the requirements of international standards are implemented in Latvia and the SRS supervises virtual currency service providers.
12. Local virtual currency service providers consider the lack of licensing to be a disadvantage, which makes it difficult for companies to conduct business and compete with foreign virtual currency service providers. Also, foreign virtual currency service providers can often be subject to much simpler ML/TF/PF prevention requirements.
13. The number of registered virtual currency service providers that provide virtual currency services in Latvia does not exceed 5 obliged entities. Compared to the regional level of the Baltic States only, the number of virtual currency service providers registered in Latvia is very low. The SRS has identified all registered virtual currency service providers and has performed inspections of all virtual currency service providers in compliance with the ML/TF/PF prevention requirements, also applying sanctions to some virtual currency service providers.
14. The policy of restricting the activities of virtual currency service providers may result in the development of unregistered virtual currency service providers, whose ML/TF/PF risks will be higher, as such merchants will try to evade the ML/TF/PF requirements. In the criminal proceedings initiated by the SP, such unregistered virtual currency service providers (or “virtual currency bankers”) have already been identified. Substantially, their business model tends to include ML, for example, by handing over virtual currency to criminals in exchange for the proceeds of crime in cash, for a “commission”. Such persons do not register with the SRS as virtual currency service providers and do not fulfil the ML/TF/PF prevention requirements, thus significantly increasing the ML/TF/PF risks.
15. In 2019 and 2020, the FIU did not receive any suspicious transactions reports from virtual currency service providers registered in Latvia or abroad, which is considered to be critically low indicator. In the context of the growing number of suspicious transaction reports

submitted by virtual currency service providers worldwide, the tendency observed in Latvia is alarming, as so far, the FIU has received suspicious transaction reports related to virtual currencies only from other obliged entity under the AML/CFT Law (mainly "traditional" financial institutions). The low number of reports is partly explained by the fact that the Latvian market of virtual currency service providers is limited and by the fact that virtual currency service providers registered abroad do not report suspicious transactions to the FIU (including transactions involving Latvian residents).

16. The ML/TF/PF risks of virtual currency service providers registered in Latvia are relatively low, as the economic performance of registered virtual currency service providers is low, they have internal control systems for the ML/TF/PF prevention, they are subject to constant SRS supervision from the ML/TF/PF prevention point of view and they provide services only in person and to natural persons. In other words, the vulnerability of virtual currency service providers registered in Latvia to servicing high ML/TF/PF risk virtual currency flows is low.
17. Taking into account the mentioned considerations, the following possibilities for improvement of regulatory enactments have been identified:
 - 17.1. To align the requirements of the AML/CFT Law on customer due diligence in virtual currency transactions with the FATF recommendations, for example by stipulating that simplified customer due diligence is required for virtual currency transactions below the "threshold" set by the FATF.
 - 17.2. To require obtaining of a license as a precondition for the provision of virtual currency services in Latvia, setting clear requirements and a verification process for granting the relevant license to persons, and setting a transition period for obtaining a license for those virtual currency service providers who already perform such economic activity.
 - 17.3. To determine the requirements for the activity of foreign-registered virtual currency service providers in Latvia (at least with regard to compliance with the regulatory enactments in force in Latvia in the field of ML/TF/PF prevention), as well as the right of competent authorities to restrict the activity of the foreign-registered virtual currency service providers in Latvia, which do not meet the specified requirements.
 - 17.4. To determine the threshold for virtual currency transactions, above which the obliged entity under the AML/CFT Law must submit a threshold declaration to the FIU.
 - 17.5. To establish a specific NACE code for virtual currency service providers to facilitate the identification and monitoring of obliged entities.
 - 17.6. In the opinion of the MoF, in addition to the mechanism that allows the identification of bank account and safe deposit box holders, it would be necessary to establish a mechanism for the identification of crypto-asset wallet holders and ensure the international exchange of this information.
18. At the international level, the supervisory institution for virtual currency service providers is mainly the financial market supervisor. The decision of the Latvian legislator to designate the SRS as the supervisory and control institution for virtual currency service providers is not incorrect, despite the fact that the SRS mainly monitors the obliged entities under the AML/CFT Law in the non-financial sector in fulfilling the ML/TF/PF prevention requirements. However, if the provision of virtual currency services in the future will be subject to requirements similar to those of traditional financial services (not only in the context of the ML/TF/PF prevention), it would be useful to consider changing the supervisory and control institution for virtual currency service providers establishing the FCMC as a supervisory and control institution for virtual currency service providers.
19. The development of new uncontrolled innovative methods in the digital environment with virtual currency transactions poses a new risk to the use of the financial system, including the transit of funds, which should be assessed by strengthening the analytical functions of the SRS (as supervisory and control institution), FIU, SP, SRS TCPD and other institutions involved, and the ability to identify crimes related to new technology, including the use of virtual currency in transactions. It is necessary to expand the amount of information available

to the responsible institutions by strengthening the skills of the institutions and the monitoring, control and analytical tools at their disposal.

20. Recent experience shows that the proceeds from crime committed abroad can be laundered using the accounts of virtual currency service providers registered in Latvia, which do not have a physical presence in Latvia and which are not registered with the SRS as virtual currency service providers.⁶ This highlights the need to enhance the analytical function, ability of the responsible institutions to identify ML cases, and the ability to monitor virtual currency transactions.

III. REGULATORY FRAMEWORK

1. Regulatory Framework of Latvia

21. The legal provisions of the AML/CFT Law applicable to virtual currencies entered into force on 09.11.2017.⁷ The annotation of the respective draft law states that one of the latest technologies that requires careful monitoring, but not restrictive regulation in order not to stifle the innovative development of the idea, is virtual currency technology.
22. As regards the virtual currencies, the AML/CFT Law provides for the following definitions:
 - 22.1. **Virtual currency** — a digital representation of the value which can be transferred, stored or traded digitally and operate as a means of exchange, but has not been recognised as a legal means of payment, cannot be recognised as a banknote and coin, non-cash money and electronic money, and is not a monetary value accrued in the payment instrument which is used in the cases referred to in Section 3, Clauses 10 and 11 of the Law on the Payment Services and Electronic Money;
 - 22.2. **Virtual currency service provider** — the person providing virtual currency services, including the provider of services of exchange of the virtual currency issued by other persons, which provides the users with the possibility to exchange the virtual currency for another virtual currency by receiving commission for it, or offer to purchase and redeem the virtual currency through a recognised legal means of payment;⁸
23. Virtual currency service providers are the obliged entities under the AML/CFT Law.⁹ In view of the above, virtual currency service providers are obliged to perform customer due diligence (including identification of the customer, identification of the ultimate beneficial owner),¹⁰ to perform the supervision of customer transactions, staff training in the area of ML/TF/PF prevention and other activities specified in the AML/CFT Law .
24. All obliged entities of the AML/CFT Law (also financial institutions, real estate agents, etc.) have an obligation to perform the customer due diligence, if the virtual currency is used in the transaction.¹¹ Thus, when conducting transactions of any size (including occasional transactions) with virtual currencies, the subject of the AML/CFT Law shall perform the customer due diligence.
25. The AML/CFT Law provides for that its obliged entities are all virtual currency service providers, however, the State Revenue Service performed the obligations under the AML/CFT Law with respect to the virtual currency exchange service providers until the amendments to

⁶ SIA Chatextech, a virtual currency service provider registered in Latvia, may be involved in laundering millions of dollars. Available at: <https://www.lsm.lv/raksts/zinas/latvija/latvija-registreta-firma-iesaistita-miljonu-dolaru-atmazgasana.a429680/>.

⁷ Amendments to the Law on the Prevention of Money Laundering and Terrorism Financing. Published: Latvijas Vēstnesis, 222, 08.11.2017. Available at: <https://likumi.lv/ta/id/294868-grozijumi-noziedzigi-iegutu-lidzeklu-legalizacijas-un-terorisma-finansanas-noversanas-likuma>.

