REPORT ON THE SECTORAL RISK ASSESSMENT OF MONEY LAUNDERING, TERRORIST FINANCING, AND PROLIFERATION FINANCING IN THE DIGITAL ASSETS SECTOR AND DIGITAL ASSET SERVICE PROVIDERS IN THE AIFC (2025)

Approved by the decision of the Executive Body of AFSA
April 2026

Astana

AFSA

Content

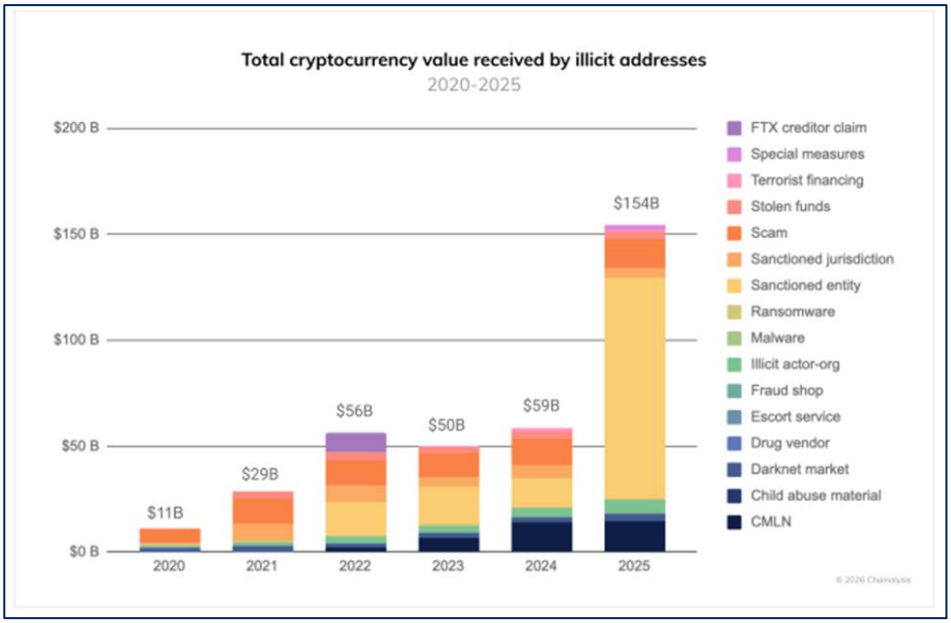
1. GENERAL CHARACTERISTICS OF THE SECTOR

The circulation of Digital Assets (DA) is gaining increasing popularity and is gradually becoming an integral part of financial markets. In many countries, there is a trend toward the legalisation of the activities of Digital Asset Service Providers (DASPs) and the circulation of DA through the development of regulatory frameworks, rather than imposing direct prohibitions. In addition, there is a growing trend toward the institutionalisation of DA usage, in which primarily traditional financial institutions invest in DA for investment purposes, or in which various forms of DA - so-called fiat-backed stablecoins[1] - are used for settlement, including cross-border payments.

Notably, the market capitalisation of the DA sector exceeded USD 4 trillion in 2025, while the market capitalisation of the stablecoin sector increased by 50%, reaching USD 305 billion. The daily transaction volume of stablecoins in 2025 reached USD 3.54 trillion, surpassing the transaction volume of one of the largest payment system operators, Visa, which amounted to USD 1.34 trillion.[2]

The volume of funds used for financial crimes, including for the purposes of money laundering, terrorist financing, and proliferation financing (ML/TF/PF), shows a growing trend. In 2024, the volume of DA received by illicit wallets amounted to USD 59 billion, while in 2025 it reached USD 154 billion. At the same time, the overall share of illicit transactions relative to the total volume of DA transactions remains insignificant, accounting for approximately 1% of total crypto transaction volume.[3]

Total digital asset value received by illicit addresses (*Fig. 1)*



At the same time, in 2025, the qualitative structure of the illicit use of DA changed significantly. According to data from the Financial Action Task Force (FATF) and industry analytics, fiat-backed stablecoins has become the dominant means of transferring illicit funds, combining high liquidity, low volatility, ease of cross-border transfers, and broad

[1]According to AIFC Glossary, Fiat stablecoin means A Digital Asset whose value purports to be determined by reference to a Fiat Currency.
[2] Full-Year 2025 & Themes for 2026, Binance Reserach *January 2026*
https://public.bnbstatic.com/static/files/research/full-year-2025-and-themes-for-2026.pdf
[3] Chainalysis report for 2025, The 2026 Crypto Crime Report.

accessibility across centralised and decentralised platforms. This indicates that the sector's risk profile is increasingly determined not solely by the "anonymity" of certain types of DA, but rather by the accessibility of stablecoin infrastructure, unhosted (non-custodial) wallets, cross-border services, and offshore digital asset service providers.

The attractiveness of DA is based on leveraging the advantages of blockchain technology (which primarily includes distributed ledger technologies and data storage in blocks), such as the reduced role of intermediaries in transactions, higher transaction speeds, irreversibility of transactions, the ability to transfer assets in a peer-to-peer (P2P) format (i.e., direct data exchange between two blockchain participants without intermediaries), anonymity of certain types of DA and the pseudo-anonymity of transactions on blockchain networks, as well as the automation of transactions through smart contracts.

Despite the significant growth of the global DA market in recent years, the sector remains in a stage of development. The application of blockchain technologies enables the optimisation of business processes, accelerates interaction with clients, market participants, and regulators, and enhances the quality and personalisation of products and services provided to consumers. DA are increasingly used for cross-border fund transfers and as a more convenient alternative to traditional instruments for investment purposes. Technological innovations and improvements continue to drive the development of the DA industry by simplifying access to financial services and technologies and increasing transaction speed.

Characteristics of the DA and DASP market in the AIFC

The active development of the DA and DASP market in the Astana International Financial Centre (AIFC) dates back to 2022, when the Astana Financial Services Authority (AFSA) launched a Pilot Project on cooperation between second-tier banks and AIFC-licensed cryptoexchanges (the Pilot Project). The Pilot Project was completed at the end of 2023. The experience gained from testing within the framework of the Pilot Project served as the basis for the development of a comprehensive regulatory regime for the DA and DASP sector in the AIFC.

In developing the regulatory framework for DA and DASP in the AIFC, consideration was given to the recommendations of the International Organization of Securities Commissions (IOSCO) and the FATF with respect to mitigating ML/TF/PF risks in the virtual asset and virtual asset service provider sector (for more details on the AIFC regulatory regime for the DA and DASP sector, see Section 4 of this Report).

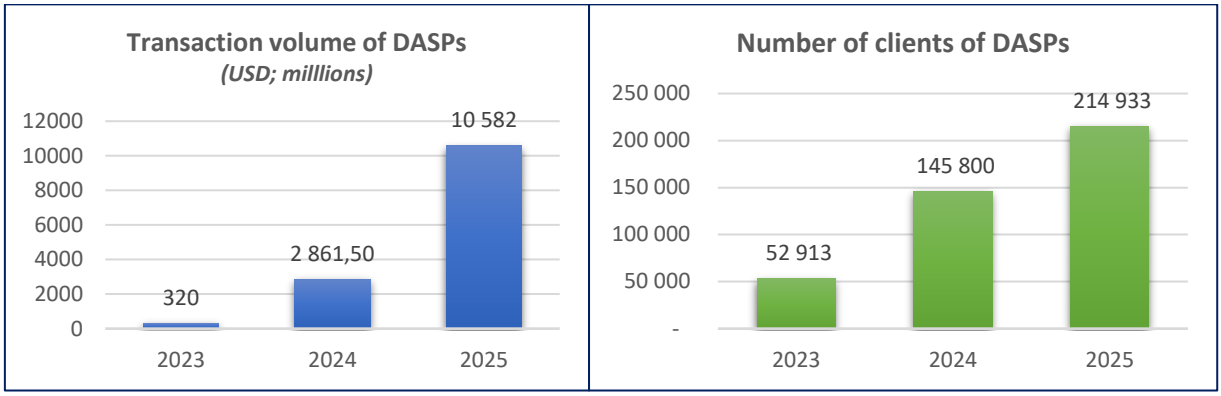
Transaction Volumes and Clients

The total transaction volume of all DASPs licensed in the AIFC amounted to more than USD 320,000,000 in 2023, with a total client base of 52,913 persons.

In 2024, the total transaction volume of all AIFC DASPs increased to more than USD 2,861,500,000, with a total client base exceeding 145,800 persons.

In 2025, the total transaction volume of all AIFC DASPs reached more than USD 10,582,000,000, with a total client base exceeding 214,933 persons.

Transaction volumes and number of clients of DASPs in 2023, 2024, and 2025 *(Fig. 2)*



The growth dynamics of transaction volumes and the number of users of DASPs licensed in the AIFC from 2023 to 2025 demonstrate an accelerated process of integrating DA market's participants in Kazakhstan into the legal trade of DAs.

Clients of DASPs primarily use their services for investment purposes. In addition, DAs are also used as a supplementary instrument for making payments, however, DAs are not recognised as legal tender within the AIFC.

DASP Market

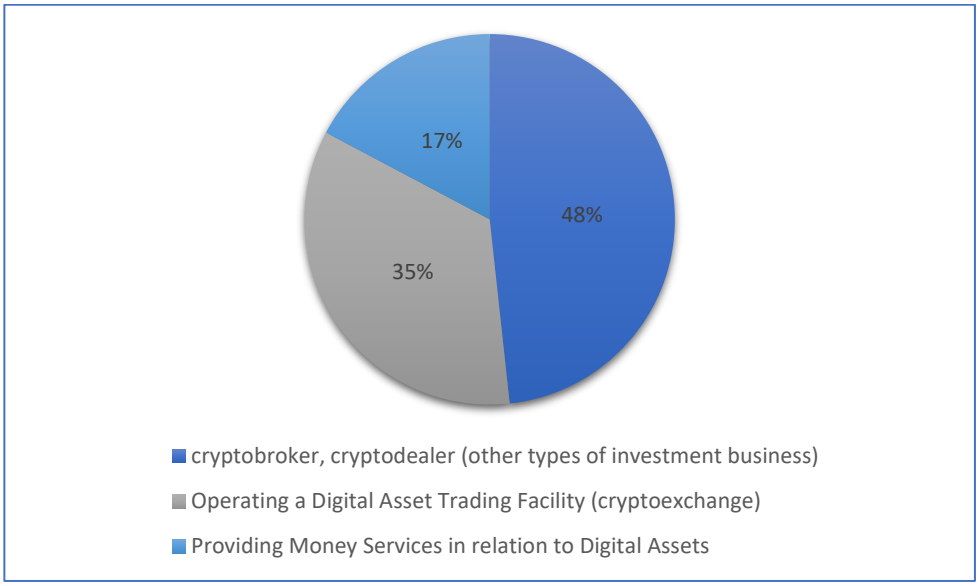
A prerequisite for conducting activities as a DASP within the territory of the AIFC is obtaining a licence issued by the AIFC.

In accordance with AIFC legislation, DASPs are companies or organisations that provide services related to DA, including: Operators of Digital Asset Trading Facilities (or cryptoexchanges), Providing Custody (or crypto custodians), Dealing in Investments as Agent and Principal (crypto-brokers and crypto-dealers), Providing Money Services in relation to Digital Assets, and other related services.

As of the end of 2025, a total of 29 DASPs were licensed in the AIFC, including:

- 14 licences for crypto-brokers, crypto-dealers (and other types of investment businesses);
- 10 licences for Operating Digital Asset Trading Facility (cryptoexchanges);
- 5 licences for Providing Money Services in relation to Digital Assets.

Main types of activities of DASPs in the AIFC (as of end of 2025) *(Fig. 3)*



According to Fig. 3 above, the prevailing type of activity among DASPs licensed in the AIFC was crypto-brokerage/crypto-dealing (48%). This was followed by cryptoexchanges (34%) and Providing Money Services in relation to Digital Assets (17%).

It should be noted that as of the end of 2025, 15 DASPs (out of 29 DASPs licensed in the AIFC) had not launched digital asset operations:

- 12 DASPs had not yet commenced digital asset operations and were conducting preparatory activities;
- 3 DASPs held licences with “pending approval” status due to ongoing preparatory work to fulfill licensing requirements prior to the commencement of operations.

Thus, the figures for 2024 and 2025 demonstrate a continuing, steady process of development of the DA’s and DASP’s market within the AIFC. The market formation process is also evidenced by the significant number of DASPs (15) that, as of the end of 2025, had not commenced the provision of digital asset services, despite the total number of DASPs licensed in the AIFC reaching 29.

