REPORT

ON SECTORAL RISK ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING USING THE DIGITAL ASSET SECTOR IN THE AIFC

Approved by the resolution of the AFSA's Executive Body

June 04, 2024

Astana

Contents

1. GENERAL CHARACTERISTICS OF THE SECTOR 3

2. CHARACTERISTICS OF THREATS 12

1) Drug trafficking 12
2) Fraud 13
3) Tax evasion 13
4) Corruption 14
5) Cybercrime 15
6) Trading in the Darknet 15
7) Sanctions evasion 16
8) Gambling 16
9) Piracy 17
10) Financing of terrorism 17

3. CHARACTERISTICS OF VULNERABILITIES 19

1) Anonymity 19
2) Usability 19
3) Immutability of transactions 20
4) Security 20
5) Weak differentiation of global platforms from DASPs registered in the AIFC. 21

4. MEASURES TAKEN BY THE AIFC TO MITIGATE THE LEVEL OF THREATS AND VULNERABILITIES 22

1) Regulation 22
2) Registration and Licensing Regulations 23
3) AML/CFT regime (AFSA procedures) 24
4) AIFC measures to reduce vulnerability due to the anonymity of DAs and crypto transactions 28
5) AIFC measures to reduce security vulnerabilities 29

5. CONTINUOUS MONITORING OF ML/TF RISKS 31

6. FINAL ASSESSMENT OF THREATS, VULNERABILITIES AND RISK LEVEL 39

1. GENERAL CHARACTERISTICS OF THE SECTOR

The issuance and circulation of Digital Assets ("DA") is a relatively new trend in the financial markets, however it has already gained high popularity among users. The attractiveness of the DAs is based on the use of the advantages of special distributed ledger technology, such as, for example, reducing the role of intermediaries in transactions and automating transactions using smart contracts. At the same time, the DA market is still at the stage of its development, and the volume of trading in DAs is inferior to the volume of transactions in traditional financial instruments.

At the same time, over the past few years, the DA market has grown significantly. The use of technologies can significantly optimize business processes, speed up interaction with customers, market participants and regulators, as well as improve the quality and personalization of products and services provided to consumers. DAs have become increasingly used for cross-border transactions or in investments as a more convenient alternative to traditional instruments. Technological innovations and improvements lead to the development of the DA industry, simplifying access to financial services and technologies, increasing the speed of transactions.

In total, the trading volume of all DASPs licensed in the AIFC for 2023 amounted to US$ 320,729,732, with a total number of 52,913 clients onboarded by DASPs.

In comparison, at the end of the first quarter of 2024 alone, the trading volume of the DASPs was US$ 232,311,156. The total number of customers registered on the DASPs platforms in the first quarter of 2024 increased by more than 20,000 users and amounted to 74,096 people. Thus, the above data confirm the high growth rates of the DA market.

Due to technological features, the issuance and circulation of DAs are carried out directly on the blockchain[1]. At the same time, transactions between owners can be carried out in three ways:

A) Through intermediaries, which are specially created centralized platforms - for example, exchanges, participants in the traditional financial market, providers of digital asset services. The transfer of digital assets and funds is carried out using the exchange infrastructure (platform), in which the corresponding wallets (accounts) of users - parties to transactions are opened.

B) Without intermediaries, that is, directly between the parties to the transaction. The transfer of the DA is carried out on the blockchain, and payments mostly take place outside the information system through traditional bank transfers. With this approach, the parties of the transaction accept the possible risks of non-delivery of a token (digital asset) or money.

C) Without intermediaries using decentralized solutions (DeFi infrastructure). With this approach, the conclusion and execution of transactions, including payments, take place in the information system without the participation of an intermediary.

The issue of a DA provides the issuer and investors with a number of advantages, such as:

- The ability to fractionalize a security and issue multiple tokens of lower value reduces the threshold for retail investors participation.
- The ability to execute trades automatically according to an algorithm that is determined by a smart contract[2], which allows to reduce costs and the role of intermediaries.

[1] Blockchain is a technology (data structure and program code) of a distributed ledger network in which data is structured in the form of a chain (sequence) of cryptographically linked blocks of transactions. Each block contains an encrypted link to the previous one to ensure the immutability of the records.

[2] A smart contract is an algorithm (program code) that fixes the rights and obligations of the parties to the transaction, the terms of contractual relations, as well as their future automatic execution in a distributed ledger.

- Simplification of the issuance procedure helps to reduce costs for issuers and increases speed.

At the same time, the issue and circulation of a DA may be associated with restrictions and features of the technologies used:

- Operational compatibility. Thus, in order to avoid fragmentation of financial markets, it is necessary to ensure compatibility both between the various information systems in which digital assets are issued and with the centralized information systems of traditional financial market participants (e.g., exchanges, depositories, brokers, clearing and settlement organizations). At the same time, market integrity and compatibility of different information systems can be ensured, in particular by establishing appropriate regulatory requirements.
- As a rule, the reliability of DAs and the ability of their owners to exercise their rights directly depend on the quality of the issuer and the reliability of the real (underlying) asset that the token is backed by. Therefore, for the full functioning of the market of such DA, an appropriate regulatory framework is required, as well as business processes and infrastructure that ensure the connection between the token and the real asset (including the possibility of receiving cash flows associated with it (dividends, interest) and physical support (i.e., the presence of securities in the depository, precious metals in the vault, etc.).

Thus, while the use of DAs can benefit both issuers and investors, their use and circulation is associated with a number of risks of possible harm to consumers, risks of using financial services for criminal purposes and damaging the financial stability not only of a particular jurisdiction, but also of the region as a whole. Due to a number of features, DAs become vulnerable to their use by criminals for the purposes of money laundering and terrorist financing (ML/TF), as well as for the commission of other crimes.

The ability to conduct rapid cross-border transactions allows criminals not only to acquire, move and store assets digitally, often outside the regulated financial system, but also to conceal the sender and recipient of funds, and make it difficult for reporting persons to identify suspicious activity in a timely manner. These and other factors create an increased risk environment for fintech.

Pseudo-anonymity, lack of a central governing body (decentralization), cross-border nature of transactions, widespread and simplified access are factors that create an attractive environment for persons using such technologies and services for ML/TF purposes.

The possibility of using the DA for ML/TF purposes creates certain conditions for the organization of the activities of digital asset service providers (DASPs) in Kazakhstan.

A condition to operate as a DASP in Kazakhstan is to obtain a license from the Astana International Financial Centre (AIFC).

In accordance with the legislation of the AIFC, DASPs are companies or organizations that offer services related to digital assets, such as exchanges, wallet providers, payment services in relation to DAs.