⁸ AML/CFT Law, Section 1, Paragraph 1, Clause 2.2 and 2.3. Available: <https://likumi.lv/doc.php?id=178987>

⁹ Ibid, Section 3, Paragraph one, Clause 11.

¹⁰ In the area of ML prevention, in English these activities frequently have the abbreviations CDD (Customer Due Diligence) or KYC (Know Your Customer).

¹¹ The AML/CFT Law , Section 11, Paragraph one, Clause 7.

the law entered into force on 01.11.2021. Since 01.11.2021 the SRS has implemented the comprehensive supervision of virtual currency service providers.¹²

26. On 6 July 2020, the amendments to the Criminal Procedure Law entered into force specifying the action when the attachment upon the virtual currency is imposed. According to Section 365(2¹) of the Criminal Procedure Law, if the attachment is imposed upon the virtual currency, it shall be handed over for sale to the person directing the proceedings. In its turn, the Cabinet Regulation No 1025 of 27 December 2011 "Regulations on the Handling of Physical Evidence and Attached Property" Chapter V.1 "Sale of Virtual Currency" determines the procedure for sale of virtual currency. The regulation was developed to improve the legal framework and provide for the handling of virtual currency, which can be withdrawn in criminal proceedings, thus ensuring the timely sale of virtual currency and its conversion into money before the final decision enters into force.
27. The regulatory enactments of Latvia do not provide for obtaining a licence as a precondition for the provision of virtual currency services. Virtual currency service providers registered in Latvia evaluate this circumstance negatively, as the lack of a license serves as an obstacle to the provision of services, including outside Latvia (e.g. foreign competent authorities require a license to provide virtual currency services, opening of current accounts are refused based on the fact that a virtual currency service provider lacks a licence, etc.).
28. The activity of foreign-registered virtual currency service providers in Latvia are implemented within the framework of the freedom to provide services. Globally, many countries have not implemented the FATF recommendations regarding the obligations of virtual currency service providers to comply with the ML and TF prevention requirements. This creates increased ML and TF risks not only in such countries, but also in countries such as Latvia, which have established a strict regulatory framework for monitoring the ML and TF prevention, as in Latvia criminals can use the services of foreign-registered but unregulated or poorly regulated virtual currency service providers.

2. EU Regulatory Framework

29. The provisions of the EU Directive 2018/843 applicable to virtual currencies entered into force on 09.07.2018, which the EU Member States had to implement in the national regulatory enactments by 10.01.2020.¹³
30. As regards the virtual currencies, the EU Directive 2018/843 provides for the following definitions:
 - 30.1. **"Virtual currencies"** are a digital reflection of value that is not issued or guaranteed by the central bank or state institution, that is not necessarily bound to lawfully established currency and that does not have the legal status or a currency or money, but natural or legal persons accept it as means of exchange and that can be transferred, stored and traded electronically;
 - 30.2. **"Custodian wallet providers"** are an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies."¹⁴
31. According to the EU Directive 2018/843, ML and TF prevention requirements are applied to (1) virtual currency and fiat currency (coins and banknotes that are designated as legal means of payment and electronic money, of a country, accepted as a medium of exchange in the issuing country)¹⁵ exchange service providers; (2) custodian wallet providers.¹⁶ The EU

¹² Ibid, Section 45, Paragraph one, Clause 6, Sub-clause a).

¹³ Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 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. Available at: <https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:32018L0843&from=EN> (ES Direktīva 2018/843).

¹⁴ Ibid, Section 1, Paragraph two, Clause d).

¹⁵ Ibid, Recital 8.

¹⁶ Ibid, Section 1, Paragraph one, Clause c), Sub-clauses g) and h).

Directive 2018/843 also stipulates that in the Member States, virtual currency and fiat currency exchange service providers, as well as custodian wallet providers shall be registered.¹⁷

32. On 20 July 2021, the European Commission presented a package of legislative proposals aimed at strengthening EU requirements for the ML and TF prevention, including specific amendments for the virtual currency sector. One of the aims of the proposals is to adapt EU legislation to the amendment made in June 2019 to the FATF Recommendation 15 on New Technologies to cover “virtual assets” and “virtual asset service providers”, in particular by introducing new disclosure obligations for both the originator of a crypto-asset¹⁸ transfer, both to the recipients (travel rule) to ensure the traceability of cryptographic transfers and to prevent and detect their possible use in ML and TF.¹⁹
33. The European Commission has provided a proposal for the Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. By this proposal it is planned to establish uniform rules for crypto-assets, including for the transparency and disclosure requirements for issuing the crypto-assets and access to trade, consumer rights protection rules for the crypto-asset issuance, trade, exchange and holding, measures for the prevention of market abuse to ensure the integrity of crypto-asset markets.²⁰

3. FATF Standards

34. FATF Recommendation 15 “New Technologies” states that in order to manage and mitigate the risks posed by virtual assets, States should ensure that virtual asset service providers are regulated for the ML and TF prevention purposes, are licensed or registered and are subject to effective systems to monitor and ensure compliance with FATF recommendations.²¹
35. Further information on the steps that countries should take to comply with FATF Recommendation 15 can be found in the Interpretive Note to the Recommendation²², as well as in the FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.²³
36. As regards virtual assets, FATF establishes the following definitions:
 - 36.1. **“Virtual assets”** are a digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

¹⁷ Ibid, Section 1, Paragraph twenty-nine.

¹⁸ Definition of crypto-assets complies with the definition of virtual assets described in the FATF standards. Proposal for Regulation of the European Parliament and of the Council of 20.07.2021 on information accompanying transfers of funds and certain crypto-assets (Recast) p.4 Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:08cf467e-ead4-11eb-93a8-01aa75ed71a1.0016.02/DOC_1&format=PDF


¹⁹ Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690.

²⁰ Proposal for the Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0016.02/DOC_1&format=PDF.

²¹ International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. Updated June 2021. Available at: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>, Recommendation 15, p. 17.

²² Ibid, p. 76.

²³ Updated guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. October 2021. Available at: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>.

- 
- 36.2. **“Virtual asset service providers”** are any natural or legal person who is not covered elsewhere under the FATF Recommendations, and as a business conduct 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;²⁴
 - 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.²⁵
37. The term “virtual assets” is used in the documents issued by the FATF, while the term “virtual currencies” is used in the regulatory enactments of the EU and the regulatory enactments of the Republic of Latvia, although their definitions overlap in essence. In the context of this Risk Assessment, the term “virtual currencies” will be used hereinafter in accordance with the definition contained in the AML/CFT Law, however, its meaning shall be interpreted identically to the term “virtual assets” used by the FATF.
38. Non-fungible tokens in the FATF standards are generally considered to be collectibles rather than virtual currencies. However, in exceptional cases, these tokens or NFTs may be considered as virtual currencies if these tokens are used in practice for making payments or investments. Given the rapid development of technologies, countries should evaluate the application of FATF standards to the use of individual NFTs.²⁶

4. Conclusions

39. The AML/CFT Law defines virtual currency service providers broadly, determining them as persons who provide virtual currency services. The list of virtual currency services includes, for example, the exchange between virtual currencies and fiat currencies, as well as exchange between one or more types of virtual currencies. However, given the rapid changes in both the virtual currency services offered and their technical solutions, this list is not exhaustive and other types of services defined by the FATF, such as virtual currency transfer or virtual currency safekeeping, are essentially included in the AML/CFT Law.
40. The AML/CFT Law imposes stricter customer due diligence requirements on transactions with virtual currencies than required by international standards. Such a requirement reduces the vulnerability of ML/TF/PF virtual currency transactions. At the same time, the introduction of stricter requirements may deter potential virtual currency service providers from registering in Latvia or other jurisdictions that impose stricter requirements than international standards.
41. Continuing the FATF's increased focus on virtual currencies, as well as following the proposals of the EU regulatory enactments, it is expected that in the future the virtual currency sector in Latvia will become more regulated, setting responsibilities both in the area of ML/TF/PF prevention and consumer protection.