In addition, when interpreting statistics on transaction volumes, number of clients, submitted suspicious transaction/activity reports (STR/SARs), and threshold transactions (TTRs), it is necessary to take into account that, given the large number of non-operational DASPs, some quantitative indicators reflect not the entire licenced perimeter of the sector but primarily the most active market participants (for STR/SAR/TTR statistics see below).

Use of Digital Assets for ML/TF/PF Purposes

Despite a number of advantages associated with the use of DAs for DASPs and their clients, their use and circulation are associated with a range of risks, including potential harm to consumers, risks of misuse of financial services for criminal purposes, and threats to financial stability - not only within a single jurisdiction but also at the regional level as a whole. Due to certain inherent characteristics, DAs are particularly vulnerable to exploitation by criminals for the purposes of money laundering, terrorist financing, and proliferation financing (ML/TF/PF), as well as for the commission of other crimes.

The ability to conduct fast cross-border transactions enables criminals not only to acquire, move, and store assets in digital form, often outside the regulated financial system, but also to obscure the identity of the sender and recipient of funds, thereby impeding the timely detection of suspicious activity by reporting entities. These and other features of modern financial technologies create an elevated ML/TF/PF risk environment.

In particular, pseudo-anonymity, the absence of a central governing authority (decentralisation), the cross-border nature of transactions, widespread and simplified access, and the irreversibility of transactions on blockchain networks are factors that create an attractive environment for individuals using such technologies and services for ML/TF/PF purposes.

The threats associated with the use of DAs for ML/TF/PF, arising from factors inherent in blockchain technology (or similar technologies), necessitated the establishment of a regulatory framework governing the operation of DASPs within the AIFC and Kazakhstan.

2. THREAT (RISK) ASSESSMENT

As part of the sectoral assessment of ML/TF/PF risks conducted in 2026, covering the period 2024 – 2025, an analysis was carried out to identify threats related to the potential involvement of entities within the assessed sector in criminal activities using ML/TF/PF typologies.

Increased attention to the DA sector is driven by the growth in the number of users of AIFC DASPs. In particular, between the end of 2024 and the end of 2025, the number of clients of DASPs licenced in the AIFC increased by more than 1.5 times.

Taking into account the specific characteristics of DAs, the following threats associated with the use of DAs and DASPs in the context of potential ML/TF/PF purposes were identified and assessed:

- Threat posed by individuals or groups that committed predicate offenses generating criminal proceeds and subsequently **use DAs and DASPs for the purpose of money laundering;**
- Threat of **terrorist financing** through the use of DAs and DASPs;
- Threat of **proliferation financing** through the use of DAs and DASPs.

In addition, it is important to provide an **overview of new and emerging threats** in the DA and DASP sector.

Identification of ML/TF/PF Threats

According to the "National Risk Assessment of legalisation (laundering) of criminal proceeds of the Republic of Kazakhstan" published in 2025 (*NRA (ML) 2025*), the following predicate crimes related to money laundering using digital assets should be highlighted:

- illegal entrepreneurship;
- fraud (scams, Ponzi schemes);
- illicit drug trafficking;
- corruption-related offences;
- online gambling;
- money laundering of criminal proceeds.

According to the NRA (ML) 2025, a total of 66 criminal cases related to the above-mentioned offences were registered in Kazakhstan.[4]

In addition to crimes committed within the territory of Kazakhstan, frequently committed offences involving DA identified in the latest FATF reports on the Virtual Asset (VA) sector,

[4]National Risk Assessment of legalisation (laundering) of criminal proceeds of the Republic of Kazakhstan, 2025, AFM of RK, https://www.gov.kz/memleket/entities/afm/press/article/details/61029?lang=ru

published in 2024 and 2025 (FATF Report 2024[5] and FATF Report 2025[6]), should also be highlighted, including:

- proliferation financing (PF);
- fraud (investment fraud);
- cybercrime (ransomware);
- terrorist financing.

Furthermore, the AFSA considers the use of DA to evade sanctions and tax evasion-related crimes to be significant threats to the AIFC DA and DASP sector.

Threat assessments

(Table 1)

Threat type	Inherent Risk
Money laundering*	**Significant**
Illicit drug trafficking*	Significant
Fraud*	Significant
Illegal entrepreneurship*	Significant
Tax evasion*	Significant
Corruption-related offences*	Significant
Cybercrime**	Significant
Online gambling**	Significant
Sanctions evasion**	Significant
Terrorist financing***	**Medium**
Proliferation financing (PF)***	**Low**
THREAT (overall)******	**Significant**

Notes:

* - assessment according to the NRA (ML) 2025;[7]

** - assessment based on the FATF Report 2024, FATF Report 2025, and the Chainalysis Report 2026;[8]

*** - assessment according to the National Risk Assessment of Terrorist Financing of the Republic of Kazakhstan (NRA (TF) 2025);

**** - taking into account the significance and prevalence of ML threats and the low level of TF and PF threats, the overall threat risk is assessed as significant.

[5] TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS, FATF, June 2024, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html *(FATF Report 2024)*;

[6] Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, June 2025, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html *(FATF Report 2025)*.

[7] National Risk Assessment of legalisation (laundering) of criminal proceeds of the Republic of Kazakhstan, 2025, AFM of RK, https://www.gov.kz/memleket/entities/afm/press/article/details/61029?lang=ru

[8] Chainalysis report for 2025, The 2026 Crypto Crime Report.

Suspicious and Threshold Transactions

AFSA conducted an analysis of suspicious and threshold transaction reports submitted in 2024 and 2025 to the Agency for Financial Monitoring of the Republic of Kazakhstan (AFM of RK). Below is a statistical overview of the submitted reports, as well as an analysis thereof, including a breakdown of the main categories of reports based on indicators of suspicious transactions in accordance with Order No. 13 of the Agency for Financial Monitoring 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 Indicators for Identifying Suspicious Transactions" *(AFM Order No. 13).*

Statistics on Suspicious and Threshold Transaction Reports Submitted by AIFC DASPs in 2024 and 2025 (Table 2)

Year	Suspicious Transaction Reports/Suspicious Activity Reports (STR/SAR) and Threshold Transaction Reports (TTR)	Number of submitted reports
2024	STR/SAR	118
	TTR	598
2025	STR/SAR	344
	TTR	1876

2024

The number of Suspicious Transaction Reports (STR/SAR) and Threshold Transaction Reports (TTR) submitted in 2024 is considered insignificant in relation to the total transaction volume of DASP (i.e., exceeding USD 2 billion).

- The main categories of STR/SAR submitted in 2024 are as follows: 30% – Suspicious transaction;
- 25% – Clients, their activities, transactions, or attempted transactions identified as suspicious in accordance with the internal procedures of the financial monitoring entity;
- 21% – Termination of business relationships (due to suspicions of money laundering or terrorist financing).

2025

In 2025, an increase in the number of suspicious and threshold transaction reports is observed; however, this growth correlates with the overall increase in transaction volumes during the year (i.e., exceeding USD 10.5 billion).

- The main categories of STR/SAR submitted in 2025 are as follows: 27% – Refusal to establish business relationships;
- 22% – Suspicious transaction;
- 21% – Clients, their activities, transactions, or attempted transactions identified as suspicious in accordance with the internal procedures of the financial monitoring entity.

Overall, the number of Threshold Transaction Reports (TTR) and Suspicious Transaction/Activity Reports (STR/SAR) remains moderate, reflecting the developing nature of the DA/DASP sector within the AIFC, as well as the relatively small number of DASPs that launched DA-related services in 2024 and 2025.

Notably, for risk assessment purposes, the analysis of additional metrics is more indicative. In 2024, the STR/SAR intensity amounted to approximately 0.81 reports per 1,000 clients and approximately 41.2 reports per USD 1 billion of transaction volume. In 2025, the STR/SAR intensity increased to approximately 1.60 reports per 1,000 clients and approximately 32.5 reports per USD 1 billion of transaction volume. This indicates that, as the sector expanded, the absolute number of reports increased, while their density relative to transaction volume declined.

2.1. Main money laundering threats of DAs and DASPs

1) Illicit Drug Trafficking

According to global practice, the use of DAs in drug trafficking is widespread. This is largely due to the ability to sell drugs without intermediaries, which maximises profits and simplifies distribution; the ability to operate beyond territorial limitations, allowing sellers from any location worldwide to access buyers globally; and the difficulty of tracing transactions involving certain types of DA. Proceeds derived from illicit drug trafficking may be laundered through DASPs by converting fiat funds into DA and subsequently exchanging them back into fiat currency.

In addition, DA are used as a medium of exchange between buyers and sellers in drug transactions. Numerous darknet marketplaces exist that connect drug buyers and sellers, where transactions are conducted exclusively using DA.

2) Fraud

Fraud represents a significant threat in the misuse of DA for criminal purposes. Taking into account the specific features of the AIFC, the most relevant threats include investment fraud (including Ponzi schemes), phishing attacks, fake websites or applications, pump-and-dump schemes, fraudulent endorsements (including those generated using artificial intelligence), and manipulation related to initial coin offerings (ICOs).

According to the FATF Report 2024, market participants highlighted the role of DA in investment fraud schemes, particularly in so-called “pig butchering” schemes. In such schemes, fraudsters build trust with victims and persuade them to invest in illicit DASPs.[9]

The rapid increase in the value of certain types of DA enables criminals to manipulate information to attract more users and subsequently misappropriate funds. In such schemes, perpetrators typically promise high returns to potential victims. By exploiting limited public understanding of digital financial products, criminals increase both the number of victims and the volume of illicit proceeds.

3) Illegal entrepreneurship

Activities involving the provision of DA-related services to third parties without the required authorisation to conduct business, as well as without obtaining a DASP licence issued by the AFSA for the provision of financial services with DA, represent one of the key threats to the lawful circulation of DA and may facilitate the commission of other predicate offences.

A common form of illegal entrepreneurship is the provision of transaction services on behalf of clients using the clients’ DA or using the service provider’s own funds. In such

[9] TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS, FATF, June 2024, *2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

cases, perpetrators typically fail to implement the AML/CFT/CPF systems and controls required under AIFC and Kazakhstan legislation (e.g., customer risk assessment, customer due diligence). In addition, such actors may accept or transfer funds and DA directly to users without conducting proper transaction monitoring, verifying the source of funds/DA, or performing other legally required compliance procedures.

4) Tax Evasion

Based on documented typologies and trends, including FATF “red flag” indicators, there is evidence that DA and DASPs are used globally for tax evasion.

One method involves the use of DA as a means of payment and store of value without converting them into fiat currency. In such cases, DAs are not reflected in bank accounts of individuals or entities. Even where such activities are prohibited, if transactions are not public, are limited in number, and are not advertised (e.g., payments in online stores), they are less likely to attract the attention of supervisory authorities. As a result, detecting tax evasion without voluntary disclosure by taxpayers in their declarations is challenging.

Tax evasion may also arise due to the high volatility of certain types of DA, particularly “unbacked” digital assets (e.g., Bitcoin, Ether), whose value may fluctuate significantly over short periods. This makes it difficult to accurately determine the value of DA at the time a tax offence is committed, thereby necessitating expert assessments during tax investigations.

Additionally, risks include the storage of undeclared income in the form of DA (e.g., unreported capital gains, mining proceeds). Businesses may also fraudulently reduce reported income through schemes such as false invoicing involving DA. Collectively, these factors reduce the effectiveness of tax enforcement.

5) Corruption Offences

DA may serve as an instrument of corruption-related crimes. The DA ecosystem is potentially attractive to politically exposed persons (PEPs). Public officials may use DA both to commit corrupt acts and to launder proceeds derived from public sector corruption. Another method involves the receipt of bribes in the form of DA.

Corrupt PEPs may illicitly obtain funds from public budgets or procurement contracts and convert them into DA via DASPs, facilitating cross-border transfers and bypassing traditional financial controls. Once converted, illicit funds may be layered using services that obscure transaction histories and hinder traceability. These funds may subsequently be integrated into the economy through investments in real estate or other assets or used to sustain ongoing corrupt activities.

6) Cybercrime

The technological features of DAs make them an attractive target for cybercriminals. Cybercrime encompasses a wide range of criminal activities, including hacking, theft,

ransom, extortion, and denial-of-service attacks, which can generate substantial illicit proceeds that are extremely difficult to trace and recover. Cybercriminals may remain anonymous or pseudo-anonymous, which hinders effective investigation of both the predicate offense and the associated money laundering.

The use by DASPs of “hot” wallets, despite their inherent security vulnerabilities, continues among many custodians to maintain readily accessible liquidity pools, thereby increasing exposure to cybercrime risks.