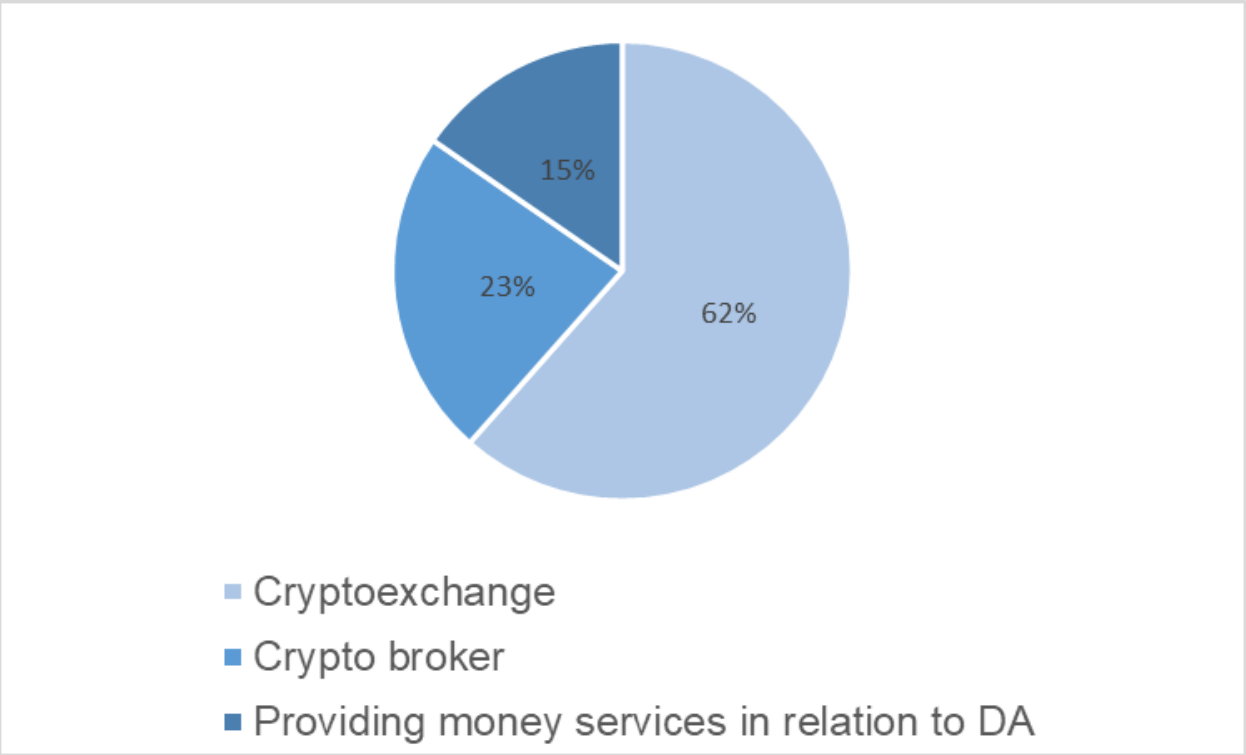
In the Q1 2024, 13 DASPs were registered in the regulatory sandbox of the AFSA, of which:

- 8 licenses for Operating a Digital Asset Trading Facility (cryptoexchange);
- 3 licenses for Dealing in Investments as an Agent (crypto broker);
- 2 licenses for the Providing Money Services in relation to Digital Assets (payment services with the DA).

It should be noted that 2 companies (Xignal&MT Ltd. and HWGC KZ Limited) out of 13 are inactive due to the suspension of the license.

Cryptoexchanges were the predominant activity among licensed DASPs at the end of the 1st quarter of 2024 in the digital asset sector of AIFC (see Fig. 1), which is 62% of all AIFC DASPs.

Figure 1. Breakdown of DASPs by type of activity



List of active DASPs:

№	DASP name	License name	License active since
1	Ataix Eurasia Ltd.	1) *AFSA-G-LA-2022-0001* - Providing Custody 2) *AFSA-G-LA-2022-0002* - Operating a Digital Asset Trading Facility	07-04-2022
2	BN KZ Technologies Limited	1) *AFSA-G-LA-2022-0008* - Providing Custody 2) *AFSA-G-LA-2022-0009* - Operating a Digital Asset Trading Facility	29-09-2022

3	Biteeu Eurasia Ltd.	1) *AFSA-G-LA-2022-0003* - Providing Custody 2) *AFSA-G-LA-2022-0004* - Operating a Digital Asset Trading Facility	03-05-2022
4	Top Line Limited	1) *AFSA-G-LA-2022-0010* - Providing Custody 2) *AFSA-G-LA-2022-0011* - Operating a Digital Asset Trading Facility	27-10-2022
5	Delta DA Ltd.	1) *AFSA-G-LA-2021-0018* - Providing Custody 2) *AFSA-G-LA-2021-0009* - Operating a Digital Asset Trading Facility	13-07-2021
6	Bigone Investment Ltd.	1) *AFSA-G-LA-2023-0008* - Providing Custody 2) *AFSA-G-LA-2023-0009* - Operating a Digital Asset Trading Facility	09-11-2023
7	Bybit Limited	1) *AFSA-G-LA-2023-0003* - Providing Custody 2) *AFSA-G-LA-2023-0004* - Operating a Digital Asset Trading Facility	07-06-2023
8	SkyBridge Digital Finance Ltd.	1) *AFSA-G-LA-2023-0006* -Dealing in Investments as Agent -Advising on Investments	18-10-2023

		-Arranging Deals in Investments -Dealing in Investments as Principal (as a matched principal) -Managing Investments -Managing a Collective Investment Scheme	
9	Paidax Limited	1) *AFSA-G-LA-2023-0007* -Dealing in Investments as Agent -Dealing in Investments as Principal (as a matched principal)	07-11-2023
10	Collect&Exchange	1) *AFSA-G-LA-2023-0002* -Providing Money Services in relation to Digital Assets	21-08-2023
11	Advanced Payment Solutions	1) *AFSA-G-LA-2021-0017* -Providing Money Services -Dealing in Investments as Agent -Arranging Deals in Investments	12-07-2021

Statistics on suspicious and threshold transactions of the AIFC DASPs in 2023

№	**DASP name**	**Suspicious Transaction Reports (STRs) and Transaction Threshold Reports (TTRs)**	**Number of reports**
1	Ataix Eurasia Ltd.	STR	3305
		TTR	0
2	BN KZ Technologies Limited	STR	31
		TTR	0
3	Top Line Limited	STR	2
		TTR	0
4	SkyBridge Digital Finance Ltd.	STR	0
		TTR	3

5	Advanced Payment Solutions Ltd.	STR	0
		TTR	235

Delta DA Ltd., Bigone Investment Ltd., Bybit Limited, and Paidax Limited, were the DASPs license holders in the AIFC in 2023, however did not carry out live operations due to the preparatory works. At the same time, 2 DASPs did not conduct transactions with DA due to suspended licenses: Xignal & MT Ltd., and HWGC KZ Limited. As a result, these entities did not send reports on suspicious and threshold transactions to the authorized body.

Biteeu Eurasia Ltd. had a low trading turnover in 2023. At the same time, for individual client transactions, their volume did not exceed the threshold level for the purposes of financial monitoring. In this regard, the company did not submit the relevant reports to the authorized body. A similar situation for individual client transactions was reported by Collect & Exchange.

SkyBridge Digital Finance Ltd. and Top Line Limited sent a small number of reports due to the start of operations in Q4 2023 and low volume.

Finally, for such DASPs as BN KZ Technologies Limited, Ataix Eurasia Ltd., Advanced Payment Solutions Ltd., the number of reports submitted to the authorized body is significantly higher due to the large volume of the customer base and transactions compared to other AIFC DASPs.