IV. GLOBAL TENDENCIES IN VIRTUAL CURRENCY SECTOR

1. Introduction of FATF Standards²⁷

42. In October 2018, the FATF adopted two new definitions — “Virtual assets” and “Virtual asset service provider” (see above), and supplemented Recommendation 15. In June 2019, the

²⁴ In this context of virtual assets, *transfer* means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.

²⁵ International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. Updated June 2021. Available at: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>, 130.lp.

²⁶ Updated guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. October 2021. Available at: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>, para 53, p. 24.

²⁷ Ibid, p. 10-16.

FATF adopted the Interpretive Note to Recommendation 15 to clarify the application of requirements to virtual assets and virtual asset service providers. New Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers were added to these changes. This guidance was updated in October 2021.²⁸

43. The FATF conducted a survey on the implementation of the standards (Recommendation 15 and its Interpretive Notes) in countries to which 128 jurisdictions responded. Overall, significant progress has been made in implementing the standards, but significant gaps remain. 58 jurisdictions indicated that they had the necessary regulatory framework to comply with FATF standards (6 of these countries banned virtual currency service providers in their respective jurisdictions). A small number of these countries inspected virtual currency service providers and even fewer number of countries sanctioned breaches of ML and TF prevention legislation.
44. 26 of the countries surveyed indicated that they were in the process of drafting legislation/framework to regulate/supervise or ban the activities of virtual currency service providers. While 44 of the jurisdictions surveyed indicated that they had not yet started the process of drafting legislation/framework to regulate/supervise or ban the activities of virtual currency service providers.
45. Almost all of 52 countries that have established a regulatory framework for virtual currency service providers, apply prevention measures to virtual currency service providers. The threshold for an occasional transaction in virtual currencies above which a customer due diligence shall be performed is EUR/USD 1000 (i.e. a customer due diligence in virtual currency transactions does not have to be performed from a 'first cent'). However, some jurisdictions indicated that they have more stringent requirements. In these countries, the customer due diligence in transactions with virtual currencies shall be performed regardless of the amount of virtual currency involved in the transaction (Latvia's regulatory framework in this area is also stricter than required by FATF standards).
46. 36 countries provided information on suspicious transactions reports received from virtual currency service providers. These 36 jurisdictions indicated that in 2019 and 2020, virtual currency service providers submitted a total of 146 704 suspicious transactions reports, an increase in the number from 55 118 reports in 2019 to 91 586 reports in 2020. It should be mentioned that the number of suspicious transaction reports related to virtual currencies has been increasing in Latvia in recent years, however, none of these reports has been submitted by a virtual currency service provider registered in Latvia.
47. Regarding the supervision of virtual currency service providers, 73 countries indicated that they had designated a supervisory institution for virtual currency service providers (e.g. the supervisor of financial service providers, national central banks, tax authorities or specialized supervisory authorities directly for virtual currency service providers). The most common (in the case of 28 jurisdictions) designated supervisory authority for virtual currency service providers is the financial services supervisory authority.
48. 29 jurisdictions indicated that they had performed on-site or off-site inspections of virtual currency service providers. The most common deficiencies identified in the ML and TF prevention relate to ML and TF risk assessments and internal control systems, reporting of suspicious transactions, staff training, customer due diligence, and storage of information and documents.
49. Regarding the risk assessment of virtual currencies and virtual currency service providers, 70 countries indicated that they had performed such assessment. The following factors were mentioned as the most frequently identified risks related to virtual currencies and virtual currency service providers:
 - 1) anonymity,
 - 2) cross-border transactions,

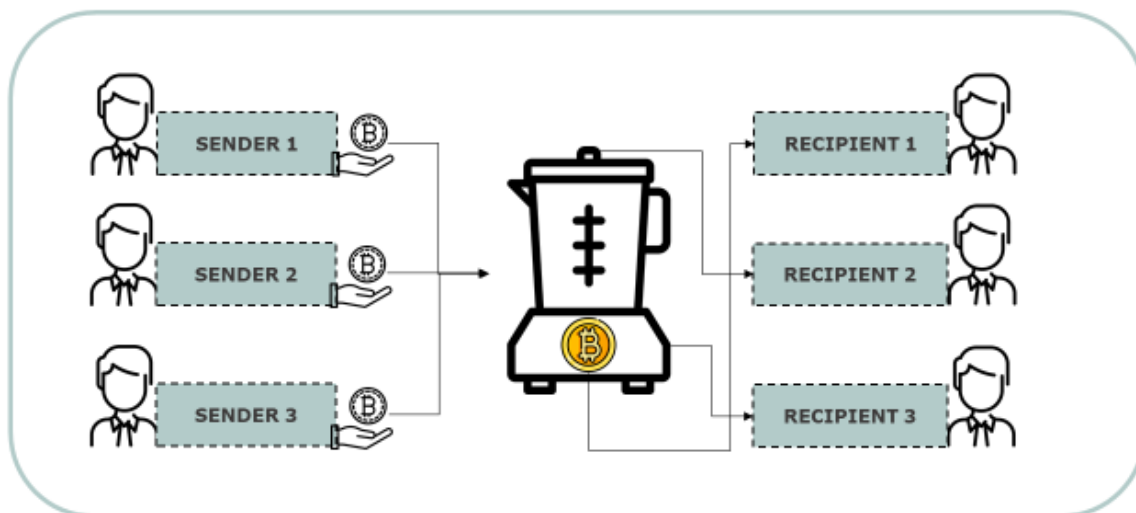
²⁸ Updated guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. October 2021. Available at: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP>

- 3) regulatory shortcomings,
- 4) level of technical knowledge about virtual currencies, virtual currency service providers, and ML and TF prevention.

2. Internationally identified virtual currency ML and TF risks²⁹


50. The popularity of virtual currencies has grown significantly over the past year, with more than a million Bitcoin addresses in April 2021. The use of virtual currencies in the traditional financial sector is also increasing. Several traditional financial institutions, including banks, credit card providers and payment service providers offer virtual currency services, sometimes also in cooperation with virtual currency service providers.
51. The value of virtual currencies in ML and TF cases identified so far has been low compared to the ML and TF cases where traditional financial services are used. Also, in most cases where ML and TF are detected, only one specific virtual currency was used. In the cases where several virtual currencies were used in the ML, their use was mainly to layer the proceeds of crime.³⁰
52. For example, often proceeds of crime (criminally acquired virtual currencies) are laundered through a service, the purpose of which is to disguise the true ownership of the funds. In a process called “mixing”, a service provider accepts virtual currency funds from multiple sources, then combines them, and then ensuring that they are returned to the sources in the same value, less a “commission” on the transactions (see Figure 1). As a result of such mixing, it is difficult to trace the transaction history and identify the initial source of funds.

Figure 1.



²⁹ Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers. July 2021. Available at: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf>, p. 21-23

³⁰ ML as a set of specific activities is a single process that can be divided into three basic stages: (1) placement, (2) layering, and (3) integration. In the layering or structuring stage, the proceeds of crime, by simulating various transactions, are: a) moved and structured with the aim of distancing them from the source of the funds; and (b) gives the impression that civil transactions are taking place. See more in the methodological material “Money Laundering Typologies and Features”. Available at: https://www.fid.gov.lv/uploads/files/2021/FID_Tipologiju%20materials_II_red.pdf.

