IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/38DigECO/2021/38114821/
Vol. 2021 (37), Article ID 38114821

Crypto Compliance: Adopting A Risk-Based Approach to Crypto Assets Exchange Within Crypto Currency Exchange Company Licensed In EU

Olegs CERNISEVS

Baltic International Academy, Riga, Latvia, olegs.cernisevs@gmail.com

Correspondence should be addressed to: Olegs CERNISEVS; olegs.cernisevs@gmail.com

* Presented at the 38th IBIMA International Conference, 23-24 November 2021, Seville, Spain

Abstract

Despite the fact that approved by Europarlament, 2018 Directive requested that Crypto currency exchange companies should apply anti money laundering norms for all operations with crypto assets, approaches to such companies still were no developed and described. These changes open crypto currency exchange companies for vulnerability in terms of exposure for money laundering and therefore money laundering risk assessment is critically necessary.

The same approach is also acceptable for financial institutions who deal with crypto assets. Within last year's number of Initial Coin offers increased dramatically (Hsieh and Oppermann, 2021) , in result variety of the crypto assets trading within crypto currency exchange was increased too. All above mentioned increase necessity for the effective money laundering risk management. This paper aims to identify the approach how to access money laundering risk in crypto currency exchange companies.

Author analyzed EU legal norms, defined the principles of the AML risk assessment for Crypto assets exchange companies and offer risk Calculation matrix.

Keywords: Crypto, AML, Compliance

Introduction

Generally, money laundering is described as the process by which the illegal nature of criminal proceeds is concealed or disguised in order to give a legitimate appearance to these illegal proceeds. (FIAU, 2021) Namely, the money laundering allows to criminals use the incomes from the illegal activity for the legal operations including financing some legal businesses. With the purpose to achieve that goal, criminals mask the source of incomes or move the funds, arise from the illegal activity, to destinations where they are less likely to attract attention.

The main methods, which use criminals for that purpose are:

- Placement
- Layering
- Integration

When we are speaking about Placement, we assume that criminals try to use official financial and nonfinancial organizations to place illicit proceeds into financial system. Like splitting amount for small tranches, mixing illicit proceeds with legal

Cite this Article as: Olegs CERNISEVS, Vol. 2021 (37) "Crypto Compliance: Adopting A Risk-Based Approach to Crypto Assets Exchange Within Crypto Currency Exchange Company Licensed In EU", Communications of International Proceedings, Vol. 2021 (37), ISBN: 978-0-9998551-7-1, ISSN: 2767-9640. Article ID 38114821

incomes, purchasing currency like forex exchange. At that moment proceeds which forms money laundering are easier detected.

The process of transformation, splitting and forming of complicated levels of financial transactions is called Layering. Within this phase of the money laundering illicit proceeds, previously placed into financial systems, converted into forms, which will allow to hide real source of incomes and/or these funds ownership.

The final stage of the money laundering is integration. Within this phase illicit proceeds, which was previously successfully layered by criminals are used for the purchase of valuables, property or finance other private or linked to any corporation expenses. Within this stage illicit proceeds may be also used to form or finance legal business.

Crypto assets and company who operate them, like crypto currency exchange can be used as the tools in all three stages of money laundering and therefore effective approach for anti-money laundering policy should be developed.

(Europarlament, 2018) defines that approach used for mitigating the effect of the money laundering to business should be risk based. That's mean that money laundering for the company is the risk, and therefore all internal anti-money laundering policies should be based on risk management.

Risk Based Approach

Before address the risk assessment, the business of crypto currency exchange companies should be assessed.