7) Online Gambling

The use of DA in the gambling sector presents a relevant threat, including the use of illegal online casinos and betting platforms for money laundering purposes. One method involves converting illicit funds into DA and depositing them into gambling platforms that accept DA. By placing bets, winning or losing, and subsequently cashing out winnings in the form of “clean” DA, individuals can effectively launder illicit funds. This process creates an additional layer of obfuscation that conceals the origin of funds.

Terrorist organisations may also use online gambling platforms to raise funds for their operations or to transfer funds between individuals and groups without attracting the attention of authorities.

Furthermore, the emergence of decentralised finance (DeFi) platforms has created new opportunities for money laundering through gambling activities. DeFi platforms enable users to access financial services such as lending, borrowing, and trading without intermediaries. While DeFi enhances financial accessibility and autonomy, it also presents challenges in terms of regulatory oversight and compliance. Illicit actors may use decentralised exchanges and lending protocols to launder funds by converting illicit proceeds into DA, engaging in crypto-gambling, and subsequently withdrawing “cleaned” funds through decentralised liquidity pools.

8) Sanctions Evasion through the Use of DA and DASPs

Another significant threat is the use of DA and DASP platforms as a means of evading sanctions. The relevance of sanctions-related risks has increased substantially in recent years, particularly in light of the strengthening of sanctions regimes across various jurisdictions.

Traditionally, commercial banks play a key role in sanctions compliance by monitoring sources of funds and screening individuals and entities against sanctions lists. However, due to the attractiveness of DA and vulnerabilities within certain DASPs, sanctioned individuals and entities may use DA to conduct international payments and transfers without the involvement of banks as intermediaries.

The risk of sanctions evasion is also linked to ML/TF/PF, as certain sanctions regimes are specifically designed to counter such threats.

Notably, in 2025 a significant portion of sanctions-related crypto transaction activity was associated not with highly anonymous DAs, but with stablecoin infrastructure, over-the-counter (OTC) intermediaries, offshore platforms, cross-chain transfers (chain-hopping), and other forms of cross-border DA movement.

2.2. Financing Terrorism via DA and DASP

One method used by terrorists to finance their activities through DA involves collecting donations from supporters worldwide. Cryptowallets can be created and publicly distributed, allowing individuals to anonymously contribute funds toward terrorist objectives without fear of detection. These donations can be utilised to fund various activities, including recruitment, training, the dissemination of propaganda, and the procurement of weapons and supplies.

Furthermore, terrorist organisations may utilise DASPs to convert fiat currency into DA, facilitating the cross-border movement of funds and enabling them to evade traditional financial controls. By depositing fiat currency into a cryptoexchange, terrorists can purchase DAs such as Bitcoin, Ether, or stablecoins, which can then be transferred to other wallets or converted back into fiat currency through various methods.

The decentralised and global nature of DA makes it difficult for authorities, such as AFSA within the AIFC, to track and intercept these illegal financial transactions. This environment allows terrorists to move funds with relative impunity, posing a continuous challenge to ML/TF/PF prevention efforts.

Case

A citizen of the Republic of Kazakhstan carried out the financing of the international terrorist organisation ISIS (DAESH) operating in Syria by transferring Bitcoin, a digital asset (DA), to the cryptowallet of a citizen of Tajikistan, a member of the terrorist organisation.

The financing was conducted with the assistance of another citizen of the Republic of Kazakhstan, who was engaged in illegal entrepreneurial activity, namely the conversion and sale of Bitcoin on a cryptoexchange.

Law enforcement authorities identified the facts of illegal activity, and subsequently, pre-trial investigations were initiated against both individuals.

2.3. Threat of Proliferation Financing through the use of DAs and DASPs

The use of DAs to support the financing of the proliferation of weapons of mass destruction continues. Notably, there is an important interconnection between PF-related crimes and cybercrime.

In recent years, a number of major cryptoexchanges, as well as well-known DeFi protocols (including decentralised exchanges and other decentralised providers of digital-asset-based financial services), have been subjected to cyberattacks carried out

by individual actors (according to publicly available sources, these actors may be associated with cyberattacks organised or sponsored by certain states).[10]

Such cybercrimes are committed, inter alia, for the purpose of using stolen DAs to finance state programs related to PF.

Case

In 2025, the largest cyberattack on Bybit cryptoexchange was carried out, resulting in the theft of DAs amounting to USD 1.46 billion.

The hackers used social engineering techniques and malicious software to gain access to the wallet infrastructure and manipulate transaction data.

With regard to money laundering methods, it should be noted that the perpetrators used services of unregistered DASPs, including over-the-counter (OTC) traders, as well as certain mixers and bridges, and a large number of wallets within complex transactional schemes (35 Bitcoin wallets and 125,000 Ethereum wallets).

The latter circumstance significantly increased the complexity of the cyberattack. It was also reported that only 3.8% of the stolen funds were recovered.[11]

2.4. Overview of new and emerging threats in the DA and DASP sector

Given the rapid development of technologies, the swift adaptation of criminals or other persons intending to commit predicate offences, changes in the digital asset (DA) market, and broader economic developments, it is important to regularly monitor newly emerging or rapidly growing threats that may become relevant to the DA/DASP sector in the near future.

According to the Kazakhstan National Risk Assessment (ML) 2025 (NRA (ML) 2025), an emerging threat may be the commission of **cyberattacks using ransomware**. Such software constitutes a type of malicious software designed to encrypt files on a victim's device until a ransom is paid in the form of digital assets to decrypt the files. At the global level, there is also an observed trend of **cyberattacks targeting cryptoexchanges**.

At the same time, the **FATF Report 2025** identifies the following **emerging and growing threats**:

- continued and increasing use of **stablecoins** for criminal purposes;
- **decentralised finance (DeFi)**;
- **large-scale theft of DAs** and laundering through digital assets;

[10] TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS, FATF, June 2024, *2024-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

[11] Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, FATF, 2025 https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf

- growth in existing and new types of **fraud**;
- **offshore (or foreign) DASPs**.

Growing threat from offshore DASPs

The latest FATF report places particular emphasis on the threats and risks posed by offshore (unregistered foreign) DASPs.[12] For the AIFC and the Republic of Kazakhstan, a particularly significant risk arises from the provision of services to Kazakhstan residents by offshore DASPs without an appropriate licence in the applicable jurisdiction, or under a formal licence issued in a jurisdiction with weak ML/TF/PF supervision.

Such a business model may include:

- active targeting of clients through internet platforms, social media, affiliate marketing schemes, mobile applications, and messengers;
- use of VPNs and geolocation masking;
- routing transactions through intermediary exchanges (so-called nested exchanges).

In addition to the threats identified in the NRA (ML) 2025 of Kazakhstan and by the FATF, according to an analytical report by market participants, the most pronounced growth trend in 2025 was observed in offences related to sanctions evasion (for more details on the growth dynamics, see Fig. 1).[13]

[12] Understanding and Mitigating the Risks of Off-shore Virtual Asset Service Providers, FATF Report, March 2026.
[13] Chainalysis report for 2025, The 2026 Crypto Crime Report.

3. CHARACTERISATION OF VULNERABILITIES

The existence of the above-mentioned threats in the **DA sector** is made possible due to a number of vulnerabilities inherent to **digital assets** (including specialised systems related thereto), as well as vulnerabilities of **financial sector participants - DASPs**, and, finally, vulnerabilities of **traditional financial institutions** when interacting with the **DA and DASP sector**.

For the purposes of this report, **vulnerabilities** are understood as characteristics inherent to the **DA sector** that make it susceptible to **illegal use for ML/TF/PF purposes**.

This report identifies the following **three main categories of vulnerabilities**:

3.1. Vulnerabilities related to the technological features of Digital Assets:

- anonymity and pseudonymity;
- ease of use;
- irreversibility of transactions and security;
- access to platforms of foreign unlicensed DASPs;
- the cross-border nature of the digital asset sector.

3.2. Vulnerabilities related to DASP activities:

- vulnerabilities related to clients;
- vulnerabilities related to DASP products and services;
- jurisdiction-related vulnerabilities;
- vulnerabilities related to delivery channels;
- vulnerabilities related to weaknesses in DASP systems and controls.

3.3. Vulnerabilities of the traditional financial sector in interactions with the DA and DASP sector

Assessment of vulnerabilities of Digital Assets and DASPs (Table 3)

Vulnerability category	Assessment of vulnerability
Technological features of DAs	**Significant**
Activities of DASPs	High
• Customers	High
• Products/services	High
• Jurisdiction	High
• Service delivery channels	Significant
• Operational activities (systems and controls)	**Medium**
Linkages between the traditional financial sector and DAs and DASPs	Significant
VULNERABILITY (overall)	**Significant**

3.1. Vulnerabilities related to the technological features of Digital Assets

1) Anonymity and Pseudonymity

Anonymity refers to a vulnerability associated with the anonymous or pseudonymous nature of transactions carried out using DAs and digital wallets, which attract criminals seeking to achieve ML/TF/PF objectives and to evade sanctions.

This risk is particularly relevant in cases where the user's identity cannot be properly established, either because the user has not undergone Know Your Customer / Customer Due Diligence (KYC/CDD) procedures or has undergone such procedures using fraudulent or falsified documents.

Different DAs offer varying levels of anonymity, and it is most likely that criminals pursuing ML/TF/PF objectives will prefer digital assets with a higher degree of anonymity.

2) Ease of Use

Ease of use reflects the transactional or exchange liquidity of a DAs, its relative price stability, and the technical knowledge required for its use.

A higher degree of ease of use increases the susceptibility of digital assets to ML/TF/PF-related crimes. Conversely, technological complexity is considered a significant limitation on ease of use and therefore acts as a barrier to the broader adoption of digital assets by potential criminals.

The vast majority of DAs are unbacked and highly volatile. At the same time, it should be noted that the largest transaction volumes in the digital asset sector are concentrated in stablecoins, which exhibit lower volatility due to their peg to traditional fiat currencies and reserve backing in the corresponding fiat currencies or other liquid instruments.

Despite the upward trend in trading volumes on AIFC-licensed DASP platforms, challenges related to ensuring sufficient liquidity remain.

3) Irreversibility of Transactions and Security

In this context, irreversibility refers to the likelihood that a user cannot cancel a DAs transaction. DAs that do not provide transaction reversibility are particularly attractive to criminals seeking to achieve ML/TF/PF objectives.

Transaction irreversibility offers significant advantages to criminals. In traditional financial instruments, such as credit cards, a transaction may be reversed by the user or the bank at certain stages if fraud is detected. In many DAs, transactions are irreversible (for example, unbacked digital assets such as Bitcoin, Ether, Solana, etc.). Consequently, even if fraudulent activity is detected at an early stage, funds cannot be automatically recovered, leading to significant challenges in the recovery of assets derived from criminal activity.

4) Access to platforms of foreign unlicensed DASPs

The ability to register with and use services of foreign DASP platforms that are not licensed in the AIFC, bypassing the requirements of the AIFC Acts, reduces the effectiveness of the regulatory regime applicable to AIFC-licensed DASPs. Such access may be enabled through web-based platforms (websites) and mobile applications of DASPs not licensed in the AIFC.

This category includes vulnerabilities arising when actual client servicing, data storage, compliance functions, technical infrastructure, and management are located in different jurisdictions. Such operating models may hinder: identification of the responsible entity, access to KYC/CDD information, application of supervisory powers, and execution of requests from competent authorities.

Additional indicators of heightened vulnerability include: use of nominal or insufficiently qualified compliance staff; weak geolocation controls; provision of services exclusively through mobile or web applications without local presence; involvement of third parties not formally licenced as DASPs in data processing or the performance of other critical functions.

5) Cross-border nature of the DA sector

Blockchain technology enables access to counterparties both through intermediaries such as DASPs and without their involvement, via the use of hot wallets and non-custodial wallets. In addition, the DA and DASP market structure necessitates active interaction between locally licenced DASPs and foreign DASPs.

Such cooperation is required due to objective characteristics of the developing digital asset market, including: insufficient liquidity on local DASP platforms; digital asset issuers (e.g., certain stablecoin issuers) operating in foreign jurisdictions; the absence of jurisdictional anchoring in blockchain technology.

At the same time, the cross-border nature of the DA sector creates specific vulnerabilities from a transaction monitoring perspective.

In particular, vulnerabilities may arise from:

- difficulties in identifying DA owners using non-custodial wallets to transfer assets in or out;
- the ability to conduct peer-to-peer (P2P) transactions between owners of non-custodial wallets outside centralised DASPs.

While P2P transactions circumventing DASPs may be popular, their effectiveness for ML/TF/PF purposes without the involvement of centralised DASPs is limited, as DAs are not recognised as legal tender, and their use for payment of goods and services remains constrained. As a result, criminals typically rely on centralised DASPs at certain stages of ML/TF/PF schemes, primarily to exchange digital assets for fiat currency and withdraw fiat funds.