- 
53. Virtual currencies are used, inter alia, for the commission of the following criminal offences: ML, the sale of controlled substances and other illegal items (including firearms), fraud, tax evasion, computer crimes (e.g. cyberattacks resulting in thefts and ransomware), child exploitation, human trafficking, sanctions evasion, and TF. Fraud (such as investment fraud and extortion) and drug-related criminal offences are the most common.
 54. There has been a significant increase in the amount of virtual currency paid as a ransom in the event of a cyberattack with ransomware. There has also been a significant increase in the use of virtual currencies in fraud and the subsequent ML, which is in line with global practices regarding the misuse of on-line financial services as a result of COVID-19-related restrictive measures.
 55. The development of encrypted ransomware should be specifically mentioned, which have affected national governments, schools, hospitals and other critical infrastructure around the world. The proceeds of such encrypted ransomware are often transferred through unhosted or privacy wallets³¹ and/or other anonymizing mechanisms and methods to virtual currency service providers, where they are exchanged for other virtual or fiat currencies.
 56. Most of the detected ML and TF cases related to virtual currencies take place in the virtual currency environment from the outset, i.e. the proceeds of crime are generated in the form of virtual currencies from the outset (e.g. virtual currency payments as a result of encrypted ransomware, Darknet virtual currency payments, investment fraud, etc.).
 57. However, globally there is less clarity about the extent to which virtual currencies are used to launder criminal assets in fiat currency, i.e. the extent to which virtual currency is used as a means of ML when the proceeds are obtained in cash, for example through bribery. At the same time, some countries have identified ML networks that use virtual currencies as one form of ML (e.g. by converting proceeds from drug sales into virtual currency for onward transfer).
 58. The decentralized nature of virtual currency also allows fraudsters to create their own virtual currencies to be used as a tool for fraud.³² Such schemes usually create new, lesser-known currencies to find investors, promising a sharp rise in the value of virtual currency in the near future. Once sufficient proceeds are obtained from the sale of virtual currency, the sellers of those currencies transfer the proceeds to their accounts to start money laundering, while investors remain with virtual currencies that have no real value.
 59. In the context of virtual currency ML and TF risks, the main tendencies are (1) virtual currency service providers with weak or non-existent ML and TF prevention requirements, as well as (2) methods and tools that enhance anonymity. Specific virtual currency service providers take the opportunity to register or license in the countries with ineffective framework and supervision of ML and TF prevention, or to provide services in several countries with very weak or non-existent controls on ML and TF prevention. Criminals, in turn, take advantage of the vulnerabilities and weak customer due diligence requirements of these virtual currency service providers to commit ML and TF.

V. SITUATION IN LATVIA

1. Identification of Local and Foreign Virtual Currency Service Providers

60. In 2021, there are 7 persons under the supervision of the SRS who have registered as virtual currency service providers. As part of the development of the risk assessment, the FIU organized meetings with 3 of the 7 registered virtual currency service providers (while another registered virtual currency service provider claimed that it has not provided services related to virtual currencies since 2019). 1 of 3 registered virtual currency service providers, whom the FIU met in person, also claimed that in practice it had not provided services related to

³¹ Privacy wallets allow you to make transfers where the transactions of several persons are combined in one transaction.

³² In the example of the "Squid game" virtual currency fraud case. Available at:

<https://www.theguardian.com/technology/2021/nov/01/squid-game-cryptocurrency-scam-fears-investors>

virtual currencies. It can be concluded that several companies that were registered with the SRS as virtual currency service providers in 2021 do not provide such services in practice. Consequently, the number of registered virtual currency service providers in practice does not exceed 5 obliged entities.

61. The 2 virtual currency service providers, whom the FIU met in person, provide only virtual currency exchange services (without providing other types of virtual currency services as defined by the FATF). The amounts of activities of registered virtual currency service providers are small. As virtual currency exchange services are provided only in person, the sectoral turnover in 2020 and 2021 was significantly affected by measures restricting the spread of COVID-19.
62. As part of the risk assessment, all virtual currency service providers indicated the reluctance of local financial institutions to open a current account to virtual currency service providers and to provide other services without which it is not possible to provide services online. Taking into account the above, virtual currency service providers perform their activities only in person without access to current accounts in Latvian financial institutions.
63. Several virtual currency service providers also pointed to problems in providing services abroad or opening current accounts with foreign financial institutions, as there is no licensing mechanism for virtual currency service providers in Latvia. In the opinion of virtual currency service providers, the introduction of a licensing system would facilitate cooperation with local and foreign partners, as well as expand the opportunities for providing services abroad.
64. The FCMC has not identified the use of virtual currencies in the framework of financial and capital market supervision, despite the identification of such risk in the segment of individual financial institutions in the sectoral ML/TF/PF risk assessment for 2018-2019 and 2017-2019. The Commission has also not received any requests for changes to the issued licenses from the obliged entities under the Commission's supervision for the purpose or intention of launching services related to virtual currency transactions.
65. The SP points out that various unregistered virtual currency service providers are identified in various criminal proceedings, which provide large-scale virtual currency exchange transactions for cash. This type of illegal services can be provided by both natural and legal persons and they are characterized by a high cash flow as well as transactions with various virtual currency service providers.
66. The identification of unregistered virtual currency service providers is possible through various information channels —suspicious transactions reports available to the FIU, publicly available information, information at disposal of registered virtual currency service providers, information at disposal of the supervisory and control authority, as well as other information channels may be used for the identification of virtual currency service providers.³³
67. Virtual currency service providers who are registered abroad and do not have physical branches in Latvia also offer services related to virtual currencies to customers from Latvia. Such foreign virtual currency service providers do not inform the SRS about their economic activities, as well as do not perform registration or receipt of a license. Only companies registered in Latvia, as well as branches of foreign-registered virtual currency service providers report to the SRS on the provision of virtual currency services in Latvia.
68. Although the FATF standard provides for the possibility for countries to require foreign-registered virtual currency service providers that provide services in the respective country to register in the jurisdiction to provide services, currently the SRS does not have the right stipulated in law to require registration of such foreign-registered virtual currency service providers. At the same time, the SRS has separate structural units that deal directly with the identification of unregistered economic activities and the control of such obliged entities.
69. Several virtual currency service providers registered abroad work purposefully to attract customers from Latvia, including providing information in Latvian on their websites and placing advertisements in the Latvian media space. In the reports received by the FIU on suspicious

³³ Ibid, p. 25, para 84.

transactions in which customers of Latvian credit institutions have transacted with currency service providers registered abroad, the most common countries of registration of virtual currency service providers are the United Kingdom, Estonia and Russia.

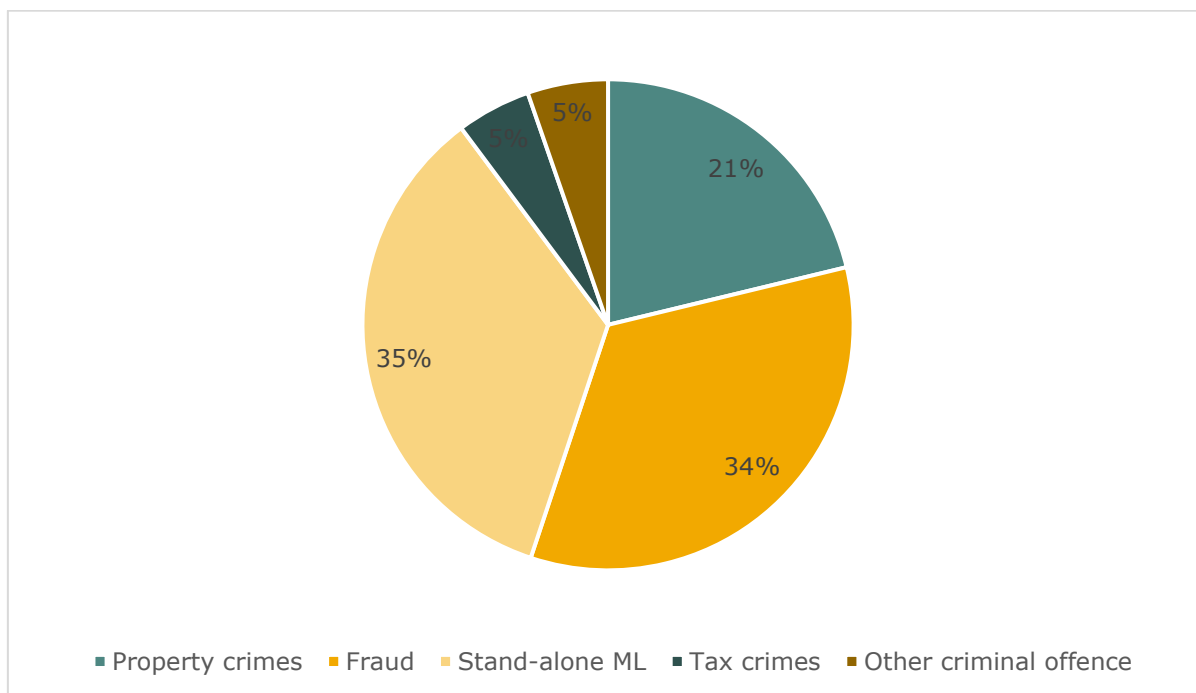
2. Reporting of Suspicious Transactions and Financial Intelligence