Crypto currency exchange companies are place for the issued crypto assets secondary market(Giudici et al., 2020). In accordance to the 5th AML directive (Europarlament, 2018) all European Economic Area (EEA) countries should adopt into their national legislation obligation to the crypto currency exchange companies became subject to local Anti-money laundering legislation. Besides that, EU countries have differences in local legislation regarding licensing of such activities and therefore operations, which may fulfill such companies are also differs (Hacker and Thomale, 2018). Despite that fact, for all crypto currency exchange companies are typical following services, they offer to customers:

- Customer Wallet services – that's mean that company holds for they customers crypto wallets where customers hold their crypto assets.
- Wallet deposit services – these services allow to company's customers place into wallets crypto assets via blockchain and/or fiat currency by traditional financial systems.
- Wallet withdrawal services - these services allow to company's customers withdraw from wallets crypto assets via blockchain and/or fiat currency by traditional financial systems.
- Exchange services – these services will allow to the company customers exchange assets within their wallets for fiat or other crypto assets.

All above mentioned services form business activity of the crypto currency exchange company, and respectively all above mentioned activities may be linked to any or even all above-described money laundering stages.

From other hand, analyzing such companies' activity by the form of providing of these services it is obvious that all above mentioned services are provided in electronic form.

The channels used for such operations are – classical financial systems and blockchain.

Summarizing all above mentioned, author define that from one perspective the money laundering within crypto currency exchange company is similar to the money laundering withing financial institution. On the other hand, similar to security risk (Amundrud et al., 2017), the risk arises from interaction of vulnerabilities – internal company business management gaps, which may lead to money laundering and treats – events, internal or external, which may provoke money laundering. Cox, 2008 defines the risk as:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence}$$

If we will address above mentioned elements to money laundering risk then, under we will assume that:

- Threat – are defined as the external elements that seek to exploit vulnerabilities of the Company.
- Vulnerability – are defined as the weaknesses that may be exploited for money laundering and terrorist financing purposes.
- Consequence – is impact.

All three above mentioned components should be assessed, taking into account the nature of the business and related to the business and it's environment characteristics.

Threats

Autor analyzed FATF recommendations (FATF, 2021), norms Based on the 5th AML directive (Europarlament, 2018) and defined following threats, typical for crypto currency exchange companies:

1. Identity Fraud
2. Fraudulent documents
3. Business activity of the customer
4. Geographical location
5. False/Incorrect personal data
6. Customer Criminal Record on ML/TF
7. Politically Exposed Person
8. Sanctions on the customer
9. Concealment of Beneficial Ownership
10. Customer's geographical location from Sanctioned country
11. Transaction received from Sanctioned country
12. Transaction sent to Sanctioned country
13. Politically Exposed Person receiver
14. Sanctions on the transaction receiver
15. Beneficiary is a Politically Exposed Person
16. Customer reputation related to scam or fraud
17. Unlicensed activity transactions in cases where it is required
18. Customer business activity or source of funds is illegal
19. Counteragent source of funds from illegal activity
20. Non-identified parties account usage
21. Distributors AML/TF non-compliance control system
22. Outsourcing company will provide illegitimate information
23. Outsource company databases not updated
24. Outsource company failure to perform an adverse media check
25. Outsource company failure of Sanction screening

Vulnerabilities

Analyzing crypto currency exchange company business activity, described above, author defines following vulnerabilities:

1. Failure of Customer KYC procedure
2. Compliance policies are not followed
3. Insufficient Customer Risk score
4. VPN usage to hide real location
5. Poor Compliance Officer training
6. Screening program on Criminal Record check database not synchronise between the countries Beneficiary has relevant link to a PEP
7. Failure of Sanction screening
8. Failure to perform an adverse media check
9. Compliance Officer non-observance
10. Human factor
11. Incorrect Customer Risk score
12. Inappropriate Transaction Monitoring rules
13. Lack of transaction monitoring system
14. Not updated monitoring transaction policy
15. Uncontrolled compliance actions
16. Transaction valuation does not reflect the real value of item
17. Transactions without logical explanation
18. Failure to comply with AML/CFT requirements
19. Beneficiary shared access to the account with 3rd parties
20. Account opening by face-to-face identification
21. Account opening by non-face to face identification
22. Transactions made in company office face to face

23. Transaction made by using mobile or desktop version
24. Face-to-face communication with the customer
25. Non-face-to-face communication with the customer