Furthermore, a major challenge for the DA and DASP industry lies in the uneven implementation of the FATF “«Travel Rule»”. Although, according to FATF, 85 out of 117 surveyed jurisdictions have adopted legislation implementing the «Travel Rule», such

legislation may not have been adopted in 42 out of 205 jurisdictions, resulting in persistent regulatory fragmentation.[14]

3.2. Vulnerabilities related to DASP activities

1) Client-Related Vulnerabilities

In accordance with AIFC requirements, each DASP client is subject to a risk assessment conducted by the DASP.

As of the end of 2025, the total number of DASP clients amounted to 214,933 individuals.

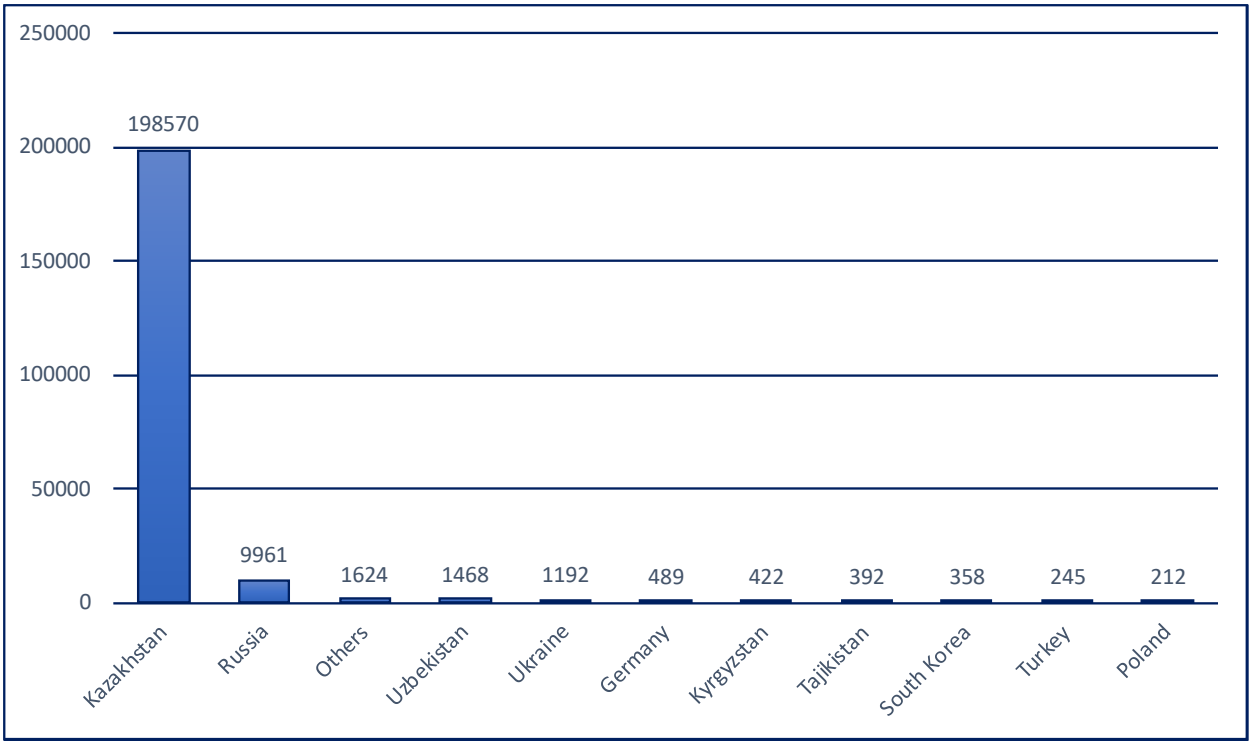
Residency

The majority of DASP clients are residents of the following countries/territories: Kazakhstan, Russia, Ukraine, Uzbekistan, Germany, Kyrgyzstan, Tajikistan, South Korea, Turkey, and Poland.

A significant majority of clients are residents of Kazakhstan, totalling 198,570 individuals (92%), while the remaining 16,363 clients (8%) are non-residents.

Below is a chart illustrating the number of AIFC DASP clients, prepared on the basis of reports submitted by DASPs to the AFSA (AFSA).

Number of AIFC DASP Clients by Country *(Fig. 4)*



[14] Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, FATF, 2025, https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf

Case

On an AIFC DASP platform, an active client carried out a transaction in the amount of X USDT to an online gambling service registered in a foreign jurisdiction. The specified platform is not authorised to operate in the territory of the Republic of Kazakhstan.

The transaction was identified by the transaction monitoring system and additionally analysed using several blockchain analytics tools. During the internal review, the responsible officer established that the client's counterparty (the recipient of the digital assets) belonged to the online gambling category with elevated ML/TF risk and was operating outside the regulatory jurisdiction of Kazakhstan and the AIFC. The transaction was classified as containing suspicious indicators, including interaction with an unregulated foreign service and the use of digital assets for the potential circumvention of restrictions.

As a result of the analysis, the DASP decided to submit a suspicious transaction report (STR) to the Agency for Financial Monitoring of the Republic of Kazakhstan. Depending on the aggregate risk factors identified, risk-mitigation measures were applied, including enhanced monitoring of the client's transactions.

Case

During the verification of the permanent place of residence of a foreign national, an employee of an AIFC DASP identified evidence of editing of a digital document submitted to confirm a residential address in the Republic of Kazakhstan. This fact was confirmed by identifying a non-existent Individual Identification Number (IIN) included in the document. In addition, it was deemed suspicious that the applicant logged in exclusively from IP addresses of a foreign country.

The DASP decided to reject the individual's registration application and immediately submitted a report to the Agency for Financial Monitoring of the Republic of Kazakhstan, indicating the fact of document falsification.

High-Risk Clients

Following the results of client risk assessments, AIFC DASPs identified 329 clients with a high ML/TF/PF risk in 2024 and 1,556 clients in 2025. The share of high-risk clients amounted to 0.2% of the total number of clients (145,800) in 2024 and 0.7% of the total number of clients (214,933) in 2025.

Non-resident DASP clients from the following countries may present an elevated ML/TF/PF risk and are subject to enhanced monitoring by the FATF as of 21 February 2025 and 13 July 2025: Algeria, Angola, Bulgaria, Burkina Faso, Cameroon, Croatia, Haiti, Kenya, Laos, Nigeria, the British Virgin Islands, and South Africa.

As of the end of 2025, the total number of DASP clients from high-risk jurisdictions amounted to 123 individuals, representing 0.057% of the total client base.

Individuals and Legal Entities

The total number of individual clients amounted to 214,382 (99.7%), while the number of legal entity clients totaled 551 (0.3%).

Notably, clients-legal entities pose an elevated money laundering and sanctions risk. Such risk may be further intensified when legal entities are incorporated in foreign jurisdictions, particularly in high-risk jurisdictions (as identified by the FATF and other lists under AIFC Acts and Kazakhstan legislation).

Of the total number of legal entities:

- 221 were resident legal entities;
- 330 were non-resident legal entities;
- 4 non-resident legal entities were incorporated in high-risk jurisdictions.

2) Vulnerabilities Related to DASP products and services

Product risk refers to the risks to which DASPs and their clients are exposed due to the characteristics of the digital assets used and the services provided. Below is a table presenting the assessment of ML/TF/PF risks of DASP products and services, as well as the results of residual risk assessments conducted by the DASPs.

Assessment of residual ML/TF/PF Risks of DASP products and services *(Table 4)*

Type of products / services	Residual ML/TF/PF risk of products / services (according to AIFC DASP assessment)
Digital assets (products)	**Significant**
Services with the use of DAs	**Medium**
Spot trading	Significant
Margin trading	Medium
Regulated P2P trading	Medium
Digital asset derivatives trading (futures, options)	Medium
OTC trading (crypto brokerage / dealer activities)	Medium
Custodial storage of DAs	Low
Crypto deposits (earn products)	Medium
Payments, transfers, acquiring, or other payment transactions using digital assets	Significant
Issuance of crypto cards	Medium
Stablecoin issuance	Medium
DASP products and services (overall)	**High**

Note: The assessment of residual ML/TF/PF risks reflects the latest product and service risk assessments conducted by DASPs, based on data provided by AIFC-licensed DASPs.

Risk ratings assigned to individual DASP products and services should be interpreted in conjunction with the maturity of the control framework and the specific business model of each DASP. In particular, a comparatively lower risk assessment for custodial services is acceptable only where strong and demonstrably effective controls are in place, including: segregation of client assets; management of hot and cold wallets; regular reconciliations; cybersecurity controls; suspicious activity monitoring; wallet-level vulnerability screening; due diligence and verification of third-party custodial arrangements.

Digital Assets (products)

DAs constitute products that are traded on cryptoexchanges or used by other DASPs licensed in the AIFC.

Taking into consideration the vulnerabilities related to the technological characteristics of digital assets, DAs represent a significant vulnerability for DASPs.

As of the end of 2025, a total of 113 digital assets had been approved for trading by DASPs within the AIFC regulatory sandbox.

Digital Asset Services

According to Table 4 – DASP products and services (2025), as of the end of 2025, AIFC-licensed DASPs provided the following services: spot trading; margin trading; regulated P2P-trading; OTC trading; derivatives trading; custodial services; Providing Money Services in relation to Digital Assets; crypto deposit (earn) products; issuance of crypto cards.

Notably, based on the data presented in the table, spot trading services and Providing Money Services in relation to Digital Assets, due to their elevated risk level as assessed by DASPs and high transaction volumes, represent a high level of vulnerability for DASPs.

Other digital asset services were assessed as presenting a medium level of residual ML/TF/PF risk and, accordingly, a moderate level of vulnerability for DASPs.

3) Jurisdiction-related vulnerabilities

Clients' residency

The majority of AIFC clients are residents of the following countries/territories: Kazakhstan, Russia, Ukraine, Uzbekistan, Germany, Kyrgyzstan, Tajikistan, South Korea, Turkey, and Poland.

The prevailing majority of clients are residents of Kazakhstan, while the share of non-resident clients remains limited. Figure 4 above presents a chart showing the number of AIFC DASP clients, compiled on the basis of reports submitted by DASPs to the AFSA.

DASP Operations

AIFC-licensed DASPs do not maintain branches or subsidiaries outside the AIFC and the Republic of Kazakhstan.

4) Vulnerabilities related to delivery channels

As the AIFC regulatory regime excludes cash transactions in the DA sector, AIFC DASPs primarily provide services remotely.

Remote delivery is traditionally considered a risk-enhancing factor, due to threats related to potential impersonation of clients, including the use of forged documents and/or third-party documents (which may be stolen or belong to relatives or acquaintances).

Accordingly, the remote establishment and ongoing maintenance of business relationships represents a factor that increases vulnerability in the provision of services by AIFC DASPs.

5) Vulnerabilities related to weaknesses in DASP systems and controls

Operational risks faced by DASPs include factors such as: the design and quality of internal control frameworks; the total number of employees; outsourcing arrangements and reliance on third parties; governance structures and formation of management bodies; processes for appointment of key personnel; interaction between control functions; and regular internal and external audit practices.

Examples from international practice demonstrate the importance of a responsible and rigorous approach by DASPs when appointing individuals to key positions.

It should be noted that, out of 29 DASPs licensed as of the end of 2025, only 15 DASPs were operational, while the remaining 14 DASPs were primarily at the stage of fulfilling licensing conditions or conducting preparatory work prior to the launch of licenced services.

In this context, despite the relatively large number of licenced DASPs, the absence of operations by approximately 50% of licenced DASPs constitutes a factor that reduces the overall level of vulnerability within the DASP sector.

Case

The recent collapse of several digital asset market intermediaries, such as Celsius Network and Voyager Digital, demonstrated the transmission of risks within the digital asset market due to significant liquidity and maturity mismatches between assets and liabilities (in the case of Celsius) and a high degree of interconnectedness among market participants (in the case of Voyager).

Trading and lending platforms of this type were able to offer investors high returns by assuming substantial liquidity and maturity risks. They promised investors an immediate redemption of funds while investing the attracted funds in less liquid assets and additionally used borrowers' collateral to increase leverage.

As long as inflows of funds exceeded outflows, these intermediaries benefited from liquidity and maturity premiums.

However, when market sentiment deteriorated, it became evident that these companies lacked sufficient resources or effective risk management systems to withstand mass client withdrawals, forced liquidations or defaults of major counterparties.

Due to the high level of interconnectedness among participants, risks originating from several entities rapidly spread across the entire digital asset market.