In addition, an analysis of suspicious transaction reports sent by all DASPs shows that the prevailing number of reports (approx. 98%) relate to transactions related to customer funds received from a digital asset exchange or are sent to a digital asset exchange that is not registered in the country or territory where this client or exchange[3] is located. Other suspicious transaction reports were made in connection with the refusal to

[3] This wording of the suspicious transaction sign was used in the previous version of Order No13 of the AFM of the Republic of Kazakhstan "On Approval of the Rules for Submission by Financial Monitoring Entities of Data and Information on Transactions Subject to Financial Monitoring and Signs of Determining a Suspicious Transaction"

establish a business relationship; as part of the termination of the business relationship; refusal to make a transaction; transactions to make a large initial deposit when establishing new relations with persons engaged in the issuance of digital assets, organizing trading in them, as well as the provision of services for the exchange of digital assets for money, valuables and other property (VASP), the amount of which does not correspond to the client's profile and/or the withdrawal of assets without additional transactions, or as soon as possible after their appearance on the account; transactions with digital asset addresses or bank cards associated with known fraud scams, extortion or the use of ransomware, with darknet marketplaces and other illegal websites, with addresses under sanctions.

In general, the number of reports of threshold and suspicious transactions remains insignificant due to the special regime of the AIFC regulatory sandbox, which (1) limits the set of transactions of clients with DAs, and (2) sets low limits on the number of transactions of retail clients at the level of US$1000.

2. CHARACTERISTICS OF THREATS

As part of the sectoral risk assessment of ML/TF, a study was carried out on the presence of threats of involvement of entities in the DA sector in criminal activities using ML/TF typologies.

Particular attention to the DA sector is caused by the steady growth of platform users – clients of DASPs registered in the AIFC. Thus, for the period from December 2022 to December 2023, the number of clients of the AIFC DA exchanges increased by more than 8 times.

Considering the characteristics of DA, the following threats associated with the use of DA and DASPs for potential ML/TF purposes have been identified:

1. The threat is posed by persons or groups of persons who have committed predicate crimes that generate income, and as a result they use DA and DASPs for the purpose of money laundering.
2. The threat is posed by persons who directly use DA and DASPs for the purpose of committing crimes and further ML/TF.

It is necessary to highlight following types of crimes: drug trafficking, fraud, tax evasion, corruption and various types of cybercrime (theft, hacking, extortion, ransomware).

1) Drug trafficking

According to global practice, the use of DAs in drug trafficking is widespread. The reason for this is mainly the ability to sell drugs without intermediaries, which leads to maximizing profits and simplifying the process of drug distribution; the ability to sell drugs outside territorial restrictions: a seller from anywhere in the world has access to any buyer; the difficulty in tracking transactions of some types of DAs. Proceeds derived from drug trafficking can be laundered through the DASPs, through the conversion of the received fiat funds into DAs and the subsequent exchange of DAs back into fiat.

In addition, DAs are also used as a medium of exchange in the drug trade between sellers and buyers.

There are numerous darknet markets connecting buyers and sellers of drugs, where trade is carried out exclusively through the exchange of DA.

2) Fraud

Fraud is a significant threat in the field of using the DA for criminal purposes. Given the specifics of the AIFC, the biggest threat are investment fraud, phishing fraud, fake websites or applications, pump and dump schemes, fake recommendations, including using AI, and initial coin offering (ICO) fraud.

The rapid growth in the value of certain types of DAs makes it possible for criminals to manipulate information in order to attract more consumers, and then appropriate funds. With such schemes, as a rule, criminals promise potential victims high profitability. Taking advantage of citizens' poor understanding of digital products, criminals lure victims, increasing the growth in the number of deceived people on the one hand and securing the volume of criminal proceeds obtained on the other.

3) Tax evasion

Based on documented typologies and trends, including the Financial Action Task Force (FATF) Red Flag Indicators, there is evidence that DAs and DASPs are used for tax evasion worldwide.

One of the options for evading tax control is to use the DA as a means of payment and accumulate profits without converting them into fiat money. In this case, the DA is not displayed for accounting in the bank accounts of organizations or citizens. Even in the context of a ban on such activities, if these transactions are not public, are not multiple and are not advertised (for example, as payment for goods in an online store), then attracting attention to them from regulatory authorities is minimized. Thus, it is quite difficult to

find out about the fact of tax evasion without the taxpayer voluntarily reporting such information in his declaration.

Also, tax evasion with cryptoasset may take place as a result of the change of the value of some types of DAs within short period of time. Therefore, it will be difficult to accurately determine the value of DA at the time of the tax crime. Thus, in relation to the materials of tax audits, the relevant examinations will always be required. Thus, it is quite difficult for law enforcement agencies to prove that the actions of the evader were intentional or intentional.

In addition, this part of the threats also includes the possibility of saving unaccounted income in the form of the DA (unaccounted capital gains, mining of digital assets, etc.). Also, businesses can fraudulently reduce their reported revenue by using DAs, for example, as part of false invoicing schemes.

These circumstances in their entirety inevitably lead to a decrease in the effectiveness of the fight against tax evasion.

4) Corruption

DA can be the subject of corruption crimes. The DA ecosystem is potentially attractive to corrupt PEPs. Officials can use DAs both to commit acts of corruption and to launder criminal proceeds related to state corruption. Another possibility for PEPs to use DAs is to receive a bribe in the form of the DA.

Corrupt PEPs can illegaly obtain funds from state budgets or procurement contracts and convert them into DAs through DASPs, which facilitates the movement of funds across borders and avoids traditional financial controls. Once converted, illicit funds can be mixed or legalized through services that hide transaction history and make it difficult to trace the source of funds

(layering). Such funds can then be used to invest in real estate or other assets (integration), as well as to continue corrupt activities.

5) Cybercrime

The technological features of DAs make them an attractive target for cybercriminals.

Cybercrime encompasses a range of criminal activities such as hacking, theft, ransom, extortion, and denial of service of attack, which can generate huge illicit profits that are nearly impossible to trace and recover. Cybercriminals may remain anonymous/pseudonymous, which hinders the effective investigation of both the predicate offence and related money laundering.

The use of 'hot' crypto wallets, which, despite their inherent insecurity, are still used by many custodians to provide an easily accessible liquidity pool, only increases the risk of cybercrime.

6) Trading in the Darknet

DAs can be used to trade on the Darknet and gain access to illegal content, such as CSAM (Child Sexual Exploitation Material). Thus, according to the Chainalysis report, the role of DAs in the sale of CSAM materials has increased significantly. According to the same report, even those DA exchanges that conduct proper KYC procedures face the risk of being affected by CSAM trading.

It is widely known that there are digital spaces where CSAM can be bought and sold by DAs, and there are cases when law enforcement agencies of foreign jurisdictions have closed such CSAM platforms as "Welcome to Video", which accept DAs as payment.

The more anonymity a particular type of DA provides, the greater the chance that CSAM providers will use DAs. For example, CSAM providers can benefit

from the use of Monero. Monero is the most popular of the so-called "privacy coins" whose blockchain uses unique privacy-enhancing features that make it harder to track the movement of funds or identify their original source.

7) Sanctions evasion

Another potential threat is the use of DAs as a tool to circumvent sanctions. Commercial banks often play a key role in sanctions enforcement, as they trace the sources of funds and check whether individuals or companies are on sanctions lists. In this regard, individuals and legal entities under sanctions can use DAs to make international payments without the participation of the bank as an intermediary.