Risk Calculation

Every vulnerability and threat identified below will have a certain likelihood of occurring and the Severity on the operations of the Company. In general, the ratio of the likelihood and severity will be assessed in the following way considering the risks ranging from the low to the extreme where the lowest is 1 and the highest is 16:

Table 1: Risk calculation table

	Severity/Impact			
Likelihood	1	2	3	4
	2	4	6	8
	3	6	8	12
	4	8	12	16

Source: Developed by author

The figures in the tables are showing the final risk scoring that provides the multiplied combinations of the probability and impact that will have the most severe consequences for the operations of the Company. The colour of the squares shows the level of the risk of each combination of Likelihood and Severity:

- Green – low
- Yellow – Medium
- Red – High
- Bordeaux – Extreme

The Company has to determine the likelihood of any one scenario materialising, and the possible impact thereof. Taken together, likelihood and impact will lead to one's inherent risk. A Likelihood Scale refers to the potential of an ML/FT risks. Four levels of risk are shown in table below.

Table 2:Likelihood scale

Likelihood	Likelihood of ML/FT Risk
4 – Extreme	Can occur several times a year
3 – High	Can occur a few times a year – reasonable chance
2 – Medium	Can occur once a year – small chance
1 – Low	Can occur less than once a year – very unlikely

Source: Developed by author

An Impact Scale refers to the seriousness of the damage (or otherwise) that could occur should the event happen (and the risk, therefore, materialises). Four levels of risk are shown in table below.

Table 3:Impact scale

Consequence	Impact of ML/FT Risk
4 – Extreme	Severe loss or damage, heavy supervisory action – long-term effect
3 – High	Large loss or damage, supervisory action – medium-term effect
2 – Medium	Limited loss or damage, minor supervisory action – short-term effect
1 – Low	Negligible loss or damage, no supervisory action – no effect

Source: Developed by author

Each classification of the treats and vulnerabilities likelihood and Impact should be done as an expert evaluation, analysing specific of the Company KYC procedure and operations monitoring.

The final risk definition should be done, by the table below, where risk in the empty columns should be placed and calculated based on expert evaluation, mentioned above.

Table 4:Risk Calculation matrix

Ref. nr	Vulnerability	Ref. nr	Threat	Base Risk for threat	Likelihood for threat	Risk for Vulnerability	Risk for Vulnerability before assessment	Impact	Final pre-mitigation Risk	Risk name
1.1.	Failure of Customer KYC procedure	**2.1.**	Identity Fraud							Identity thief
1.1.	Failure of Customer KYC procedure	**2.2**	Fraudulent documents							Identity thief
1.1.	Failure of Customer KYC procedure	**2.3**	Business activity of the customer							Unknown business activity of the customer
1.1.	Failure of Customer KYC procedure	**2.4**	Geographical location							Unknown customer real location/address
1.1.	Failure of Customer KYC procedure	**2.5**	False/Incorrect personal data							Unidentified beneficiary
1.1.	Failure of Customer KYC procedure	**2.6**	Customer Criminal Record on ML/TF							Account opening to a criminal/terrorist
1.1.	Failure of Customer KYC procedure	**2.7**	Politically Exposed Person							Account opening to unidentified Politically Exposed Person
1.1.	Failure of Customer KYC procedure	**2.8**	Sanctions on the customer							Account opening to a sanctioned person
1.1.	Failure of Customer KYC procedure	**2.9**	Concealment of Beneficial Ownership							Unknown account beneficial owner
1.2		**2.1.**	Identity Fraud							Identity thief