Information Security

Special attention should be given to vulnerabilities in the IT and cybersecurity systems of DASPs. At the global level, DASPs have repeatedly been targeted by cyberattacks, as a result of which both DASPs and their clients may incur significant losses.

3.3. Vulnerabilities of the traditional financial sector in interaction with the DA and DASP Sector

The development and use of DAs and the activities of DASPs rely heavily on interaction with the traditional financial sector, including the banking system, payment institutions, and other financial intermediaries. In particular, access to "fiat on- and off-ramps", especially access to the banking system of Kazakhstan, has played a key role in the development of the DA and DASP sector.

Furthermore, alongside the regulation and growth of the DA and DASP sector, there is a growing trend toward the integration of traditional financial services with financial services involving digital assets.

However, such interconnections may lead to the spillover of ML/TF/PF risks from the DA sector into the traditional financial sector, thereby increasing the vulnerabilities of traditional financial institutions. These vulnerabilities may arise from an insufficient understanding by traditional financial sector participants of the risks associated with

digital assets and DASPs, as well as a lack of familiarity with new technologies and digital-asset-related crime typologies.

Banking sector and the DA/DASP sector

Taking into consideration the critical role of the banking system as a fiat gateway for the inflow and outflow of funds, the vulnerability of Kazakhstan's banks to ML/TF/PF risks originating from the DA/DASP sector remains relevant. As noted above, eight second-tier banks of the Republic of Kazakhstan participated in the Pilot Project, interacting with eight digital asset exchanges licensed in the AIFC. As of the end of 2025, more than 10 second-tier banks in Kazakhstan interact with various AIFC-licensed DASPs.

Combination of traditional financial services with DA

A trend has been observed whereby companies licensed in the AIFC, primarily as broker-dealers, fund managers, or payment service providers, either

(i) launch additional services or products alongside existing instruments, or

(ii) initially obtain licences covering both securities or fiat-based products and digital asset-based products.

As of the end of 2025, such combinations can be categorised as follows:

- **Investment business (broker-dealers, fund managers, etc.):**
  9 licenced companies combine financial services involving securities and digital assets. Of these, two companies had not launched DA services by the end of 2025, while seven companies were operational.

- **Payment institutions:**
  8 DASPs licensed in the AIFC are authorised to provide payment transactions in fiat funds while also using digital assets. Among these DASPs, four were operational, while four had not commenced operations as of the end of 2025.

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

When DAs are used for ML/TF/PF purposes or for committing predicate offences, potential offenders are using specific vulnerabilities described above. Accordingly, measures aimed at reducing the level and number of vulnerabilities inevitably affect the conditions enabling the emergence of potential threats and contribute to an overall reduction of threat levels.

Regular risk environment analysis and monitoring of the digital asset sector enable the AFSA to apply targeted measures to reduce ML/TF/PF risks. These special procedures, measures, and control tools apply to the activities of licensed DASPs operating within the AIFC.

Taking into consideration the high inherent risk of the DA and DASP sector (taking into account identified threats and vulnerabilities), the AFSA previously conducted sectoral risk assessments of the DA and DASP sector in 2021 (prior to the launch of the Pilot Project) and subsequently in 2024.

The following key measures are identified to reduce the level of threats and vulnerabilities:

4.1. General measures to reduce threats and vulnerabilities

- AIFC regulatory framework;
- Licensing and supervisory measures of the AFSA;
- Practical measures implemented by the AFSA.

4.2. Measures aimed at reducing vulnerabilities related to the technological features of Digital Assets

- Measures to reduce vulnerabilities arising from the pseudo-anonymous and anonymous nature of digital assets and crypto transactions;
- Measures to reduce vulnerabilities related to the ease of use of digital assets;
- Measures to reduce vulnerabilities associated with the irreversibility of transactions and security;
- Measures aimed at reducing threats posed by foreign unlicenced platforms;
- Measures aimed at mitigating vulnerabilities related to the cross-border nature of the digital asset sector.

4.3. Measures aimed at reducing vulnerabilities related to DASP activities

- Measures to reduce client-related vulnerabilities;
- Measures to reduce vulnerabilities related to products and services;
- Measures to reduce jurisdiction-related vulnerabilities;
- Measures to reduce vulnerabilities related to service delivery channels;
- Measures to reduce operational vulnerabilities.

4.4. Measures aimed at reducing vulnerabilities of the traditional financial sector resulting from exposure to risks from DAs and DASPs

Effectiveness assessment table of measures

(Table 5)

Type of control	Control efficiency
General measures to mitigate threats and vulnerabilities	Efficient
Measures aimed at reducing vulnerabilities related to the technological features of DAs	Efficient
Measures aimed at reducing vulnerabilities related to the activities of DASPs	Efficient
Measures aimed at reducing vulnerabilities of the traditional financial sector arising from interaction with the DA/DASP sector	Efficient
THREAT AND VULNERABILITY MITIGATION MEASURES (overall)	**Efficient**

Note: Measures may be assessed as having the following level of effectiveness: highly effective, effective, partially effective, or ineffective.

4.1. General measures to reduce threats and vulnerabilities

1) Regulatory framework of AIFC

Overall Regulatory Overview

Within the framework of establishing a licensing regime for DASPs and the subsequent supervision and oversight of their activities by the AIFC, an innovative legal and regulatory framework governing the circulation of DAs and DASP activities has been developed, implemented, and applied within the AIFC.

Comprehensive regulation was adopted and entered into force in 2024, following the implementation of the Pilot Project, which was conducted from 2022 through the end of 2023. The key prerequisite for providing digital-asset-related services is obtaining a licence from the AFSA, which authorises the provision of financial services involving digital assets within the AIFC and in the territory of the Republic of Kazakhstan.

The AIFC regulatory framework is comprehensive and covers, inter alia, the following areas:

- regulation of a wide range of DA-related financial services, including but not limited to cryptoexchanges, custody of digital assets, crypto-brokers, crypto-dealers, stablecoin issuance, managing investments (including digital assets), and financial advisory services involving digital assets (for further details on licence types, see the section Digital Asset Service Provider);
- regulation of ML/TF/PF and sanctions compliance requirements;
- prudential regulation, including regulatory capital requirements for DASPs;
- establishment of IT and cybersecurity systems and controls;
- corporate governance requirements;
- protection of client and investor rights and interests;
- other related requirements.

Notably, AIFC regulatory regime excludes the circulation of cash within the DA sector, which significantly reduces risks associated with the use and movement of cash, including risks relevant to the DA sector.

Besides, AIFC regulatory regime for DAs and DASPs is aligned with international best standards, as confirmed by:

i) the results of the IOSCO Thematic Review "Assessing the Implementation of IOSCO Recommendations for Crypto and Digital Asset Markets"[15], published in October 2025, in which the AIFC demonstrated the highest level of progress among participating jurisdictions, having fully implemented the IOSCO recommendations as of 31 July 2025;
ii) the completion of the Mutual Evaluation of the national AML system, finalised in 2023, following which Kazakhstan was placed under regular (standard) monitoring.[16]

Definitions of DA and DASP

According to the AIFC Glossary, a Digital Asset (DA) is a *digital representation of value that:*

can be digitally traded and functions as

(a) a medium of exchange, or

(b) a unit of account, or

(c) a store of value;

can be exchanged for fiat currency but is neither issued nor guaranteed by the government of any jurisdiction;

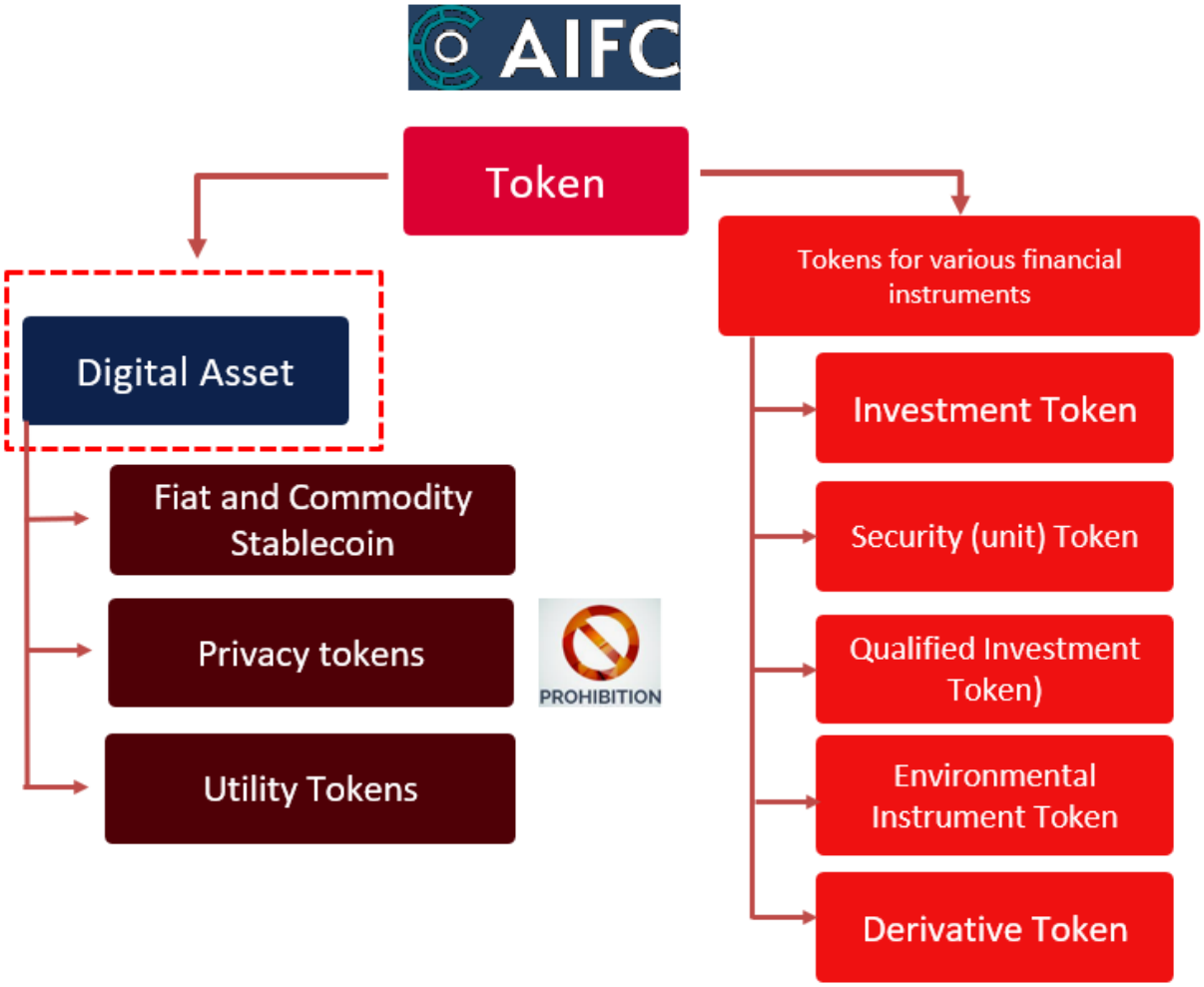
performs the above functions solely by agreement within the community of users of the digital asset; and

is therefore distinct from fiat currency and electronic money.

The AIFC definition of a DA is consistent with the definition of a virtual asset as set out in the FATF Guidance on Virtual Assets and Virtual Asset Service Providers (2019).[17]

[15] Thematic Review Assessing the Implementation of IOSCO Recommendations for Crypto and Digital Asset Markets, Final Report, IOSCO, October 2025. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD801.pdf
[16] Mutual Evaluation Reportof the Republic of Kazakhstan, EAG, 2023, https://eurasiangroup.org/files/uploads/files/ME_(2023)_1_rus_rev1_2.pdf
[17] A virtual asset is 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. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

Taxonomy of Digital Assets and other assets using blockchain technology



Digital Asset Service Provider

According to the AIFC Glossary, the term Digital Asset Service Provider (DASP) covers all types of activities falling within the scope of the FATF definition of a Virtual Asset Service Provider (VASP).