8) Gambling

The threat of the use of DAs in the gambling industry, including the use of illegal casinos and bookmakers for ML, is relevant. One of the ways to use gambling for ML-TF purposes by using DAs is to convert illegal funds into the DAs. By depositing illegal funds on gambling platforms that accept DAs, people can effectively launder money by betting, winning or losing, and then cashing out their winnings in the form of pure DA. This process creates a layer of disguising that can hide the illegal origin of the funds. Terrorist organizations can use online gambling platforms to raise funds for their operations or to transfer funds between individuals and groups without attracting the attention of the authorities.

In addition, the emergence of decentralized finance (DeFi) platforms has opened up new opportunities for money laundering through gambling. DeFi platforms allow users to access financial services such as lending, borrowing, and trading without resorting to intermediaries. While DeFi provides greater financial inclusion and autonomy, it also poses challenges in terms of regulatory oversight and compliance. Prohibited entities can use decentralized exchanges and lending protocols to launder money by

converting illicit funds into DAs, participating in crypto gambling, and then withdrawing their "net" winnings through decentralized liquidity pools.

9) Piracy

DAs and related technologies are attractive to Internet pirates and are used by them to make a profit by illegally copying, hacking and/or distributing video and audio content, literary works, software and other types of information products.

One of the ways piracy can contribute to money laundering through the use of DAs is the sale of pirated content on online platforms that accept the DAs as payment. Such marketplaces operate on the Darknet or other anonymous platforms, allowing sellers to post ads and sell pirated content to buyers around the world anonymously. By accepting DAs such as Monero as payment, sellers can hide the source and destination of funds, making it difficult for law enforcement to track and stop these illegal transactions.

10) Financing of terrorism

One of the ways terrorists finance their activities using DAs is to collect donations from supporters around the world. Cryptoassets wallets can be created and publicly distributed, allowing people to anonymously deposit funds to support terrorist causes without fear of detection. These donations can be used to finance a variety of activities, including recruitment, training, dissemination of propaganda, and the purchase of weapons and materials.

In addition, terrorist organizations can use crypto exchanges to convert fiat currency into DA, which makes it easier to move funds across borders and evade traditional financial control measures. By depositing fiat currency into a cryptoexchange, terrorists can purchase cryptoassets such as Bitcoin, Ethereum, or Monero, which can then be transferred to other wallets or converted back to fiat currency in a variety of ways. The decentralized and global nature of cryptoassets makes it difficult for authorities to track and

disrupt these illicit financial transactions, allowing terrorists to move funds with relative impunity.

Example.

A citizen of the Republic of Kazakhstan financed the international terrorist organization ISIS operating in Syria by transferring Bitcoin to the crypto wallet of a citizen of Tajikistan, a member of the terrorist organization.

The financing was made with the assistance of another citizen of the Republic of Kazakhstan, who was engaged in illegal business activities expressed in the conversion and sale of Bitcoin on a cryptoexchange.

Law enforcement agencies revealed the facts of illegal activities and subsequently a pre-trial investigation was launched against both persons.

3. CHARACTERISTICS OF VULNERABILITIES

The existence of the above-mentioned threats in the DA sector became possible due to the presence of a number of vulnerabilities specific to DAs and special systems associated with DAs.

For the purposes of this report, vulnerabilities refer to properties inherent in the DA sector that make the sector available for illegal use for ML/TF purposes.

Among the main vulnerabilities are anonymity, ease of use, irreversibility of transactions and vulnerabilities associated with the presence of weaknesses in the network and systems of DAs and DASPs.

1) Anonymity

Anonymity refers to a vulnerability related to the anonymous nature of transactions, which attracts the attention of criminals aiming to achieve their ML/TF goals.

This risk is relevant in cases where identity cannot be established if the user has not passed the KYC procedure or has passed it using forged documents.

Different DAs have varying levels of anonymity, and it is most likely that criminals will prefer the DA with a higher level of anonymity to achieve ML/TF goals.

2) Usability

Usability reflects the transactional or exchange liquidity of the DA, its relative exchange rate stability, and the necessary technical knowledge to use it.

A higher degree of usability increases the susceptibility of DA to crimes related to ML/TF. On the contrary, the technological complexity of DAs is considered a significant limitation of the usability and, therefore, prohibits the wider use of DAs by potential criminals.

3) Immutability of transactions

In this context, immutability refers to the possibility that the user will not be able to reverse their operations. DAs that do not have the function of transaction reversibility become the most attractive for criminals to achieve their ML/TF goals.

The irreversibility of transactions provides significant advantages to criminals. In traditional financial instruments such as credit cards, the user or bank can reverse a transaction if it is fraudulent. In many DAs, transactions are irreversible, so even if fraud is detected at an early stage, the funds cannot be automatically returned. This leads to the problem of returning assets that have become the subject of criminal acts.

4) Security

The security issues of DA/DASP systems depend on the existence of gaps and weaknesses on the DA's blockchain and DASP systems. In addition, much depends on the behavior of the user.

Example.

On a cryptoexchange licensed in the AIFC, the client provided a scanned bank statement as proof of annual income. When checking the accuracy of the data provided, inconsistencies were identified. In particular, in the column "Transaction amount" in the line "Receipt to the account of an individual entrepreneur" the amount of 1,258,000 tenge was indicated, while in the column "Receipt in the currency of the account" for the same entry there was 258,270 tenge. Such a discrepancy indicates a deliberate increase in the funds received, presumably to increase the trading limit on the cryptoexchange platform. Such behavior is in line with the classification set out in the AIFC Participant's internal policy as "Provision by the client of forged documents or alteration of photographs and/or identification documents during the registration process". The cryptoexchange decided

to terminate the business relationship with this client, due to the increased risk posed by such customers.

5) Weak differentiation of global platforms from DASPs registered in the AIFC.

The availability of the ability to register on the global platform, bypassing the existing rules and regulations for DASPs on the territory of the AIFC, reduces the effectiveness of the current regime applicable to DASPs licensed in the AIFC.

4. MEASURES TAKEN BY THE AIFC TO MITIGATE THE LEVEL OF THREATS AND VULNERABILITIES.

When using DAs to achieve ML/TF goals or commit predicate crimes, potential criminals are guided by the presence of the vulnerabilities identified above. Accordingly, measures aimed at reducing the level and number of vulnerabilities inevitably affect the conditions for the formation of potential threats and have a positive effect on reducing the level of these threats.

Regular analysis of environmental risk and monitoring of the DA sector allows the AIFC to apply measures to reduce the level of ML/TF risk. These special procedures, measures and controls relate to the activities of registered and licensed DASPs in the AIFC.

1) Regulation

As part of the creation of a licensing regime for the activities of DASPs and further supervision and control of their business by the AIFC, innovative legal regulation of digital assets has been developed, implemented and applied.

The regulation covers such areas as: the operation of DASPs licensed in the AIFC; activities of the DASPs licensed in the AIFC for the storage and administration of DAs; activities of DASPs licensed in the AIFC to provide investment services in the field of digital assets. It should be noted that the regulatory regime of the AIFC excludes cash turnover in the DA sector.

Below is the regulatory framework governing the authorization of persons and entities engaged in the DA sector, as well as certain requirements for doing business with DAs, including mandatory AML/CFT requirements.