70. Virtual currency service providers became the obliged entities of the AML/CFT Law on 1 July 2019, however, neither in 2019, nor in 2020, nor in the first 9 months of 2021, were any reports received from virtual currency service providers. In 2019, the FIU received 45 suspicious transactions reports related to virtual currencies from other legally obliged entities.³⁴ The number of suspicious transactions reports received in 2020 increased by 87 % compared to 2019, reaching 84 reports. The rapid growth continued in the first 9 months of 2021, when 161 suspicious transactions reports in virtual currencies were received. The share of such reports in the total number of reports also increased from 0.85 % in 2019 to 1.80 % in 2020 to 3.95 % in the first 9 months of 2021.
71. The total amount of transactions included in the 2020 reports is EUR 5.0 million. On average, the total amount of transactions included in one report is about 60 thousand euros, but in only two cases the reported suspicious transactions related to virtual currencies in one transaction exceeded 100 thousand euros. Similar figures can be seen in the 2021 reports, where the average total amount of transactions included in one report is about 69 thousand euros. It can therefore be concluded that, although the number of suspicious transactions reports related to virtual currencies was growing rapidly in 2020 and 2021, the volumes of transactions are still low compared to suspicious transactions conducted through traditional financial services.
72. Compared to previous years, there is an increase in the understanding of the obliged entities of the AML/CFT Law and knowledge of virtual currencies and signs of suspicion. In 2019, approximately one quarter of the reports on transactions with virtual currencies were classified as defensive reporting,³⁵ where there was no fixed suspicion that the transaction was likely related to the commission of a criminal offence. No such reports were received in 2020 and the quality of suspicious transaction reports has significantly improved.
73. Almost half (49 %) of the suspicious transactions reports in virtual currencies were received, identifying fraud as a possible predicate criminal offence (i.e. the criminal offence resulting in the proceeds of crime), in 35 % of cases the predicate offence was not identified and the report identified suspicions of stand-alone ML (i.e. signs of ML are identified, but the subject of the AML/CFT Law does not have sufficient information to make a presumption, namely, what criminal offences have been obtained), but in another 7 % of reports other property crimes were identified as possible predicate offences.

³⁴ It is not possible to determine the exact number of reports related to virtual currencies received by the FIU because they do not have a common selection element or keyword. Various keywords are chosen to select statistics, including virtual currency names. A separate classifier will be available for reporting virtual currency transactions during the transition of the e-reporting system to the goAML system.

³⁵ Reports submitted with the aim of avoiding possible sanctions from supervisory and control authorities, rather than substantially preventing ML, TF and PF.


Table 1. Breakdown of suspicious transactions reports in virtual currencies by a group of criminal offences



74. Assessing the suspicious transactions reports received according to their content, most reports can be divided into two groups:
- (1) The customer of the subject of the AML/CFT Law (most often a financial institution) is identified as a victim of fraud, from whom the data of the means of payment or the means of payment themselves have been deceived and virtual currency has been purchased with them.
 - (2) The customer account of the subject of the AML/CFT Law (most often a financial institution) is used as a transit account for receiving funds and the subsequent purchase of virtual currencies or receiving payments from virtual currency platforms and disbursement of funds in cash. Also, in these cases, it is often recorded that the customer's data of the means of payment was obtained by a third party (often with foreign IP addresses) without the customer's knowledge.
75. In rare cases, the purchase of virtual currencies by means of possibly criminal origin is recorded, as well as in some cases suspicions are related to the structuring of virtual currency transactions and other typologies specific to ML.

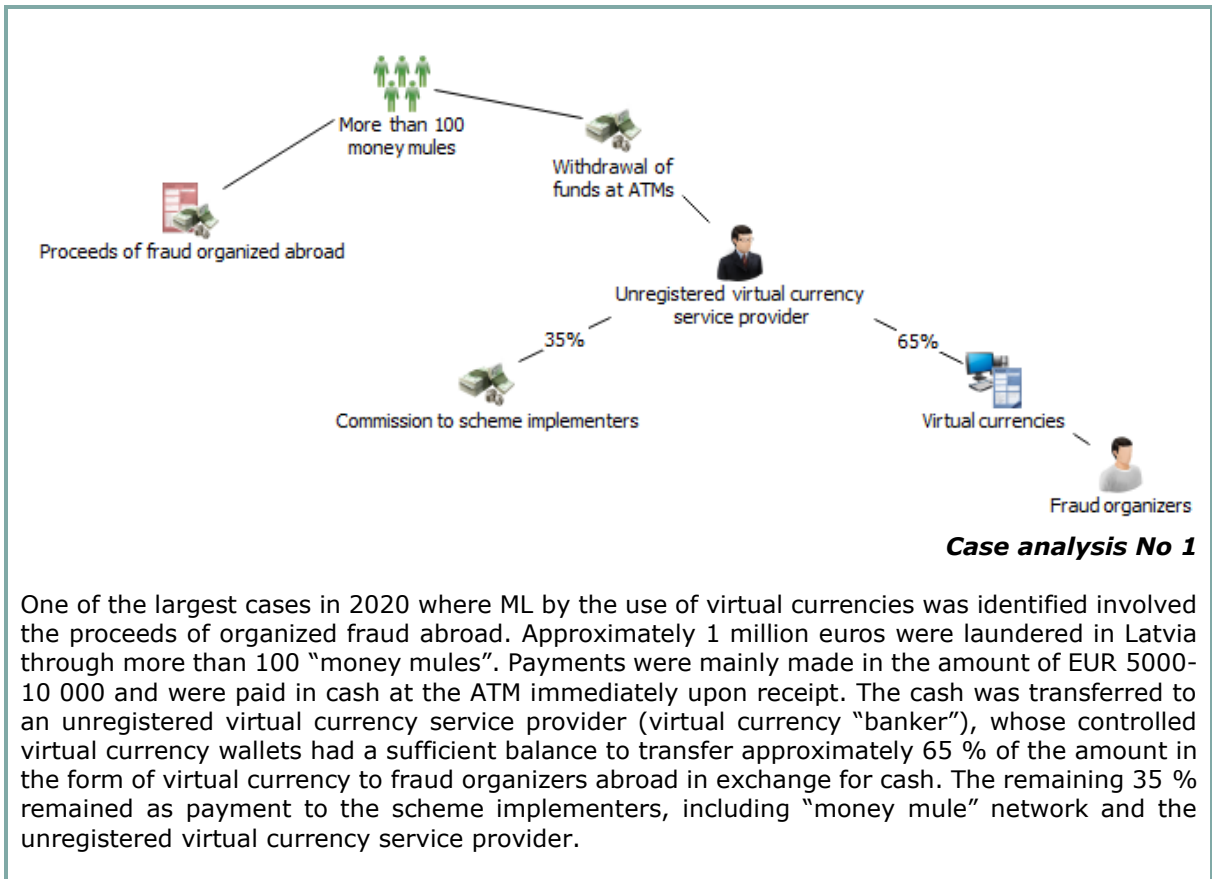
3. Investigation

76. Computer crimes in Latvia is investigated by the SP ECED. In recent years, the SP ECED has been paying increased attention to the illicit circulation of virtual currencies.
77. Currently, there are only a few cases in Latvia where virtual currency is seized as part of criminal proceedings, however, taking into account the spread and use of virtual currency in criminal activities, as well as the continuing education of officials in this area, it can be expected to increase in the future.