AIFC DASP and FATF VASP Terminology

(Table 6)

Under the FATF definition, a Virtual Asset Service Provider (VASP) is any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person.	*A Digital Asset Service Provider (DASP) under the AIFC Glossary is A Centre Participant which has been licensed by the AFSA to carry on one or more of the following Regulated Activities in relation to Digital Assets:* • *Operating a Digital Asset Trading Facility;* • *Dealing in Investments as Agent;* • *Dealing in Investments as Principal;* • *Managing Investments;* • *Managing a Collective Investment Scheme;* • *Providing Custody;* • *Arranging Custody;* • *Advising on Investments;* • *Arranging Deals in Investments;* • *Providing Money Services.* *Below are the types of licences under the AIFC DASP definition, corresponding to the types of services under the FATF VASP definition.*
i. Exchange between virtual Assets and fiat currencies;	• Operating a Digital Asset Trading Facility; • Providing Money Services; • Dealing in Investments as Agent; • Dealing in Investments as Principal.
ii. exchange between one or more forms of virtual assets;	• Operating a Digital Asset Trading Facility • Providing Money Services; • Dealing in Investments as Agent; • Dealing in Investments as Principal.
iii. transfer of virtual assets;	• Such DA transfer activities may be carried out under most types of AIFC DASP licences*.
iv. safekeeping and/or administration of virtual assets, or instruments enabling control over virtual assets; and	• Providing Custody.

v. participation in and the provision of financial services related to an issuer's offer and/or sale of a virtual asset;	• Providing Money Services
	  ○ Issuance of Fiat stablecoins;
	  ○ Issuance of Commodity stablecoins.

Overview of relevant regulatory acts

Below is the regulatory and legal framework governing the authorisation of persons operating with DAs, as well as specific requirements for conducting DA-related activities, including mandatory ML/TF/PF requirements.

- **AIFC Financial Services Framework Regulations (FSFR).** FSFR establishes the legal foundations and general requirements for the regulation of all financial services within the AIFC.

More detailed requirements applicable to companies operating in the AIFC are set out in the following regulatory acts:

- **AIFC Rules on Digital Asset Activities** - These are the primary regulations establishing the requirements and procedures for the activities of DASPs, including, inter alia, cryptoexchanges, crypto-brokers, investment managers, and other DASPs.
- **Stablecoin Regulatory Framework** - This framework regulates the issuance of stablecoins pegged to fiat currencies or commodities. The relevant provisions are set out in Part 4 of the AIFC Rules on Digital Asset Activities.
- **AIFC Rules and mechanisms of cooperation of Unbacked Cryptoexchanges and/or Centre Participants authorised to carry out digital asset-related activities with second-tier banks of the Republic of Kazakhstan (Rules of cooperation)** - these rules regulate the interaction between DASPs and second-tier banks of Kazakhstan, including limitations and thresholds applicable to DASP services when cooperating with such banks.
- **AIFC Providing Money Services Framework** - this framework establishes new requirements for the use of DAs in the provision of payment services, including requirements related to client protection, cyber resilience, and operational resilience.
- **AIFC General Rules (GEN)** - these rules contain general licensing requirements for companies, provisions related to the appointment of key and compliance officers (including Money Laundering Reporting Officer (MLRO)), procedures for the approval of controllers, and the list of licensable regulated activities, including financial services involving DAs.
- **AIFC Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Rules (AML Rules)** - these rules establish the ML/TF/PF regulatory regime, including specific requirements applicable to DASPs, such as compliance with the "«Travel Rule»". In addition, DASPs are required to comply with national ML/TF/PF legislation of the Republic of Kazakhstan.[18]
- **Guidance (Requirements) applicable to the Rules of Internal Control for the purposes of counteracting the legalisation (laundering) of proceeds from crime and the financing of terrorism for financial monitoring entities of the**

[18] LAW OF THE REPUBLIC OF KAZAKHSTAN On Counteracting the Legalization (Laundering) of Proceeds Derived from Criminal Activities, the Financing of Terrorism, and the Financing of the Proliferation of Weapons of Mass Destructionб 28 August 2009, № 191-IV.

Astana International Financial Centre (the Relevant Persons) (Rules of Internal Control)

- **Guidance (Requirements) for the purposes of counteracting the legalisation (laundering) of proceeds from crime and the financing of terrorism, applicable to the Customer Due Diligence in cases when the Astana International Financial Centre Participants (the Relevant Persons) establish non-face to face business relations with customers (Requirements on remote CDD)**
- **Practical Guidance for to AIFC Anti-Money Laundering and Counter-Terrorist Financing Framework;**
- **AIFC Conduct of Business Rules (COB)** - these rules establish requirements applicable to DASPs aimed at ensuring protection of client and investor rights and interests.
- **AIFC Financial Technology Rules (FINTECH Rules)** - these rules regulate activities carried out within the AIFC regulatory sandbox.

ML/TF/PF regime (requirements applicable to DASPs and other financial monitoring entities)

To prevent the misuse of DASPs by criminals, the AIFC AML Rules establish the following ML/TF/PF requirements applicable to DASPs:

- application of ML/TF/PF requirements to licensed firms (Rules 1.2 and 2.1 of the AIFC AML Rules);
- application of a risk-based approach, including assessment of risks related to the business of the AIFC Participant and its clients (Chapters 4 and 5 of the AML Rules);
- customer identification and verification, including identification of the ultimate beneficial owner, PEPs, and source of funds (Chapter 6 of the AML Rules);
- establishment and conduct of Customer Due Diligence (CDD) procedures, including enhanced and simplified CDD (Chapters 6–8 of the AML Rules).

Taking into consideration that the AIFC is a non-cash jurisdiction and client relationships are established remotely, simplified CDD is not permitted for AIFC Participants, including DASPs, in accordance with the Requirements on remote CDD.

Under the AIFC legal framework, customer due diligence measures also include mechanisms for detecting illegal or criminal activity, including other predicate offences such as proliferation financing, drug trafficking, fraud, and others.

As part of ongoing CDD, in accordance with Rule 6.5.1 of the AML Rules, an AIFC Participant is required to screen its clients, their business, and transactions against:

United Nations Security Council sanctions lists and “black lists” of individuals and entities published by the authorised bodies of the Republic of Kazakhstan.

Procedural details of such screening are set out in the AIFC Rules of Internal Control, dated 15 May 2020. In particular, pursuant to sub-paragraph 5 of Paragraph 22 of these

Rules of Internal Control, an identification program must be established for clients, their representatives, and beneficial owners, which includes verification against relevant lists.

Screening is conducted to identify: involvement in terrorist or extremist activities and possible links to proliferation financing, in accordance with the lists specified under sub-paragraph 10 of Paragraph 15 of the Rules of Internal Control.

1) Licensing and supervisory measures of the AFSA

AML/CFT/CPF regime (AFSA's procedures)

The AML/CFT/CPF regime of the AIFC represents a risk-based model of supervision and regulation, grounded in the AIFC AML Rules, which are aligned with the principles, guidance, and recommendations of the FATF.

The AFSA has implemented all three lines of defence:

1. First Line of defence

1.1. At the registration and licensing stage, the following is ensured:
• disclosure of ownership structure through identification of ultimate beneficial ownership;
• fit and proper assessments of shareholders, beneficial owners, and key management personnel (Part 3, Chapters 1–2 of the FSFR; Part 1, paragraphs 1.1.4 and 1.1.5 (for regulated entities), and Part 1.2, paras 1.2.3 and 1.2.4 (for Authorised Market Institutions) of the AIFC General Rules);
• as part of preventing the misuse of AIFC-based DASP platforms for ML/TF/PF and other illicit activities, requirements include: completion of customer due diligence on prospective DASPs at the licensing application stage; verification that internal AML/CFT/CPF policies and procedures have been adopted by DASP management; appointment of a designated MLRO as a licensing condition; mandatory confirmation that such officer has no criminal record and possesses relevant experience or knowledge in AML/CFT/CPF, including an interview process; requirements for ongoing monitoring, review, and updating of AML/CFT/CPF policies and procedures; disclosure of ownership structure and ultimate beneficial owner of the applicant; and mandatory screening of directors and owners against World-Check "blacklists" to identify individuals linked to criminal activities.

1.2. Following registration and licensing, companies are assigned risk ratings and corresponding Risk Mitigation Programs. Compliance with all requirements and recommendations of such programs is a mandatory condition within the AIFC (either before commencing operations or within a specified timeframe) in accordance with para 5.5 of the AFSA FinTech Lab Supervisory Procedures dated 23 April 2020 or Authorisation/Licence Notices of DASPs.

1.3. At the supervisory stage, ongoing monitoring of companies is conducted based on reporting (off-site supervision), as well as through on-site scheduled, unscheduled, and thematic inspections (focused on specific areas of activity). One of the key supervisory priorities is ensuring the mitigation of ML/TF/PF risks (para. 3.3 of the FinTech Lab Supervisory Procedures).

2. Second line of defence

2.1. Within the second line of defence, the Anti-Financial Crime Division of the AFSA provides additional expertise, support, monitoring, and coordination across departments at all stages, with a focus on ML/TF/PF risk management. Additionally, it acts as the coordinator for interaction with the financial intelligence unit, law enforcement agencies, and courts.

At this stage, enhanced due diligence measures are applied to companies and their beneficial owners; thematic inspections and monitoring are conducted; and typologies of ML/TF/PF schemes are identified.

To raise awareness of ML/TF/PF risks, the Anti-Financial Crime Division conducts regular training for AFSA staff, including mandatory knowledge testing, and organises outreach and information sessions with AIFC DASPs.

3. Third line of defence

3.1. Within the third line of defence, the Internal Audit function of the AFSA provides independent and objective assurance and recommendations regarding the adequacy and effectiveness of the AFSA's corporate governance and risk management framework.

Thus, the existing risk-based supervisory model adopted by the AFSA enables supervisory units to systematically assess entities from a risk perspective, as well as to ensure continuous monitoring and identification of ML/TF/PF risks.

Case

AFSA rejected the application of individual A for approval as the ultimate beneficial owner of a company registered in the AIFC.

The main reasons for the refusal were:

1) the provision of insufficient evidence regarding the source of wealth, which did not allow confirmation of the origin of funds in accordance with applicable regulatory requirements;
2) the failure to disclose information regarding the withdrawal of a previously submitted application to conduct similar activities in another jurisdiction.

Alongside ensuring the effectiveness of the three lines of defence, the AFSA carries out ongoing engagement with AIFC Participants to maintain and enhance their awareness of

current ML/TF/PF trends and typologies. In addition, AFSA conducts informational sessions aimed at explaining AIFC requirements related to the development and implementation of ML/TF/PF measures.

Training and awareness-raising activities are delivered both by the AFSA itself and with the involvement of international experts. As of the end of 2025, more than 30 seminars, training sessions, and roundtables had been conducted specifically for DASPs, including events with the participation of experts from the IMF, UNODC, RUSI, the U.S. Embassy, the UK Embassy, the EAG, and the International Training and Methodology Center for Financial Monitoring.

3) **Practical measures of the AFSA**

Preventive measures implemented by AFSA

In the course of implementing procedures within the framework of the three lines of defence, the AFSA has taken the following preventive measures:

- Six (6) applicants were refused a DASP licence;
- Ten (10) DAs were denied approval for admission to trading;
- In the course of cooperation with foreign and national financial and other regulatory authorities, in 2024 the AFSA received 1 request and sent 10 requests concerning DASPs and/or DASP licence applicants.
- In 2025, information-exchange statistics amounted to 4 incoming requests and 24 outgoing requests to foreign and national regulators. Requests for information exchange primarily concerned obtaining information on the reputation of DASPs, DASP senior officers, or candidates for positions subject to AFSA approval. Information exchange between the AFSA and regulatory authorities is carried out on the basis of an extensive legal cooperation framework, including:
    - 58 bilateral memoranda of understanding between the AFSA and foreign/national regulators;
    - Participation in the IOSCO Multilateral Memorandum of Understanding (MMoU);
    - Participation in the IOSCO Enhanced Multilateral Memorandum of Understanding (EMMoU).

Supervisory Measures of the AFSA (including measures aimed at detecting violations)

The supervisory measures applied by the AFSA include:

- Regulatory monitoring, conducted through the collection and analysis of monthly and quarterly regulatory reports;
- On-site and off-site inspections, including scheduled and ad-hoc inspections of supervised entities;
- Thematic supervisory reviews, conducted either on a sector-wide basis and/or to assess specific internal controls of supervised entities (for example, CDD procedures and client risk classification frameworks).

A summary of supervisory measures applied by the AFSA in respect of DASPs as of the end of 2025 is presented in the table below.

Supervisory measures of the AFSA in relation to DASPs
(as of end-2025) (Table 7)

DASP inspections*	Thematic reviews**	Supervisory measures***
4	1	2

Note:
* Inspections may include a review of a wide range of issues related to compliance with AIFC Acts and, as a rule, include an assessment of the ML/TF/PF systems and controls of a specific DASP.
** Thematic reviews are conducted to assess compliance with AIFC Acts in a specific area (including ML/TF/PF). Thematic reviews typically cover a broad range of companies licenced in the AIFC.
*** Supervisory measures in this context include measures such as the suspension or revocation of a licence, or the withdrawal of the approval status of a senior officers subject to approval by the AFSA (AFSA).