The AIFC Financial Services Framework Regulations (FSFR) No. 18 dated 20 December 2017 sets out the legal framework and general requirements for the regulation of all financial services in the AIFC.

More detailed requirements in relation to companies in the AIFC are set out in the following acts:

- **General Rules (GEN)** No. FR0001 dated 17 October 2017 **-** contains general requirements for company licensing, provisions on company obligations and detailed supplements to the FSFR.
- **Anti-Money Laundering and Counter-Terrorist Financing and Sanctions Rules (AML Rules)** sets out the requirements for the AML/CFT regime.
- Requirements for the AML/CFT Internal Control Rules
- Requirements for CDD when establishing relationships remotely
- Practical Guidance for Organizing an AML/CFT System
- **Conduct of Business Rules (COB)** – contains provisions on the principles of working with clients, counterparties and other participants of the financial market.
- **FINTECH Rules** – contains provisions for conducting activities in the regulatory sandbox of the AFSA, in which the participant, after registering and obtaining a license, tests new financial technologies or business models in a favorable regulatory environment under the supervision of the AFSA.
- **The AIFC Rules on Digital Asset Activities** establish the requirements and procedure for cryptoexchanges when working with DAs.

2) Registration and Licensing Regulations

In addition to the existing legal regulation, the requirement to obtain registration and an appropriate license from the AFSA in order to legally act as a DASP is a separate effective threat mitigation measure. The legal regulation of the AIFC establishes administrative and civil sanctions for conducting activities without registration and obtaining a license.

In addition to licensing procedures, the AFSA carries out activities to identify unlicensed DASPs. As of November 2023, the AFSA sent 543 requests to

state authorities to block the websites of identified unlicensed cryptoexchanges.

3) AML/CFT regime (AFSA procedures)

The AIFC AML/CFT regime is a risk-based supervisory and regulatory model based on the FATF Guidance and Recommendations.

The AFSA has implemented all three lines of defense:

1. At the stage of registration and licensing of companies, the disclosure of the ownership structure and the establishment of the ultimate beneficial ownership are ensured, checks are carried out for the professional compliance and suitability of both owners and key managers, as well as mandatory due diligence of companies and their owners; (Section 3, Chapters 1-2 (FSFR); Part 1, Clauses 1.1.4 and 1.1.5. (in relation to regulated entities) and Part 1.2., Clause 1.2.3. and 1.2.4. (in relation to authorized market institutions) of the General Rules. There is also a due diligence procedure for a potential Participant at the application stage (Section 6 of the General Rules), prior to registration.

1-1. After completing the registration and licensing stages, companies are assessed and assigned ratings based on risk levels and are assigned the appropriate Risk Mitigation Program. Compliance with all the requirements and recommendations of this Program is a prerequisite for starting activities on the AIFC platform; (as per clauses 5.5.3, 5.8. of the Procedures for the Supervision of the Fintech Lab of the AFSA dated April 23, 2020).

1-2. During the regulation and supervision stage, ongoing monitoring of companies' activities is conducted through reporting (remote supervision), scheduled and unscheduled on-site inspections, as well as "thematic" inspections focused on specific areas of activity. One of the primary supervisory priorities is to mitigate AML/CFT risks (as outlined in clause 3.3 of the Fintech Lab Supervision Procedures)

2. As part of the second line of defense, the AML/CFT Department of the AFSA provides additional expertise, support and monitoring, coordination of

units at any stage, focusing on ML/TF risk management issues, and also acts as a coordinator for interaction with the authorized body for financial monitoring. At this stage, enhanced due diligence measures are applied for companies and their beneficiaries, "thematic" audits of companies are carried out, monitoring, as well as identifying typologies of ML/TF schemes. The AML/CFT Department of the AFSA, as part of raising awareness of ML/TF risks, conducts regular training for employees of the AFSA, including mandatory knowledge testing, and also conducts information meetings with the AIFC DASPs;

2-1. Also, the relevant expertise in the investigation is provided by the Financial Investigation Department of the AFSA, which interacts with law enforcement agencies and courts;

3. As part of the third line of defense, the Internal Audit of the AFSA provides independent and objective assurances and recommendations regarding the adequacy and effectiveness of corporate governance and risk management of the AFSA.

Thus, the existing model of the risk-based approach adopted by the AIFC Committee allows supervisory units to systematically assess companies from the point of view of risks, as well as to constantly monitor and identify ML/TF risks.

As part of the prevention of the use of the AIFC platform by DASPs for ML/TF purposes and other illegal activities, they are required to complete the due diligence procedure of a potential DASP at the stage of applying for a license; to verify the availability of AML/CFT rules and instructions adopted by DASP management; requirement for DASP at the stage of obtaining a license to appoint a responsible AML/CFT officer; mandatory confirmation of the absence of a criminal record and the presence of relevant work experience or knowledge in the field of AML/CFT, conducting an interview with the candidate; requiring Participants to monitor, revise and update AML/CFT policies and procedures; the requirement to disclose the ownership structure

and the ultimate beneficiary of the applicant; mandatory verification of the applicant's managers and owners against the "black" lists of World-check in order to identify persons involved in criminal activities.

Example.

The AFSA rejected the application of Person A for admission as the ultimate beneficiary of a company registered in the AIFC. Among the main reasons for refusal set out by the AFSA were: 1) deliberate concealment from the AFSA of the fact that Person A had a different name and surname; 2) the applicant was the chairman of a large foreign company, the license of which was revoked by a foreign regulator due to repeated AML/CFT violations, which was reported to the AFSA by a foreign regulator.

Person A appealed to the AIFC Court against the decision of the AFSA. Nevertheless, the AIFC Court found sufficient reasons for refusing to issue a license and rejected the applicant's appeal.

The AIFC Court's agreement with the decision of the AFSA confirms:

1) the effectiveness of the authorization procedures of the AFSA. The audit revealed the facts of name change and concealment of information about the revocation of the license by another jurisdiction due to AML/CFT. Accordingly, the regulatory requirements of the AFSA made it possible to protect the territory of the AIFC from an unscrupulous participant;
2) the effectiveness of the dialogue between regulators, within the framework of which a successful exchange of confidential information took place.

Along with ensuring the effectiveness of the three lines of defense, the AFSA is constantly working to interact with the AIFC Participants in terms of maintaining their level of awareness of current AML/CFT trends and typologies. In addition, the AFSA conducts information sessions to explain the AIFC requirements for the development and implementation of AML/CFT

measures. Training events are carried out both by the AIFC Committee itself and with the involvement of international experts. As of April 1, 2024, 15 seminars, trainings and round tables have been held for DASPs alone (2021 - 2; 2022 - 4; 2023 - 7; 2024 - 2), including with the participation of experts from IMF, UNODC, RUSI, USA Embassy, UK Embassy, EAG, ITMCFM.