	Compliance policies are not followed									
1.2	Compliance policies are not followed	**2.2**	Fraudulent documents							Identity thief
1.2	Compliance policies are not followed	**2.3**	Business activity of the customer							Unknown business activity of the customer
1.2	Compliance policies are not followed	**2.4**	Geographical location							Unknown customer real location/address
1.2	Compliance policies are not followed	**2.5**	False/Incorrect personal data							Unidentified beneficiary
1.2	Compliance policies are not followed	**2.6**	Customer Criminal Record on ML/TF							Account opening to a criminal/terrorist
1.2	Compliance policies are not followed	**2.7**	Politically Exposed Person							Account opening to unidentified Politically Exposed Person
1.2	Compliance policies are not followed	**2.8**	Sanctions on the customer							Account opening to a sanctioned person
1.2	Compliance policies are not followed	**2.9**	Concealment of Beneficial Ownership							Unknown account beneficial owner
1.3	Insufficient Customer Risk score	**2.1.**	Identity Fraud							Identity thief
1.3	Insufficient Customer Risk score	**2.2**	Fraudulent documents							Identity thief
1.3	Insufficient Customer Risk score	**2.3**	Business activity of the customer							Unknown business activity of the customer
1.3	Insufficient Customer Risk score	**2.4**	Geographical location							Unknown customer real location/address
1.3	Insufficient Customer Risk score	**2.5**	False/Incorrect personal data							Unidentified beneficiary
1.3	Insufficient Customer Risk score	**2.6**	Customer Criminal Record on ML/TF							Account opening to a criminal/terrorist
1.3	Insufficient Customer Risk score	**2.7**	Politically Exposed Person							Account opening to unidentified Politically Exposed Person
1.3	Insufficient Customer Risk score	**2.8**	Sanctions on the customer							Account opening to a sanctioned person
1.3	Insufficient Customer Risk score	**2.9**	Concealment of Beneficial Ownership							Unknown account beneficial owner
1.4	Real location does not correspond to virtual location	**2.1.**	Identity Fraud							Identity thief
1.4	Real location does not correspond to virtual location	**2.2**	Fraudulent documents							Identity thief
1.4	Real location does not correspond to virtual location	**2.3**	Business activity of the customer							Unknown business activity of the customer

1.4	Real location does not correspond to virtual location	**2.4**	Geographical location							Account opening to a person from a sanctioned country
1.4	Real location does not correspond to virtual location	**2.5**	False/Incorrect personal data							Unidentified beneficiary
1.4	Real location does not correspond to virtual location	**2.6**	Customer Criminal Record on ML/TF							Account opening to a criminal/terrorist
1.4	Real location does not correspond to virtual location	**2.7**	Politically Exposed Person							Account opening to unidentified Politically Exposed Person
1.4	Real location does not correspond to virtual location	**2.8**	Sanctions on the customer							Account opening to a person from a sanctioned country
1.4	Real location does not correspond to virtual location	**2.9**	Concealment of Beneficial Ownership							Unknown account beneficial owner
1.5	Poor Compliance Officer training	**2.1.**	Identity Fraud							Identity thief
1.5	Poor Compliance Officer training	**2.2**	Fraudulent documents							Identity thief
1.5	Poor Compliance Officer training	**2.3**	Business activity of the customer							Unknown business activity of the customer
1.5	Poor Compliance Officer training	**2.4**	Geographical location							Unknown customer real location/address
1.5	Poor Compliance Officer training	**2.5**	False/Incorrect personal data							Unidentified beneficiary
1.5	Poor Compliance Officer training	**2.6**	Customer Criminal Record on ML/TF							Account opening to a criminal/terrorist
1.5	Poor Compliance Officer training	**2.7**	Politically Exposed Person							Account opening to unidentified Politically Exposed Person
1.5	Poor Compliance Officer training	**2.8**	Sanctions on the customer							Account opening to a sanctioned person
1.5	Poor Compliance Officer training	**2.9**	Concealment of Beneficial Ownership							Unknown account beneficial owner
1.6	Screening program not synchronise between the countries	**2.1.**	Identity Fraud							Identity thief
1.6	Screening program not synchronise between the countries	**2.2**	Fraudulent documents							Account opening to a criminal/terrorist
1.6	Screening program not synchronise between the countries	**2.3**	Business activity of the customer							Account opening to a person with a criminal business activity