Notably, during conducting the sectoral risk assessment, a thematic review of participants of the AFSA's regulatory sandbox was in progress, which included 17 (seventeen) DASPs. The thematic review was launched in 2025.
In addition to assessing compliance with other areas of the AIFC financial regulatory framework, the thematic review also covers compliance with customer due diligence (CDD) requirements in accordance with the AML/CTF/PF requirements of the AIFC and the Republic of Kazakhstan. As of the date of issuance of this questionnaire, the thematic review is ongoing.

4.2. Measures aimed at reducing vulnerabilities related to the technological features of Digital Assets

1) Measures to reduce vulnerabilities arising from the pseudo-anonymous/ anonymous nature of Digital Assets and crypto transactions

Due to the anonymous nature of certain DAs (e.g., DAs such as Monero) and the pseudo-anonymous nature of digital wallets within blockchain infrastructure[19], the AIFC regulatory acts have established the measures outlined below.

In particular, the anonymity of DA is mitigated through a prohibition on the use of anonymous tokens and anonymous devices, in accordance with Rule 2.15 of the AIFC Rules on Digital Asset Activities. In addition, incoming and outgoing digital asset transactions involving mixers are considered to have indicators of suspicious transactions and are subject to mandatory reporting by DASPs to the AFM of the RK, in accordance with Order No. 13 of the Agency for Financial Monitoring of the Republic of Kazakhstan.

Measures implemented by the AIFC to reduce vulnerabilities arising from the anonymity of DAs and the pseudonymity of digital wallets and crypto transactions also include:

[19] Digital wallets or public addresses on a blockchain consist of a sequence of alphanumeric characters and are not inherently linked to real-world identities.

- a requirement for DASPs to implement procedures for identifying senders and recipients of digital assets;
- a requirement for the identification of all trading participants;
- a requirement to implement client identification and verification tools and procedures (e.g., biometric identification, use of electronic digital signatures, video calls, and/or other measures) when establishing remote business relationships;
- a requirement for cryptoexchanges to conduct due diligence on digital assets themselves prior to admitting them to trading;
- a requirement to obtain approval from the AFSA for the admission of digital assets to trading;
- a requirement for DASPs to be knowledgeable about typologies and schemes involving the use of blockchain technology and digital assets for criminal purposes;
- a requirement to implement transaction monitoring to detect signs of suspicious transactions identified by the FATF;
- a requirement to establish systems and controls to determine the source of digital assets for incoming transactions and the destination of digital assets for outgoing transactions, in order to mitigate ML/TF risks;
- a requirement for AIFC DASPs to comply with the «Travel Rule» when conducting client transactions with other DASPs, as well as a requirement to establish ownership of a client's digital wallet (i.e., a non-custodial wallet) when DASPs transact directly with clients who are not customers of other DASPs.

2) Measures to reduce vulnerabilities related to the ease of use of Digital Assets

The measures aimed at reducing vulnerabilities associated with the ease of use of Das include the following:

- Limits on deposits by retail individual clients who are residents of the Republic of Kazakhstan, set at no more than USD 1,000 (one thousand) per calendar month;
- Limits established within the AFSA regulatory sandbox, applicable to both individual and legal entity clients; notably, the majority of DASPs (19 out of 29) hold regulatory sandbox licences;
- DASPs are not permitted to onboard legal entities that are residents of Kazakhstan, except for AIFC legal entities classified as professional clients, as well as DA miners and mining pools.

3) Measures to reduce vulnerabilities related to transaction irreversibility and security

Due to the technological characteristics of blockchain infrastructure, measures aimed at mitigating vulnerabilities related to the irreversibility of transactions are inherently limited. Nevertheless, a number of approaches exist to mitigate such vulnerabilities.

Given the decentralised nature of most DAs, the issue of transaction irreversibility remains relevant. At the same time, certain DAs, such as backed digital assets (e.g., stablecoins such as USDT and USDC) are issued by identifiable entities and operate within a framework that includes a centralised issuer. As a result, such assets may be frozen and returned to affected parties or seized in favor of the state in accordance with established legal procedures.

Notably, transaction volumes involving stablecoins are significant within the DA sector, and the above-mentioned freezing measures have been repeatedly applied by stablecoin issuers in practice.

Case

On 11 January 2025, Tether froze more than USD 182 million in its stablecoin USDT across five wallet addresses on the Tron blockchain.

Each wallet held approximately USD 12 million to USD 50 million in USDT.

This action was taken in line with Tether's voluntary wallet-freezing policy, which the company formalised in late 2023 to comply with the sanctions regime of the U.S. Treasury's Office of Foreign Assets Control (OFAC).

Under its Terms of Service, Tether reserves the right to freeze addresses or disclose user information if required by authorities or if the company deems such actions necessary.

USDT, the largest stablecoin by market capitalisation, is centrally issued and controlled, allowing Tether to render tokens unusable without directly seizing them.

The frozen USDT remain visible on the blockchain but cannot be transferred or redeemed for as long as the wallet addresses remain blacklisted.[20]

In addition, DAs may be frozen at the level of a DASP platform. In 2025, the share of transactions involving non-custodial wallets accounted for 24.80% of the total volume of inbound and outbound transactions, representing significant volumes. Taking into consideration the limited use of digital assets as a means of payment, criminals tend to rely on centralised DASP platforms.

As measures aimed at preventing, for example, the withdrawal of already deposited digital assets and enabling their freezing, it should be noted that DASPs are required to:

- establish the source of digital assets;
- prohibit the use of privacy-enhancing tools/devices, such as mixers; and
- submit reports to the AFM of RK when mixers are used, as such transactions are considered to have suspicious characteristics.

4) Measures aimed at reducing threats posed by foreign unlicenced platforms

[20] https://www.coindesk.com/markets/2026/01/12/tether-freezes-usd182-million-in-usdt-stablecoin-across-five-tron-blockchain-wallets

Measures of the AFSA with respect to foreign unlicenced platforms

(as of end-2025) (Table 8)

Requests to block websites	Requests to block mobile applications	Requests to restrict fiat transactions	Notifications sent to foreign DASPs regarding the cessation of unlawful activities
543	738	621	20

Blocking of websites and mobile applications of unlicensed DASPs

The AFSA carries out ongoing activities to identify unlicensed DASPs. As of the end of 2025, the AFSA submitted 543 requests to state authorities to block the websites of identified unlicensed cryptoexchanges.

In addition to facilitating the blocking of websites, the AFSA, in cooperation with state authorities, undertakes efforts to block mobile applications of unlicensed DASPs, as the use of mobile applications is a popular means of accessing unlicensed DASP platforms due to the widespread use of mobile devices. Accordingly, in 2025, the AFSA submitted to the relevant state body a list comprising 738 unlicensed DASPs for the purpose of subsequently blocking their mobile applications.

Furthermore, in order to block mobile applications of unlicensed DASPs, the AFSA filed a claim with the AIFC Court (AFSA v Persons Unknown) against nineteen unlicensed cryptoexchanges identified, based on cooperation with AIFC Participants, as being the most active in Kazakhstan.

The claim seeks a recognition that the activities of the operators of the aforementioned platforms are unlawful, and the imposition of a prohibition on providing unlicensed services to users in the Republic of Kazakhstan, including requirements imposed on major mobile application platform operators (application marketplaces) to remove or restrict access to the mobile applications of the relevant platforms for users in Kazakhstan.

Restrictions on fiat transactions with unlicensed DASPs

In addition, on 30 October 2024, the AFSA and the Agency for Regulation and Development of the Financial Market of the Republic of Kazakhstan (ARDFM) adopted a joint order establishing a procedure under which the AFSA provides lists of unlicensed DASPs to the ARDFM, for subsequent transmission to second-tier banks of the Republic of Kazakhstan, with the purpose of refusing to process fiat transactions in favor of unlicensed DASPs.

Following the adoption of this order, beginning in 2025, the AFSA has been submitting lists of unlicenced DASPs on a regular basis to the ARDFM. For example, at the end of 2025, the AFSA provided ARDFM with a list of mobile applications covering 621 DASPs.

Notifications to unlicenced DASPs on the cessation of unlawful activities

In addition, on 21 July 2025, the AFSA sent official notifications to 20 foreign cryptoexchanges, requiring them to cease providing digital asset services to residents of the Republic of Kazakhstan since they lacked an appropriate AIFC licence.

The notifications included:

(i) an explanation of requirements of digital asset regulatory framework, particularly regarding mandatory licensing;

(ii) a requirement to cease onboarding and servicing clients from Kazakhstan until an AIFC licence is obtained.

The notifications also outlined potential regulatory measures in the event of non-compliance with these requirements, including the restriction of access to the platforms within the territory of the Republic of Kazakhstan.

5) Measures aimed at mitigating vulnerabilities related to the cross-border nature of the Digital Asset sector

The key requirements aimed at mitigating vulnerabilities associated with the two main types of cross-border DA transactions are as follows:

Vulnerability related to transfers of digital assets between DASPs (including cross-border transactions) - mitigated through the requirement to comply with the «Travel Rule» in accordance with Sections 11-1 and 11-2 of the AIFC AML Rules. The key requirements include:

- conducting customer due diligence (CDD) on the receiving DASP;
- when transferring DAs to another DASP, accompanying the transfer with transaction-related information;
- for transactions exceeding USD 1,000, requesting and transmitting additional information.

Vulnerability related to transfers of digital assets between a DASP and a client using a non-custodial digital wallet - mitigated through the requirement to comply with Rule 11-1.2 of the AIFC AML Rules. The key requirements include:

- identification of the owner of the non-custodial wallet for DA transactions up to USD 1,000;
- for transactions exceeding USD 1,000, application of additional client identification measures based on a risk-based approach.

For the purposes of this assessment, compliance with the «Travel Rule» should be evaluated not only based on the formal inclusion of the requirement in DASP internal policies, but also on the actual operational effectiveness of the implemented measures, including:

- incorporation of «Travel Rule» requirements into DASP internal policies and procedures;

- implementation and/or use of technical solutions for «Travel Rule» messaging;
- methods used for the identification and verification of owners of non-custodial (self-custody or unhosted) digital asset wallets in DASP transactions with clients who use such wallets for DA deposits or withdrawals;
- the share of transactions rejected due to the inability to identify or verify the owner of a non-custodial wallet;
- specification by DASPs of a list of countries or counterparties with which «Travel Rule» messages cannot be transmitted.

As a result, 19 out of 29 DASPs have implemented the «Travel Rule» requirements set out in the AIFC AML Rules within their internal policies. In addition, DASPs sent 14,079 «Travel Rule» messages in 2024 and 20,605 messages in 2025. Furthermore, 16 DASPs (out of 29) confirmed the availability of external or internal software solutions that enable the secure transmission of «Travel Rule» messages.

4.3. Measures aimed at reducing vulnerabilities related to DASP activities

1) Measures to reduce client-related vulnerabilities

The client data presented above indicate that DASPs primarily focus on residents of the Republic of Kazakhstan, who accounted for 92% of the total number of clients as of the end of 2025. Despite the presence of clients from high-risk jurisdictions, it should be noted that the total number of clients from jurisdictions with elevated ML/TF/PF and sanctions risks is extremely limited, amounting to 0.057% of the total client base as of the end of 2025.

Although high-risk clients are present within DASP client bases, their share constitutes only 0.7% of total clients, which is also considered a low proportion.

As of the end of 2025, DASPs serviced 551 legal-entity clients, representing 0.3% of the total number of DASP clients. At the same time, only four legal-entity clients originated from high-risk jurisdictions, which is an insignificant figure. The share of individual clients remains predominant at 99.7%, and, as noted above, the majority of these clients are residents, which represents a lower inherent risk profile.

Accordingly, it is concluded that the predominant share of AIFC DASP clients consists of residents of Kazakhstan, while the proportion of non-resident clients from high-risk ML/TF/PF jurisdictions is negligible.

Supervisory activities have established that, overall, AIFC-licensed DASPs have implemented internal control measures. Specifically, DASPs have developed and approved Internal Control Rules (ICRs); appointed MLROs; established internal control systems within their organizations; and ensured effective interaction between business units and control functions.

DASP Internal Control Rules are reviewed by the AFSA during the licensing application process. Subsequently, DASPs update their internal policies to reflect amendments to AIFC legislation and the AML/CFT legislation of the Republic of Kazakhstan, or outcomes of regular business risk assessments.

As part of annual ML/TF/PF reporting, DASPs submit updated Internal Control Rules and other relevant policies and procedures.

In accordance with the AIFC AML Rules, DASPs conduct a business risk assessment of their activities; ML/TF/PF risk assessments of clients; Customer Due Diligence (CDD); and ongoing monitoring of client transactions and activities.