3.1) AML/CFT Regime (Requirements for Participants)

In order to prevent the use of DASPs by criminals in relation to DASPs, the AIFC AML/CFT Rules (AIFC AML/CFT Rules) establish the following AML/CFT requirements:

- Application of AML/CFT requirements to Authorised Firms (clauses 1.2 and 2.1 of the AIFC AML/CFT Rules)
- Application of the Risk-Based Approach, which includes an assessment of the risks of the business of the AIFC Participant and its clients (Sections 4 and 5 of the AIFC AML/CFT Rules);
- Customer Identification and Verification, which includes the identification of the Ultimate Beneficial Owner, PEP and sources of funds (Section 6 of the AIFC AML/CFT Rules);
- Organizing and conducting Customer Due Diligence, which includes enhanced and simplified CDD measures (Sections 6-8 of the AML/CFT Rules);

According to the legal regulation of the AIFC, customer verification measures also include certain mechanisms for detecting illegal or criminal activities, including for other categories of predicate crimes - financing the proliferation of weapons of mass destruction, drug trafficking, fraud and others.

As part of additional verification measures, an AIFC participant, when conducting routine customer due diligence in accordance with Rule 6.5.1 of the AML/CFT Rules, is obliged to check its customers, their business and transactions for inclusion in the UN Security Council sanctions lists and

"black" lists of persons and organizations published by the authorized bodies of the Republic of Kazakhstan. The procedural details of the audit are established in accordance with the Requirements for the AIFC AML/CFT Rules of Internal Control (IRC) dated 15 May 2020. Thus, according to sub-paragraph 5 of paragraph 22 of the Requirements for AIFC RIC , a program for the identification of the client, his representative and beneficiary is established, which, among other things, includes a procedure for verifying these persons for their inclusion in the lists. The lists are used to check clients for their participation in terrorist and extremist activities and possible links with the financing of the proliferation of weapons of mass destruction (FPWMD) (the list of persons included in the lists is established in accordance with sub-paragraph 10) of paragraph 15 of the Requirements for the AIFC RIC).

4) AIFC measures to reduce vulnerability due to the anonymity of DAs and crypto transactions

The AIFC's measures to reduce vulnerability due to the anonymity of DAs and crypto transactions are: the requirement for DASPs to implement procedures for identifying senders and recipients of digital assets; the requirement to identify all bidders; monitoring the presence of crypto mixers and connections with dubious accounts; the requirement to implement tools and procedures for biometric identification of the client when establishing relationships remotely; the requirement for the crypto exchange to check the DA itself before admission to trading; obtaining the approval of the AFSA for the admission of the DA to trading; a requirement for the DASPs to know the typologies and schemes for the use of blockchain technology and digital assets for criminal purposes; the requirement to implement monitoring of customer transactions for signs of suspiciousness identified by the FATF.

Example.

At the stage of establishing relations with a potential client, a crypto exchange licensed in the AIFC established circumstances that did not allow the completion of the customer due diligence procedure (KYC/CDD). In particular, in the process of analyzing the information provided by the client for the purpose of identification and verification (ID&V), signs were found that give reason to believe that the documents and information provided by the applicant for identification purposes are unreliable (suspicious). Further analysis conducted by the MLRO of the crypto exchange also found a high level of risk in terms of the applicant's business goals. In connection with these circumstances, the applicant was denied the registration procedure on the crypto exchange platform. A report on the circumstances of the refusal was sent to the FIU.

Example.

The client of the crypto exchange licensed in the AIFC was identified as an PEP, with an exact match of the full name. Subsequently, a request was sent to the client in order to confirm its status as a PEP. The client did not respond to this request. Due to the lack of confirmation by the client of his status, on the basis of the client's unwillingness to provide or refusal to provide information and documents for the purposes of due diligence, taking into account the revealed facts, the client was denied the registration procedure on the crypto exchange platform.

5) AIFC measures to reduce security vulnerabilities

The AIFC's measures to mitigate security vulnerabilities include the following requirements: a requirement for the DASPs to have the appropriate software, analysis and approval at the authorization stage; the requirement for the presence of an information security specialist responsible for the security of

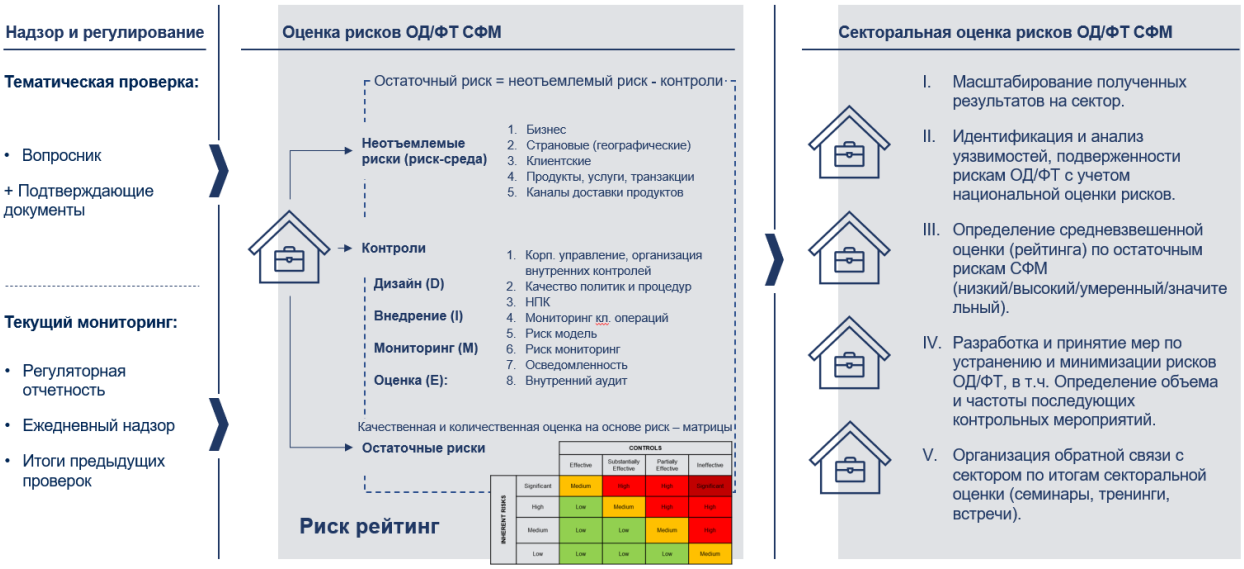
IT systems; the requirement to conduct penetration testing; constant monitoring of the activities of DASPs, the requirement for regular updating of tools and software; requirements for DASPs to implement cybersecurity policies and procedures; requirements for DASPs to implement systems and measures for the secure use of personal keys and an electronic wallet.

5. CONTINUOUS MONITORING OF ML/TF RISKS

In order to ensure adequate and timely supervisory regulatory measures, the AFSA monitors the level of risks of the Participants. When considering individual DASPs or specific products, services or activities related to DAs, the AFSA takes into account the level of risk associated with DASP products and services, business models, corporate governance systems, financial information, supply channels, characteristics of the customer base, geographical location, countries in which it operates, and the level of implementation of AML/CFT measures by DASPs, as well as the risks associated with specific products based on virtual assets that have the potential to mask transactions or reduce the ability of DASPs and supervisors to apply effective AML/CFT measures.

The AFSA also pays particular attention to the controls implemented by DASPs, including the quality of their risk management policies and procedures and the functioning of their internal controls. In addition, information on the degree of professional suitability and integrity of DASPs managers, AML/CFT officers, the availability of compliance services and internal audit is necessarily taken into account.