1.6	Screening program not synchronise between the countries	**2.4**	Geographical location							Unknown customer real location/address
1.6	Screening program not synchronise between the countries	**2.5**	False/Incorrect personal data							Unidentified beneficiary
1.6	Screening program not synchronise between the countries	**2.6**	Customer Criminal Record on ML/TF							Account opening to a criminal/terrorist
1.6	Screening program not synchronise between the countries	**2.7**	Politically Exposed Person							Account opening to unidentified Politically Exposed Person related to corruption or bribery
1.6	Screening program not synchronise between the countries	**2.8**	Sanctions on the customer							Account opening to a sanctioned person
1.6	Screening program not synchronise between the countries	**2.9**	Concealment of Beneficial Ownership							Account opening to unknown person with a criminal record
1.7	Beneficiary has relevant link to a PEP	**2.1.**	Identity Fraud							Identity thief
1.7	Beneficiary has relevant link to a PEP	**2.2**	Fraudulent documents							Identity thief
1.7	Beneficiary has relevant link to a PEP	**2.3**	Business activity of the customer							Account opening to unidentified Politically Exposed Person related to corruption or bribery
1.7	Beneficiary has relevant link to a PEP	**2.4**	Geographical location							Unknown customer real location/address
1.7	Beneficiary has relevant link to a PEP	**2.5**	False/Incorrect personal data							Account opening to unidentified Politically Exposed Person related to corruption or bribery
1.7	Beneficiary has relevant link to a PEP	**2.6**	Customer Criminal Record on ML/TF							Account opening to unidentified Politically Exposed Person related to corruption or bribery
1.7	Beneficiary has relevant link to a PEP	**2.7**	Politically Exposed Person							Account opening to unidentified Politically Exposed Person
1.7	Beneficiary has relevant link to a PEP	**2.8**	Sanctions on the customer							Account opening to a sanctioned Politically Exposed Person related to

										corruption or bribery
1.7	Beneficiary has relevant link to a PEP	**2.9**	Concealment of Beneficial Ownership							Account opening to unidentified Politically Exposed Person
1.8	Failure of Sanction screening	**2.1.**	Identity Fraud							Identity thief
1.8	Failure of Sanction screening	**2.2**	Fraudulent documents							Identity thief
1.8	Failure of Sanction screening	**2.3**	Business activity of the customer							Account opening to a person with sanctioned business activity
1.8	Failure of Sanction screening	**2.4**	Geographical location							Account opening to a person from a sanctioned country
1.8	Failure of Sanction screening	**2.5**	False/Incorrect personal data							Account opening to a sanctioned person
1.8	Failure of Sanction screening	**2.6**	Customer Criminal Record on ML/TF							Account opening to a sanctioned person
1.8	Failure of Sanction screening	**2.7**	Politically Exposed Person							Account opening to Politically Exposed person with sanctions
1.8	Failure of Sanction screening	**2.8**	Sanctions on the customer							Account opening to a sanctioned person
1.8	Failure of Sanction screening	**2.9**	Concealment of Beneficial Ownership							Account opening to unknown sanctioned person
1.9	Failure to perform an adverse media check	**2.1.**	Identity Fraud							Identity thief
1.9	Failure to perform an adverse media check	**2.2**	Fraudulent documents							Identity thief
1.9	Failure to perform an adverse media check	**2.3**	Business activity of the customer							Unknown business activity of the customer
1.9	Failure to perform an adverse media check	**2.4**	Geographical location							Unknown customer real location/address
1.9	Failure to perform an adverse media check	**2.5**	False/Incorrect personal data							Unidentified beneficiary
1.9	Failure to perform an adverse media check	**2.6**	Customer Criminal Record on ML/TF							Account opening to a criminal/terrorist
1.9	Failure to perform an adverse media check	**2.7**	Politically Exposed Person							Account opening to unidentified Politically Exposed Person
1.9	Failure to perform an adverse media check	**2.8**	Sanctions on the customer							Account opening to a sanctioned person
1.9	Failure to perform an adverse media check	**2.9**	Concealment of Beneficial Ownership							Unknown account beneficial owner