- 
78. The most common cases identified in practice where ML is committed through virtual currencies can be classified into three categories — virtual currency laundering, conversion of proceeds of crime into virtual currencies and layering, as well as conversion of proceeds of crime into virtual currencies to hide and store them.
79. In practice, **virtual currency laundering** is most often recorded in fraud cases where the criminal has gained access to the victim's means of payment data and purchased virtual currencies, as well as in extortion cases where the ransom is paid in the form of virtual currencies.
80. In practice, in some cases when committing the ML various foreign-registered virtual currency service providers are used, and traceability of proceeds after their conversion into virtual currencies is extremely difficult or even impossible. The following “red flags” or risk indicators are identified as part of the Risk Assessment that could indicate an attempt of fraud or extortion:
1. The purchase transaction of virtual currencies and its amount is not characteristic to the customer profile;
 2. The connection to the customer's digital banking services is made from an IP address located abroad;
 3. Funds are transferred to an unfamiliar virtual currency platform (virtual currency service provider) with low transaction volumes or to a virtual currency platform with weak ML/TF/PF prevention controls;³⁶
 4. Shortly before purchasing virtual currencies, the customer receives one or more consumer loans, including from non-bank creditors.
81. **Conversion of proceeds of crime into virtual currencies and layering** is the most common in practice in fraud cases. Schemes involving the laundering of the proceeds of fraud through virtual currencies are characterized by the use of “money mules”.³⁷ Funds defrauded abroad or domestically are structured in smaller amounts to diversify the risks associated with the seizure and confiscation of funds, to avoid the monitoring and declaration of transactions by the FIU, and to disguise the identity of the scheme's executors.

³⁶ Various websites offer virtual currency analytics services, including data collection on VC platforms, two examples are provided below. Coinmarketcap, “Top cryptocurrency spot exchanges”. Available at: <https://coinmarketcap.com/rankings/exchanges/>. Coingecko, “Top Cryptocurrency Exchanges Ranking by Trust Score - Spot”. Available at: <https://www.coingecko.com/en/exchanges>.

³⁷ “Money mule” is a person who transfers (electronically or in cash) money received from a third party to another person in return for a commission.



82. Case analysis No 1 should highlight the role of the credit institution in question in identifying the scheme for the ML detection. The network of "money mules" was, by various features, linked as members of a single scheme, which ensured a much more efficient and faster course of action than if each "money mule" was reported separately. Features by which the interrelation of "money mules" was identified:
- 1) features attributable to "money mules" (e.g. citizenship);
 - 2) features attributable to transfers (e.g. similar payment purposes, similarity of senders);
 - 3) features attributable to the disbursement of funds (e.g. similar disbursement times, amounts).
83. **Conversion of proceeds of crime into virtual currencies to hide and store them** is one of the growing threats posed by new technologies. Unlike layering of proceeds (see definition above), the main purpose of which is to make it difficult to trace the flow of funds, the long-term preservation of the value of funds is as important a factor as anonymity in the concealment and safekeeping of the proceeds of crime. This is confirmed by the cases recorded in practice, where criminals choose to diversify the risks of virtual currency price fluctuations by investing in different virtual currencies, as well as the funds are stored on well-known, reliable virtual currency exchange platforms.
84. The experience and knowledge required to manage such multi-virtual currency portfolios can be offered to criminals by unregistered virtual currency service providers (virtual currency "bankers"), who also hide and store the proceeds of crime in the form of virtual currencies on a day-to-day basis.

Case analysis No 2

In 2020, SP ECED terminated the activity of a group of cybercriminals that committed various types of fraud abroad, while ML committed in Latvia. Three persons were detained within the framework of criminal proceedings.

During the search and other investigative activities, a significant amount of cash and tangible assets — cash — around EUR 280 000 and USD 37 000, as well as virtual currency (BTC, ETH, XRP and USDT) worth more than EUR 110 000 thousand were seized. A number of seizures were made on the suspects' private property and vehicles — 11 real estates with a total market value of around EUR 315 000 and three cars with a total market value of around EUR 30 000.

In order to use the proceeds of crime for the purchase of real estate, vehicles and everyday goods, ML was mainly committed without the involvement of new technologies, using ML methods such as payment for fictitious services, gambling imitation, etc.

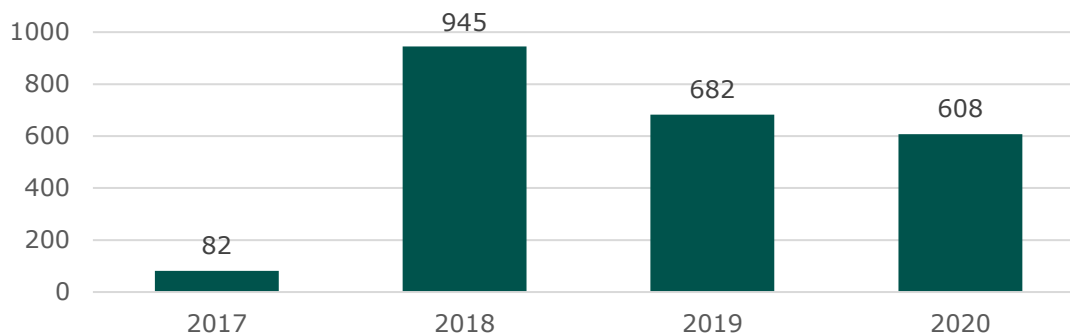
85. *Table No 1* categorizes features of each of the ML (using virtual currency) categories identified in practice.

Table No 1.

| | Virtual currency laundering | Conversion of proceeds of crime into virtual currencies and layering | Conversion of proceeds of crime into virtual currencies to hide and store them |
|---|---|---|---|
| Virtual currency service provider | Higher risk, less-known virtual currency service provider | Higher risk, less-known virtual currency service provider | Lower risk, well-known virtual currency service provider |
| Types of virtual currencies | The most common virtual currencies, in some cases virtual currencies that provide greater anonymity, make it difficult to trace | The most common virtual currencies, in some cases virtual currencies that provide greater anonymity, make it difficult to trace | Both the most common and other virtual currencies with the aim of diversifying risk and preserving the value of funds |
| Typical predicate criminal offences | Criminal offences committed in the digital environment (fraud, extortion) | Criminal offences committed in the digital environment (fraud) | Any predicate criminal offence, including corruption |
| Conversion of proceeds into virtual currencies | n/a | Most frequently committed by unregistered virtual currency service provider | Most frequently committed by unregistered virtual currency service provider |

86. Drug trafficking is a criminal offence in which virtual currencies are often used to purchase drugs, while proceeds (from the sale of drugs) are often converted into virtual currencies to commit a repeat criminal offence. Since 2018, a significant amount has been included in the records of the SRS TCPD with criminal proceedings for the purchase of drugs in Darknet and illegal import into Latvia via postal items. According to *Table No 2*, the number of such criminal proceedings in which virtual currencies are used for the purchase of drugs exceeds 600 each year, which makes up 80-90 % of all criminal proceedings initiated by the SRS TCPD for illegal import of drugs into Latvia.

Table No 2. Criminal proceedings initiated by the SRS TCPD for drug shipments the payment for which is made by the use of VC



87. These criminal proceedings are initiated for small purchases up to a minimum 50 monthly wages (or EUR 21 500 in 2020 and EUR 25 000 in 2021). This is how drugs are bought for both own use and further distribution and marketing. Virtual currencies for the purchase of drugs in Darknet are often purchased through both peer-to-peer (P2P) platforms (i.e. without using a virtual currency service provider) and virtual currency exchange platforms, but the use of unregistered virtual currency service providers is less common.
88. Characteristics of a drug dealer:
- 1) no regular income;
 - 2) many small incoming payments;
 - 3) investments in virtual currencies are structured in a number of small payments.
89. SP ECED investigators have so far demonstrated the ability to investigate ML committed through virtual currencies, but it should be noted that the initiated criminal proceedings in these cases are still ongoing and the litigation process will reflect, inter alia, the quality of the investigators' work. In order to further improve the quality of investigation, it is important to provide SP ECED investigators with software for more efficient tracking of virtual currency transactions, as well as to provide training in these issues.
90. The need for software and training is also applicable to SRS TCPD investigators. In criminal proceedings for drug shipments by mail, in practice the person is most often charged with one particular shipment, while an investigation of virtual currency transactions would likely allow the recording of multiple drug purchases (if any), thus increasing the effectiveness of the fight.