Figure 2. ML/TF risk assessment model at the individual and sectoral levels



For the purposes described above, the AFSA applies a risk assessment model based on the classic risk management formula ("Residual risk = inherent risks – existing controls"), where:

1) The first step is to determine the risk environment:

   Risk - environment = inherent risks of the organization.

   In this regard, the AFSA takes into account the fact that fintech companies and related services can stimulate financial innovation and increase efficiency. However, their features also open up new opportunities for money launderers, terrorist financiers and other criminals to launder criminal proceeds and finance their criminal activities, and also go beyond AML/CFT as a tool for predicate crimes.

   The model establishes five categories of risks for which the so-called initial vulnerability analysis is carried out or the immediate risk environment of DASP is determined: 1) business, 2) country (geographic), 3) customer, 4) products, services, transactions, 5) product delivery channels.

   In addition to risk categories, in order to more accurately determine the source of risk origin (root-cause), the Model contains a list of risk factors for each of the listed risk categories (i.e., factors contributing to the occurrence of a risk or threat).

   These risk categories are determined by the degree of "probability" and "impact" using a matrix. As a result, one of the following ratings is set: "Significant", "High", "Medium", "Low".

2) The next step is to determine the available controls:

   At the same time, the key aspect of the assessment of controls is the criteria according to which the degree of their effectiveness and their

quality are analyzed, namely: 1) Design, 2) Implementation, 3) Monitoring, 4) Evaluation.

Each of the eight elements of VASP internal controls 1) Corporate Governance, Organization of Internal Controls, 2) Quality of Policies and Procedures, 3) CDD, 4) Monitoring of Customer Transactions, 5) Risk Model, 6) Risk Monitoring, 7) Awareness, 8) Internal Audit) is evaluated against these four criteria and assigned a corresponding score. Then the number of points is measured as a percentage of the maximum value and one of the following ratings is displayed: "Effective", "Sufficiently effective", "Partially effective", "Ineffective".
After receiving the final value for each control, the arithmetic mean for all controls is calculated and the corresponding rating is assigned. At the same time, the analysis and assessment are carried out taking into account the expert analysis of quantitative and qualitative data/information collected for the purpose of risk assessment, as well as on the basis of available expert judgments.

In this way, the Model shows how the available VASP controls allow for the mitigation and management of the inherent risks or risk environment of VASP.

3) Ultimately, a qualitative and quantitative assessment of the VASP is obtained, which is transferred to the appropriate matrix to determine the residual risk rating.

   Residual ratings are classified as follows: Significant, High, Moderate, Low.

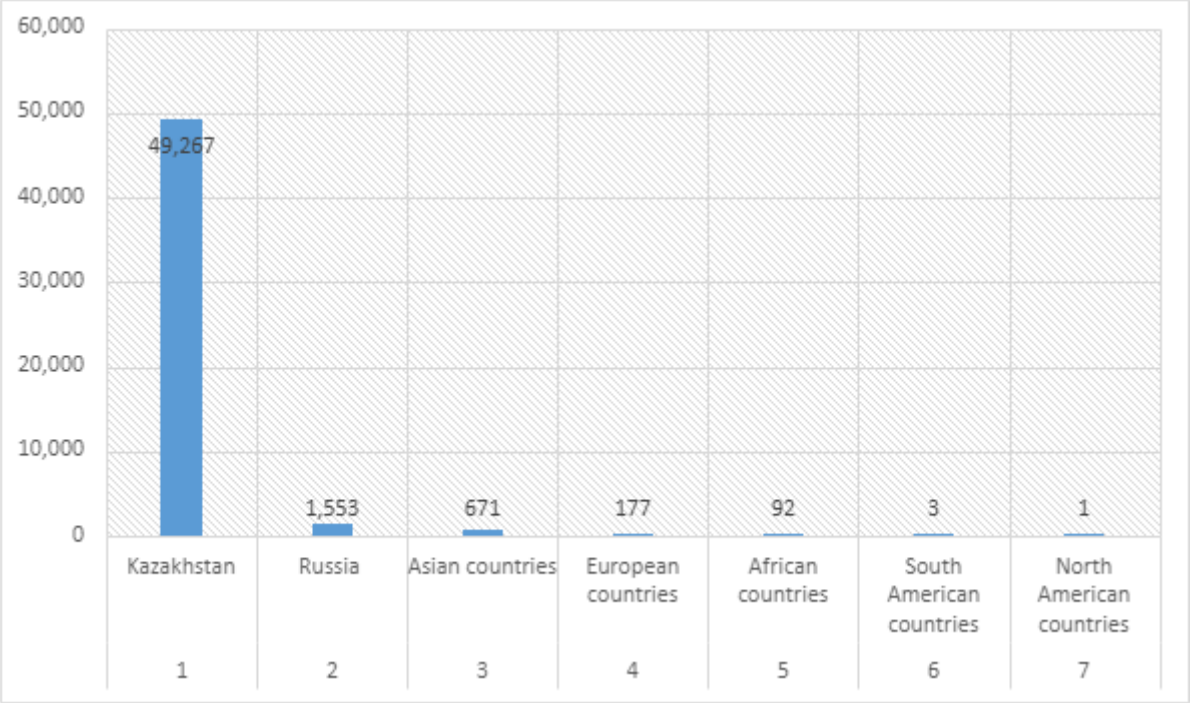
Summary of risks associated with DASPs clients and AIFC measures to mitigate them

In accordance with the requirements of the AIFC, each of the DASPs clients undergoes an assessment for the level of risk of DASP.

Clients are residents of the following countries/territories: Kazakhstan, Russia, Central Asian countries, Turkey, Nigeria, etc.

Mostly, clients are residents of Kazakhstan, while the share of non-residents is small. The following is a chart on the number of AIFC MACA clients, compiled on the basis of the annual reports of the AIFC Authority submitted to the AIFC Authority by the end of February.

Fig.3 Number of AIFC DASPs clients by country and region



Non-resident customers from the following countries may pose an increased AML/CFT risk:

Turkey (on the list of the FATF group under enhanced monitoring),

South Africa (on the list of the FATF group under enhanced monitoring),

UAE (until 24 February 2024 were on the list of countries with enhanced monitoring).

Example.

A user of a crypto exchange licensed in the AIFC attempted to withdraw DAs to a wallet registered with a foreign DASP located in a jurisdiction included in the sanction lists. Further investigation established that the user used a wallet opened on a crypto exchange licensed in the AIFC as an intermediate link in the chain to withdraw funds to a sanctioned address. The business relationship with the user has been terminated and the relevant information has been submitted to the FIU within the prescribed time limit.

It should be noted that the total number of clients from these countries with an increased risk of ML/TF/sanctions is extremely small.

Additionally, based on the risk assessment of clients, AIFC DASPs identified that 131 clients pose a high AML/CFT risk, accounting for just 0.0025% of the total client base.

Thus, we note that AIFC DASPs clients are mainly residents of Kazakhstan, the share of non-residents from countries with a high ML/TF risk is insignificant.

As part of the oversight, it was established that, in general, AIFC DASPs have implemented internal control measures. Namely, they developed and approved the RIC, appointed persons responsible for AML/CFT risks, organized an internal control system within organizations, and established interaction between departments and functions. RIC are reviewed by the AFSA when applying for a license. In the future, the DASPs update the policies taking into account changes in the legislation of the AIFC and the AML/CFT Law of the Republic of Kazakhstan, or as a result of regular business risk assessments. At the end of the year, when submitting

AML/CFT reports, DASPs provide up-to-date RIC and other policies and procedures.