1.10	Compliance Officer non-observance	**2.1.**	Identity Fraud							Identity thief
1.10	Compliance Officer non-observance	**2.2**	Fraudulent documents							Identity thief
1.10	Compliance Officer non-observance	**2.3**	Business activity of the customer							Unknown business activity of the customer
1.10	Compliance Officer non-observance	**2.4**	Geographical location							Unknown customer real location/address
1.10	Compliance Officer non-observance	**2.5**	False/Incorrect personal data							Unidentified beneficiary
1.10	Compliance Officer non-observance	**2.6**	Customer Criminal Record on ML/TF							Account opening to a criminal/terrorist
1.10	Compliance Officer non-observance	**2.7**	Politically Exposed Person							Account opening to unidentified Politically Exposed Person
1.10	Compliance Officer non-observance	**2.8**	Sanctions on the customer							Account opening to a sanctioned person
1.10	Compliance Officer non-observance	**2.9**	Concealment of Beneficial Ownership							Unknown account beneficial owner
1. 11	Human factor	**2.1.**	Identity Fraud							Identity thief
1. 11	Human factor	**2.2**	Fraudulent documents							Identity thief
1. 11	Human factor	**2.3**	Business activity of the customer							Unknown business activity of the customer
1. 11	Human factor	**2.4**	Geographical location							Unknown customer real location/address
1. 11	Human factor	**2.5**	False/Incorrect personal data							Unidentified beneficiary
1. 11	Human factor	**2.6**	Customer Criminal Record on ML/TF							Account opening to a criminal/terrorist
1. 11	Human factor	**2.7**	Politically Exposed Person							Account opening to unidentified Politically Exposed Person
1. 11	Human factor	**2.8**	Sanctions on the customer							Account opening to a sanctioned person
1. 11	Human factor	**2.9**	Concealment of Beneficial Ownership							Unknown account beneficial owner

Source: Developed by author

Conclusion

In accordance to Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-Assets, and Amending Directive (EU) 2019/1937, 2020 all EEA

Countries will be forced to harmonized national legislation regarding cryptocurrency exchange companies' supervision and all such companies will become financial institutions. In a view of that fact, already today this sector of economy should use anti-money laundering approach, expandable with necessary adaptive characteristics, which in the future will allow transformation of crypto currency exchange companies into financial institutions.

Author developed list of threats and vulnerabilities may be easily adopted for any type of operations and services offered by financial institution in future and currently existing crypto currency exchange companies. Developed by author Risk calculation matrix may be used as template for AML risk assessment. In case if based on the Business model of assessed company, some vulnerabilities are admitted as non-existing – all rows containing such vulnerabilities may be removed from the Risk calculation matrix. As well, with the money laundering risk assessment, which will be formed by above mentioned companies, understanding on vulnerabilities of the company will allow more targeted selection of mitigation strategy.

References

- Amundrud, Ø., Aven, T., Flage, R., 2017. How the definition of security risk can be made compatible with safety definitions. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 231. https://doi.org/10.1177/1748006X17699145
- Cox, L., 2008. Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks. Risk analysis : an official publication of the Society for Risk Analysis 28, 1749–1761. https://doi.org/10.1111/j.1539-6924.2008.01142.x
- Europarlament, 2018. 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. Europarlament.
- FATF, 2021. Consolidated Processes and Procedures for Mutual Evaluations and Follow-Up .
- FIAU, 2021. Financial Intelligence Analysis Unit Implementing Procedures. FIAU, Valetta.
- Giudici, G., Milne, A., Vinogradov, D., 2020. Cryptocurrencies: market analysis and perspectives. Economia e Politica Industriale: Journal of Industrial and Business Economics 47, 1–18.
- Hacker, P., Thomale, C., 2018. Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law. European Company and Financial Law Review 15, 645–696. https://doi.org/10.1515/ecfr-2018-0021
- Hsieh, H.-C., Oppermann, J., 2021. Initial coin offerings and their initial returns. Asia Pacific Management Review 26, 1–10. https://doi.org/https://doi.org/10.1016/j.apmrv.2020.05.003
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, 2020. . THE EUROPEAN PARLIAMENT, Brussels.