4. Case Law

91. Among the case law judgements analysed, where virtual currencies are mentioned, most relate to the purchase of narcotic/psychotropic substances from various Darknet websites. Darknet's "Dream market" site, where Bitcoin is used to pay for purchases, is the most frequently mentioned site in court decisions for the purchase of narcotic/psychotropic substances, while the less frequently mentioned sites are "AlphaBay" and "Evolution". In the analysed court judgements, persons have been punished for the movement of goods and substances, the circulation of which is prohibited or specially regulated, across the border of the Republic of Latvia and for the unauthorized manufacture, acquisition, storage, transportation and forwarding of narcotic and psychotropic substances.
92. At the end of 2020, more complicated ML cases using virtual currencies are still pending. It is expected that in the coming years, more and more criminal proceedings involving virtual currencies will be brought before the courts, demonstrating the ability of both prosecutors and judges to prosecute and adjudicate in these criminal proceedings, respectively.

Court judgement analysis No 1

Judgement No K73-0061-19/41 of Zemgale District Court of 16 October 2019.

Person B is accused according to Section 190¹(1), Section 190¹(2) of the Criminal Law (Movement of Goods and Substances the Circulation of which is Prohibited or Specially Regulated across the State border of the Republic of Latvia) and Section 253(1) (Unauthorised Manufacture, Acquisition, Storage, Transportation and Forwarding of Narcotic and Psychotropic Substances). Person B purchased the psychotropic substance from the Netherlands using the TOR internet browser on the "Dream Market" website, using the virtual currency Bitcoin, i.e. performed activities to receive a postal item with a psychotropic substance in Latvia. The consignment with the psychotropic substance was received at the SRS Customs Department in airport, there with the help of a special investigative activity — within the control of criminal activity, the psychotropic substances with the same appearance and size were replaced and delivered to the person's B address, where, being aware that the psychotropic substances were in the postal item, person B accepted the consignment from the postman against a signature. The psychotropic substance ordered by person B is included in Schedule I "Prohibited especially dangerous narcotic substances, equal psychotropic substances and plants the illicit circulation and abuse of which endangers health". Person B illegally purchased and stored psychotropic substances without the intention of selling them. Person B pleaded guilty, the court found him guilty and sentenced him to 3 years' imprisonment, with probation period for 2 years.

Court judgement analysis No 2

Judgement No K33-0135-19/9 of Riga District Court of 7 February 2019.

Person B is accused according to Section 190¹(1), Section 190¹(2) and Section 253(1) of the CL. Person C is accused according to Section 20(4) (Participation), Section 190¹(2) and Section 253(3) (Unauthorised Manufacture, Acquisition, Storage, Transportation and Forwarding of Narcotic and Psychotropic Substances for the Purpose of Sale and Unauthorised Sale thereof) of the CL. Person B ordered a psychotropic substance from the "AlphaBay" website — two pieces of paper perforated in 10 stamps impregnated with LSD. This psychotropic substance was ordered by person B with delivery by post, paying for the previously purchased virtual currency Bitcoin. Person C supported the forwarding of a large amount of narcotic and psychotropic substances across the border of the Republic of Latvia, he agreed to give person B his address to which to send the consignment from the Netherlands. The court found both persons guilty, person B was sentenced to 5 years' imprisonment, community service for 120 hours and probation supervision for 1 year. Person C was sentenced to 4 years' imprisonment.

93. In the analysis of the court judgement No 3, persons converted the proceeds of crime into other values, changing their location and affiliation being aware of the fact that the proceeds were obtained as a result of crime. These activities were performed to help another person involved in the commission of a criminal offence avoid legal liability. The virtual currency was also purchased using the proceeds of crime, which then was transferred to an unidentified person.

Court judgement analysis No 3

Judgement No K33-1795-19/43 of Riga City Vidzeme Suburb Court of 9 July 2019.

Person A and person B are accused according to Section 195(2) of the CL (Money laundering). Person A agreed with person B to take concerted activities on money laundering, in particular, under the agreement, person B undertook to find persons to open current accounts in their own name, to which an unidentified person would transfer the proceeds of crime. Subsequently, person B ensured the transfer of the received funds to person A, who, by prior arrangement, transferred part of the proceeds of crime to an unidentified person using the services of financial institutions, as well as by transferring electronic money in the system to the virtual currency Bitcoin. In this way, the persons agreed to commit a common criminal offence, namely to hide the criminal origin of the proceeds and to help another person — an unidentified person, to avoid legal

liability, decided to convert the proceeds of crime into other values and to change the location and ownership of the proceeds being aware of the fact that these proceeds were obtained as a result of crime. The court found both persons guilty, with person A being sentenced to 3 years' imprisonment and an additional punishment — community service of 100 hours, and person B being fined the minimum 10 monthly wages set by the Cabinet, i.e. in the amount of EUR 4300.

VI. TF and PF RISKS OF VIRTUAL CURRENCIES

94. In 2019 and 2020, the FIU received one report of suspicions against the TF using virtual currencies. In general, no significant TF risks related to the use of virtual currencies have been identified in Latvia. It should be noted that according to the NRA, the risk level of Latvia's national TF was also assessed as low.
95. However, given the benefits of virtual currencies, including anonymity element, virtual currencies can be used in TF. Virtual currency (with some exceptions) transactions and operations are publicly visible, but there are difficulties in identifying who made them, it is difficult to identify the customer, and blockchains are located in many countries, which makes it difficult to detect the criminal offence, to identify and charge with criminal liability the persons involved.

Case analysis No 3

In March 2020, the United States issued a conviction related to TF by the use of virtual currencies. Zoobia Shahnaz, a U.S. citizen of Pakistani descent, was convicted and sentenced to 13 years' imprisonment for attempting to travel for terrorism purposes.

Between March and July 2017, the person defrauded several credit institutions, including in the form of a loan of approximately USD 22 500, and fraudulently acquired control of more than ten credit cards and used them to purchase Bitcoin and other virtual currencies in the amount of approximately USD 62 000.

Funds, including virtual currency, totalling USD 150 000 were transferred to Islamic State agents in Pakistan, China and Turkey. On 31 July 2017, Shahnaz was detained at the airport before a scheduled flight to Turkey to later join Islamic militants.

96. The FATF's 2015 TF Risk Study³⁸ indicates that social networks and mobile communication platforms are used to disseminate terrorist propaganda material, communicate with supporters, and organize fund-raising campaigns, often requesting to donate through virtual currencies. Funds are requested to be donated, both openly addressing the supporters of a terrorist organization and through misleading fund-raising campaigns, where the person committing the TF may not be aware of the true purpose of the funds.
97. There are different levels of user anonymity between different virtual currencies. Bitcoin, the first virtual currency with the convincing highest market capitalization rate, provides users with only partial anonymity.³⁹ Cryptographic addresses that are publicly available, although not directly related to the identity of the trader, can be used to establish the identity of the trader with appropriate investigative resources.
98. Although Bitcoin does not provide anonymity on a scale similar to other virtual currencies, the widespread use of Bitcoin and its market status make it a common use in the commission and support of criminal offences, including TF. To ensure the anonymity of supporters, terrorist organizations request to make donations in Bitcoin currency in cash via virtual currency exchange points (virtual currency "ATMs")⁴⁰ or to transfer funds between multiple

³⁸ Available at: <https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>

³⁹ Europol, "Internet Organised Crime Threat Assessment Report, 2021" Available at: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2021>.