In accordance with the AIFC AML/CFT Rules, DASPs conduct a business risk assessment of its activities, an assessment of the ML/TF risks of clients, a customer due diligence (CDD) procedure, and organizes the monitoring of transactions and customer activity. It is not allowed to conduct a simplified CDD when establishing a business relationship remotely.

The CDD includes measures to verify the identity of the client and its beneficial owner, obtain and understand information about the purpose and nature of the business relationship, understand the source of funds, the source of wealth, and conduct follow-up CDD.

Example.

A client of a crypto exchange licensed in the AIFC could not explain the source of funds for a large replenishment of the account. The client claimed that the specified amount represented the return of the debt. However, the client did not respond to a subsequent request for relevant documentary evidence. Given the significant amount of funds and the lack of the necessary documentary support, it was decided to terminate the business relationship with this client, and the relevant information was provided to the FIU in due time.

Brief description of product and service risks and AIFC measures to mitigate them

Product risks include the risks to which DASPs and customers are exposed in connection with the properties of the DAs used and the services provided.

DAs are products that are traded on crypto exchanges licensed by the AIFC. According to the requirements provided for in the AIFC, each DA that the

AIFC crypto exchange plans to trade must be approved by the AFSA. In total, at the end of 2023, 106 DAs were approved, 10 DAs were refused. There are no anonymous tokens among the approved DAs, as this parameter is a criterion for assessing compliance with the AIFC requirements. All DAs are issued on an open decentralized blockchain, which allows you to track transactions with these DAs, thereby significantly reducing the risk of using DAs traded on AIFC platforms for ML/TF purposes.

Currently, all AIFC crypto exchanges provide two types of services under licenses - spot trading and custodial services.

Compared to P2P trading, in spot trading, the crypto exchange customers pre-deposit fiat and DA, thereby the crypto exchange as an intermediary reduces the risk of fraud from customers.

Brief description of risks associated with operating activities and AIFC measures to mitigate them

Risks in the operational activities of DASPs include such parameters as: risks of the features and quality of the organization of internal control, the total number of employees, the outsourcing of part of the work (reliance on third parties), the procedure for the formation of the governing bodies of the organization, the procedure for the formation and appointment of certain officials in the organization, the interaction of functions, regular audit.

Existing examples in international practice demonstrate the importance of a responsible approach on the part of DASPs to the appointment of employees to key positions.

Example.

The case of the FTX crypto exchange is related to the bankruptcy of the company in November 2022 amid accusations that its owners appropriated and misused customer funds. As a result, within two weeks, the crypto

exchange, which had more than a million users and ranked third among cryptocurrency exchange services in terms of trading volume, suffered critical losses and declared bankruptcy.

On the part of AIFC as part of measures to mitigate these risks are:

1) a requirement for the organization of procedures for the appointment of authorized persons, such as: Executive Director, Compliance Officer, Financial Director, Responsible AML/CFT Officer (MLRO), CITO (Chief Information Technology Officer, Head of Information Technology Department).

Each of these functions is subject to special requirements of the AIFC and are checked by the AFSA for compliance with proper professional experience, knowledge and business reputation.

2) a requirement for the organization of the appointment of the board of directors of the company.

3) the requirement to have systems and controls in place to prevent conflicts of interest, insider trading, risk management systems, including, in addition to ML/TF, operational, reputational, legal, fraud and business continuity risks.

6. FINAL ASSESSMENT OF THREATS, VULNERABILITIES AND RISK LEVEL

The above measures and procedures are applied to each company authorized (licensed) in the AIFC – the subject of an individual risk assessment. The conclusion obtained as a result of the risk assessment for each company is scaled to the sector under consideration as a whole. As part of the sector assessment, the indicators reflected in the results of the previous National Risk Assessment of the Republic of Kazakhstan are taken into account. In doing so, a general analysis of vulnerabilities, exposure to ML/TF risks, and the threats (and potential risks) of possible use of companies for illegal purposes is carried out in qualitative terms. In quantitative terms, the weighted average assessment (rating) for the analysis of residual risks of VASP is determined based on the rating of each company. Thus, the individual characteristics of VASPs, the set of products and services provided by VASPs, their vulnerabilities and exposure to risk, as well as the quality and effectiveness of the controls implemented and the measures taken to minimize the risks of each company, have an impact on the level of risk in the sector as a whole**.**

According to the analysis of the current situation, the inherent risks, given the level of threats and the presence of vulnerabilities, in the issue of achieving ML/TF goals in the DA and DASP sector are **high.** DAs have a number of attractive properties that criminals can exploit for ML/TF purposes. The use of DAs is widely available, the use of DAs can be implemented through a number of means and/or at relatively low cost; this method is considered attractive and relatively safe, and does not require much planning, knowledge and/or technical experience.

The overall assessment of the level of vulnerabilities shows that, taking into account risk mitigation measures, the degree of vulnerability of the AIFC for involvement in ML schemes is assessed as low, and the risk is **medium**.

Further, the measures implemented to reduce the level of inherent risk, both from the point of view of the AIFC's preventive and supervisory procedures, and from the point of view of the Participants who comply with the AIFC requirements for their internal control systems, can significantly reduce the level of inherent risks. Thus, taking into account the risk mitigation measures, the degree of vulnerability of the AIFC for involvement in ML schemes is assessed as low, and the **residual risks of the AIFC Participants are assessed as medium**.

In this area of activity, the AIFC has deterrent measures and control measures that allow quite effectively preventing cases of money laundering and terrorist financing. Among the characteristics that reduce the risks of the DA sector in the AIFC, it is necessary to designate, in addition to the above, the following:

- the presence of constant supervision over the activities of companies;
- a limited number of products, services or transactions that facilitate very fast or anonymous transactions/operations;
- cash limitation;
- mainly secure and/or controlled supply chains are used;
- new technologies and/or new payment methods are effectively managed;
- a relatively small number of high-risk customers;
- there is a relatively small number of customers located in regions identified as high-risk.

Conclusion:

The scale of the AIFC DA sector, the presence and understanding of the identified threats and vulnerabilities of the area under consideration, taking into account the measures applied in accordance with international practice and FATF requirements, allow us to conclude that there is a high level of inherent risks, and **a medium level** of residual risks of using the DA sector for ML/TF purposes.

The results of the sectoral risk assessment are used by the AIFC as part of further supervisory activities. Namely, based on the findings obtained, measures are developed and taken to eliminate and minimize ML/TF risks, including the scope and frequency of subsequent control activities, strategies are developed to manage the identified risks, which provide for measures, including prevention, precaution, risks mitigation and an action plan to reduce them (Remediation Plan). Such measures include increasing the frequency of updating data on the number and quality of companies' customers, strengthening regulatory control, implementing risk-based supervision in the sector (desk based/on-site/thematic reviews or inspections) in order to increase the awareness and quality of the expert staff responsible for AML/CFT and compliance, holding regular meetings with supervised companies, conducting training and information events, and regularly providing participants with sectors of typological reports and signs of ML/TF, more active interaction with law enforcement agencies, etc.