⁴⁰ See: <https://coinatmradar.com/>.

cryptographic addresses before making a donation, thus making the supply chain more complicated.⁴¹

99. The FIU did not receive any reports of suspected PF in virtual currencies in 2019 and 2020, and the risks of national PF using virtual currencies are not considered high. However, it should be noted that virtual currency may be used to obtain, store and transfer funds for PF purposes. It is necessary to trace suspicious transactions when assessing their possible connection with the Democratic People's Republic of Korea (hereinafter referred to as — North Korea), which is included in the European Union sanctions list, and which actively uses the virtual currency in PF.
100. The Royal United Services Institute (RUSI) indicated that North Korea is using the virtual currency to evade sanctions against North Korea and fund the development of nuclear weapons. The use of Bitcoin and other virtual currencies in computer crime provides funding for North Korea's weapons of mass destruction programme. The cross-border nature of virtual currencies makes it an attractive tool for those who want to bypass the traditional financial system. It can be concluded that North Korea performs transactions with other countries and persons with the help of virtual currency in order to circumvent the sanctions intended to restrict PF.⁴²
101. In 2019, the media reported that North Korean hackers had stolen up to 1.8 billion euros from financial institutions and virtual currency exchanges.⁴³ According to an expert report to the UN Security Council, large-scale attacks on virtual currency exchanges are enabling North Korea to generate revenue in more difficult-to-trace ways and direct those funds to weapons of mass destruction programmes.⁴⁴
102. In order to perform the layering of funds, criminals carry out thousands of virtual currency exchange transactions through service providers in different jurisdictions before the funds are exchanged from the virtual currency for cash. After one of these attacks, international transactions in the amount of at least 5 thousand were performed using a blockchain platform for layering funds before the virtual currency is exchanged for a legal means of payment.⁴⁵

⁴¹ In early 2018, organisation “Al-Sadaqah”, through the Darknet website, Twitter and Telegram accounts, requested to make donations to support Syrian militants through virtual currency exchange points or by transferring funds through various cryptographic addresses. Available at:

<https://www.memri.org/reports/coming-storm-%E2%80%93-terrorists-using-cryptocurrency>

⁴² Available at: https://www.rusi.org/sites/default/files/20190412_closing_the_crypto_gap_web.pdf

⁴³ Available at: <https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf>

⁴⁴ Semi-annual report 2019 of UN Security Council. Available at: https://www.securitycouncilreport.org/atf/cf/%7B65BF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf

⁴⁵ Semi-annual report 2019 of UN Security Council. Available at: https://www.securitycouncilreport.org/atf/cf/%7B65BF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf

VIRTUAL CURRENCY “RED FLAGS” OF ML/TF

1. In 2020, the FATF published material on the ML and TF “red flags” or risk indicators⁴⁶ of virtual currencies to help the obliged entities of the AML/CFT Law (financial institutions and non-financial service providers and virtual currency service providers) identify signs of suspicious transactions related to virtual currencies.
2. The risk indicators mentioned in the FATF’s material are specific to the nature of virtual currencies and related financial activities. It is not considered an exhaustive list of risk indicators. **Risk indicators should always be considered in the context of other facts and circumstances that characterize the customer, the transaction and the business relationship. The identification of a risk indicator does not in itself give rise to suspicion of ML or TF, but may provide a basis for further inspection or enhanced supervision.**⁴⁷ Frequently, a set of several risk indicators in a single transaction without a logical explanation may give rise to suspicion of possible connection to the crime.⁴⁸ Some of the FATF-identified indicators of ML/TF risks associated with virtual currencies are listed below.

1. Risk Indicators Related to Transactions and Transaction Patterns⁴⁹

- Structuring virtual currency transactions (e.g. exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds, similar to structuring cash transactions.
- Making multiple high-value transactions:
 - in short succession, such as within a 24-hour period;
 - in a staggered and regular pattern, with no further transactions recorded during a long period afterwards, which is particularly common in ransomware-related cases; or
 - to a newly created or to a previously inactive account.
- Transferring virtual currencies immediately to multiple virtual currency service providers, especially to virtual currency service providers registered or operated in another jurisdiction where:
 - there is no relation to where the customer lives or conducts business; or
 - there is non-existent or weak AML/CFT/CPF regulation.
- Depositing virtual currencies at an exchange and then often immediately:
 - withdrawing the virtual currencies without additional exchange activity to other virtual currencies, which is an unnecessary step and incurs transaction fees;
 - converting the virtual currencies to multiple types of virtual currencies, again incurring additional transaction fees, but without logical business explanation (e.g. portfolio diversification); or
 - withdrawing the virtual currencies immediately to a private wallet. This effectively turns the exchange/virtual currency service provider into an ML mixer.
- Accepting funds suspected as stolen or fraudulent:
 - depositing funds from virtual currency addresses that have been identified as holding stolen funds, or virtual currency addresses linked to the holders of stolen funds.

⁴⁶ FATF Report: Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing. September 2020.

Available: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf>

⁴⁷ Ibid, p. 4.

⁴⁸ Ibid, p. 5.

⁴⁹ Ibid, p. 5-8.

- Conducting a large initial deposit to open a new relationship with a virtual currency service provider, while the amount funded is inconsistent with the customer profile.
- Transactions involving the use of multiple virtual currencies, or multiple accounts, with no logical business explanation.
- Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency.
- Conducting virtual currency-fiat currency exchange at a potential loss (e.g. when the value of virtual currency is fluctuating, or regardless of abnormally high commission fees as compared to industry standards, and especially when the transactions have no logical business explanation).

2. Risk Indicators Related to Anonymity⁵⁰

- Transactions by a customer involving more than one type of virtual currency, despite additional transaction fees, and especially those virtual currencies that provide higher anonymity.
- Moving a virtual currency that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an anonymity enhanced cryptocurrency or privacy coin.
- Customers that operate as an unregistered/unlicensed virtual currency service providers on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amount of virtual currency transfers on its customer's behalf, and charge higher fees to its customer than transmission services offered by other exchanges. Use of bank accounts to facilitate these P2P transactions.
- Transactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and Darknet marketplaces.
- The use of decentralised/unhosted, hardware or paper wallets to transport virtual currencies across borders.
- A large number of seemingly unrelated virtual currency wallets controlled from the same IP-address, which may involve the use of shell wallets registered to different users to conceal their relation to each other.
- Receiving funds from or sending funds to virtual currency service providers whose customer due diligence or know-your-customer processes are demonstrably weak or non-existent.
- Using virtual currency ATMs:
 - despite the higher transaction fees and including those commonly used by mules or scam victims; or
 - in high-risk locations where increased criminal activities occur.⁵¹


3. Risk Indicators Related to Senders and Recipients⁵²

⁵⁰ FATF Report: Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing. September 2020.

Available: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf>, p.9-11

⁵¹ A single use of an ATM is not enough in and of itself to constitute a red flag, but would if it was coupled with the machine being in a high-risk area, or was used for repeated small transactions (or other additional factors).

⁵² FATF Report: Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing. September 2020 Available at: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf>, p. 12-15

- 
- Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by virtual currency service providers.
 - Sender/recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty.
 - A customer's virtual currency address appears on public forums associated with illegal activity.
 - Customer purchases large amounts of virtual currency not substantiated by available wealth or consistent with his or her historical financial profile, which may indicate ML, a money mule, or a scam victim.
 - A customer frequently changes his or her identification information, including email addresses, IP addresses, or financial information, which may also indicate account takeover against a customer.

4. Risk Indicators Related to the Source and Geography of Funds or Wealth⁵³

- Virtual currency transactions originating from or destined to online gambling services.
- The use of one or multiple credit and/or debit cards that are linked to a virtual currency wallet to withdraw large amounts of fiat currency (crypto-to-plastic), or funds for purchasing virtual currencies are sourced from cash deposits into credit cards.
- Bulk of a customer's source of wealth is derived from investments in virtual currencies, initial coin offerings (ICOs) and fraudulent ICOs.
- A customer's source of wealth is disproportionately drawn from virtual currencies originating from other virtual currency service providers that lack AML/CFT controls.
- Customer's funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located.
- Customer sets up offices in or moves offices to jurisdictions that have no regulation or have not implemented regulations governing virtual currencies, or sets up new offices in jurisdictions where there is no clear business rationale to do so

⁵³ FATF Report: Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing. September 2020. Available at: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf>, p. 15-18