DASPs' CDD procedures include verification of the identity of the client and beneficial owner; obtaining and understanding information on the purpose and nature of the business relationship; assessment of the source of funds and source of wealth; and conducting ongoing CDD throughout the business relationship.

Case

An active DASP client carried out DA transactions in volumes inconsistent with the client's declared financial profile. In response to a request to confirm the source of funds, the client submitted a loan agreement with a legal entity. During verification, it was established that a loan agreement identical in structure and wording had previously been submitted by other clients, with the same organisation indicated as the counterparty. No documentary evidence confirming the actual transfer of funds was provided.

The materials were referred to the DASP's MLRO for an enhanced review. Based on the results of the assessment, taking into account the documentary similarities and the nature of the transactional activity, the responsible ML/TF/PF officer concluded that there were indicators of an organised money-laundering scheme. The client's transactions were temporarily restricted pending completion of the internal investigation.

MLRO decided to submit a suspicious transaction report (STR) to the Agency for Financial Monitoring of the Republic of Kazakhstan in accordance with established procedures. Subsequently, the competent authority initiated a criminal case, and the business relationship with the client was terminated due to an unacceptable level of risk.

2) Measures aimed at reducing vulnerabilities related to DASP products and services

DASPs, including cryptoexchanges licensed within the AIFC regulatory sandbox, are required to obtain approval for each DA prior to its admission to trading or use for the provision of other services. Both DASPs licensed under the regulatory sandbox regime and those operating under the full authorisation regime are required to conduct their own due diligence of DAs to ensure compliance with the criteria established by AIFC Acts,

including, inter alia: traceability using blockchain analytics tools; security of the underlying technology; volatility; and other relevant risk factors.

Cryptoexchanges and Providers of Money in relation to Digital Assets operating under the full authorisation regime are additionally required to obtain approval from the AFSA for the admission of certain types of digital assets.

As of the end of 2025, 21 DASPs (out of 29) confirmed the use of blockchain analytics tools. The vast majority of DASPs rely on third-party blockchain analytics service providers, such as Crystal, Elliptic, Chainalysis, AMLBot, Global Ledger, TRM Labs, and Scorechain. Other DASPs have not yet implemented blockchain analytics tools primarily due to ongoing preparatory work required to obtain authorisation to commence operations.

As of the end of 2025, a total of 113 digital assets were approved within the AIFC regulatory sandbox, while 10 digital assets were rejected. All approved digital assets are issued on public decentralised blockchains, which enables transaction traceability and thus significantly reduces the risk of misuse of digital assets traded on AIFC platforms for ML/TF/PF purposes.

In addition to approval for the admission of digital assets to trading or use, DASPs participating in the regulatory sandbox are required to obtain AFSA approval prior to launching any digital-asset-related service, which serves as an additional risk-mitigation mechanism. By contrast, DASPs operating under the full authorisation regime are required to conduct their own internal assessments, including a mandatory ML/TF/PF risk assessment of each digital-asset-related service prior to its launch.

Notably, as a risk-mitigation measure, all products and services are subject to ML/TF/PF risk assessment. These business risk assessments must be retained and submitted to the AFSA on an annual basis following the end of each calendar year.

Furthermore, the AIFC regulatory regime excludes the circulation of cash within the digital asset sector, which significantly reduces risks associated with the use and movement of cash, including risks relevant to the DA sector.

Special attention should also be given to the official AIFC market notice issued by the AFSA (AFSA NOTICE AFSA-F-NB-2024-0005), published in March 2024, which establishes AFSA's approach to various digital-asset-related products and services within the regulatory sandbox. In accordance with this notice, the launch of traditional peer-to-peer (P2P) digital asset trading services is not permitted, as such services pose high ML/TF and fraud risks due to direct fiat settlements between clients.

The aforementioned notice provides for a special regulatory approach to mitigate risks associated with P2P trading. As of the end of 2025, two cryptoexchanges had launched "regulated P2P trading" services within the AIFC.

3) Measures aimed at reducing vulnerabilities related to jurisdictional risks

In line with client-related risk-mitigation measures, AIFC DASPs' clients are predominantly residents of the Republic of Kazakhstan, while the share of non-resident clients from jurisdictions with elevated ML/TF/PF risk remains negligible.

To mitigate jurisdictional risks, DASPs conduct:

- business risk assessments;
- client ML/TF/PF risk assessments;

- Customer Due Diligence (CDD); and
- ongoing monitoring and periodic CDD.

During licensing and subsequently as part of supervisory activities (including inspections and thematic reviews), the AFSA assesses DASPs' methodologies for business risk assessment and client risk assessment with a focus on exposure to ML/TF/PF risks.

As noted above, DASPs do not conduct operations in foreign jurisdictions.

In accordance with the AIFC Acts, the following factors may increase jurisdictional risk and must be taken into account by DASPs in their activities:

- foreign countries/territories that do not implement or insufficiently implement FATF Recommendations;
- foreign countries/territories subject to United Nations Security Council sanctions;
- foreign countries/territories included in national lists of the Republic of Kazakhstan with preferential tax regimes;
- foreign countries/territories presenting high ML/TF risk due to factors such as levels of corruption, illicit production or trafficking of narcotic drugs, and information indicating support for international terrorism.

4) Measures aimed at reducing vulnerabilities related to service delivery channels

Heightened risks and vulnerabilities associated with the remote provision of digital-asset-related services are mitigated through the following regulatory requirements:

- under the Requirements on remote CDD, simplified CDD is not permitted for licensed AIFC financial companies, including AIFC DASPs;
- mandatory client identification and verification requirements as part of CDD;
- the requirements on remote CDD provide for the following client verification methods: telephone contact (welcome call), gathering biometric identification, fingerprinting verification, use of electronic digital signatures, and other methods.

The above regulatory requirements are assessed during authorisation and subsequently through supervisory procedures (e.g., scheduled or ad-hoc inspections). Accordingly, each DASP is required, as part of licensing, to:

- demonstrate its IT platform and the functioning of systems, including third-party solutions used for client verification;
- submit copies of outsourcing agreements concluded with third-party providers delivering identity verification services prior to launching services.

Notably, AIFC DASPs have implemented appropriate software solutions, typically through contractual arrangements with third-party providers.

Case

The DASP identified indicators of suspicious activity typologically consistent with the use of money mules/structuring (smurfing).

At the verification stage, it was established that the client used an email address and telephone number belonging to another individual, and also submitted a forged document to confirm the residential address (a statement from a second-tier bank of the Republic of Kazakhstan mobile application that had been altered and contained an address inconsistent with the data in the State Database of Individuals).

To enhance the review, a video call with audio and video recording was conducted. During the call, the client stated that he did not wish to open an account for a legal entity and intended to carry out transactions of a company and its clients "under the guise of his own", which further increased suspicions of an attempt to circumvent ML/TF requirements and to conceal the beneficial owner and/or source of funds.

Based on the results of the analysis, the DASP decided to refuse to establish a business relationship and prevented the execution of any transactions. Subsequently, the DASP submitted a relevant report to the Agency for Financial Monitoring of the Republic of Kazakhstan, describing the identified inconsistencies and the risk of the account being used as a "nominee" account.

5) Measures aimed at reducing vulnerabilities related to operational risks

1) Requirements for the appointment of authorised senior officers, such as Senior Executive Officer (CEO), Compliance Officer, Finance Officer (FO), Money Laundering Reporting Officer (MLRO), Chief Information Technology Officer (CITO).

In addition, DASPs operating within the AIFC regulatory sandbox are required to appoint a specialist responsible for data protection.

Specific AIFC requirements apply to each of these functions and are assessed by the AFSA in terms of relevant professional experience, qualifications, competence, and integrity.

2) Requirement to establish a board of directors for the company.

3) Requirement to establish systems and controls aimed at preventing: conflicts of interest; insider trading; deficiencies in risk management systems, including, but not limited to, ML/TF/PF risks, operational risks, reputational risks, legal risks, fraud risks, and business continuity risks.

AIFC measures to reduce vulnerabilities related to information security

Measures implemented by the AIFC to mitigate information security vulnerabilities include the following requirements:

- requirement for DASPs to implement appropriate software solutions;
- assessment and approval at the licensing stage;
- requirement to appoint an information security specialist responsible for the security of IT systems;
- requirement to conduct penetration testing of IT systems;
- ongoing monitoring of DASP activities;
- requirement for DASPs to implement cybersecurity policies and procedures;

- requirement for DASPs to implement systems and controls ensuring the secure use of private keys and digital wallets.

In addition, an important mitigating factor for information security risks is the requirement applicable to all DASPs to conduct IT audits by an independent, qualified third party.

Within the framework of AFSA supervisory practice, DASPs have demonstrated compliance with internationally recognised information security standards, including ISO 27001, ISO 27701, Cyber Essentials, and others.

Measures Implemented by DASPs

Preventative Measures of DASPs

The core measures for preventing threats include business risk assessment systems, client ML/TF risk assessment, CDD during onboarding, periodic CDD, and ongoing transaction monitoring. The above-mentioned systems and controls are reviewed by the AFSA during the DASP licensing process and subsequently as part of supervisory activities. In addition, prior to commencing operations, DASPs provide copies of contracts concluded with third-party providers of client verification solutions and blockchain analytics tools.
It should also be noted that, following the results of the sectoral risk assessment and the entry into force of detailed requirements for compliance with the «Travel Rule», 16 DASPs (out of a total of 29) confirmed the availability of external or internal software solutions enabling the secure exchange of «Travel Rule» messages. At the same time, 9 DASPs are at the preparatory stage, including the process of selecting an external provider or implementing an internal solution. Finally, 4 AIFC DASPs rely on cryptoexchange solutions for the transmission of «Travel Rule» messages, as such exchanges are the primary counterparties of these DASPs due to the custodial storage of digital assets on platforms of cryptoexchanges.

As part of «Travel Rule» compliance, AIFC DASPs exchanged messages with other DASPs, including foreign DASPs, in 2024 and 2025, as reflected in Table 9 below. The data demonstrates a growing trend in the number of messages transmitted. «Travel Rule» messaging serves as an additional preventive measure and enhances transaction transparency when using blockchain technology.

«Travel Rule» reports in 2024 and 2025 *(Table 9)*

Type of report	2024	2025
Reports submitted by DASPs under «Travel Rule» requirement	**14 079**	**20 605**

DASP measures aimed at detection

Taking into account the requirement to submit reports on suspicious activities and suspicious transactions, AIFC-licensed Digital Asset Service Providers (DASPs) submitted a significant number of reports to the authorised bodies, as reflected in the table below.

In addition, in 2025, amendments were introduced to the Law of the Republic of Kazakhstan on ML/TF, pursuant to which DASPs are required to submit reports on threshold transactions conducted directly using digital assets. Statistics on threshold transaction reports (TTRs) submitted by DASPs to the authorised bodies for 2024 and 2025 are presented in Table 10 below. The increase in DASP transaction volumes correlates with the growth in the number of reported threshold transactions.

Furthermore, according to information received from DASPs within the framework of the sectoral risk assessment, DASPs collectively received 583 requests from law enforcement authorities of the Republic of Kazakhstan and foreign jurisdictions in 2024, and 1,344 requests in 2025.

Reports submitted by DASPs on suspicious activities/transactions (SAR/STR) and threshold transactions (TTR), as well as requests from law enforcement authorities to DASPs in 2024 and 2025

(Table 10)

STR/SAR/TTR and law enforcement requests	2024	2025
STR/SAR	118	344
TTR	598	1876
Requests from law enforcement authorities and from foreign authorities to DASPs	583	1344

Case

On an AIFC-licensed cryptoexchange platform, multiple cases were identified involving attempts to pass KYC/CDD verification using identity documents belonging to third parties.

During the identification process, prospective clients uploaded documents of other individuals, after which the biometric verification system (liveness check) detected a mismatch between the photograph in the document and the person undergoing verification.

In other cases, conversely, clients submitted their own identity documents, while the biometric verification was completed by a different individual.

The identification system automatically rejected such verification attempts due to detected inconsistencies and indicators of identity misuse.

In accordance with the DASP's internal ML/TF policy, these actions were classified as the submission of false information and an attempt to use another person's identity during registration.

In such cases, the DASP decided to refuse the establishment of a business relationship. In addition, given the presence of suspicious activity indicators, the DASP also decided to submit suspicious activity/transaction reports (STRs) to the Agency for Financial Monitoring of the Republic of Kazakhstan.

Corrective Measures Implemented by DASPs

As corrective measures aimed at addressing identified risks, the following actions taken by DASPs should be highlighted:

- Freezing of digital assets and other assets was carried out in 1,741 cases, either on the DASP's own initiative or at the request of law enforcement authorities;

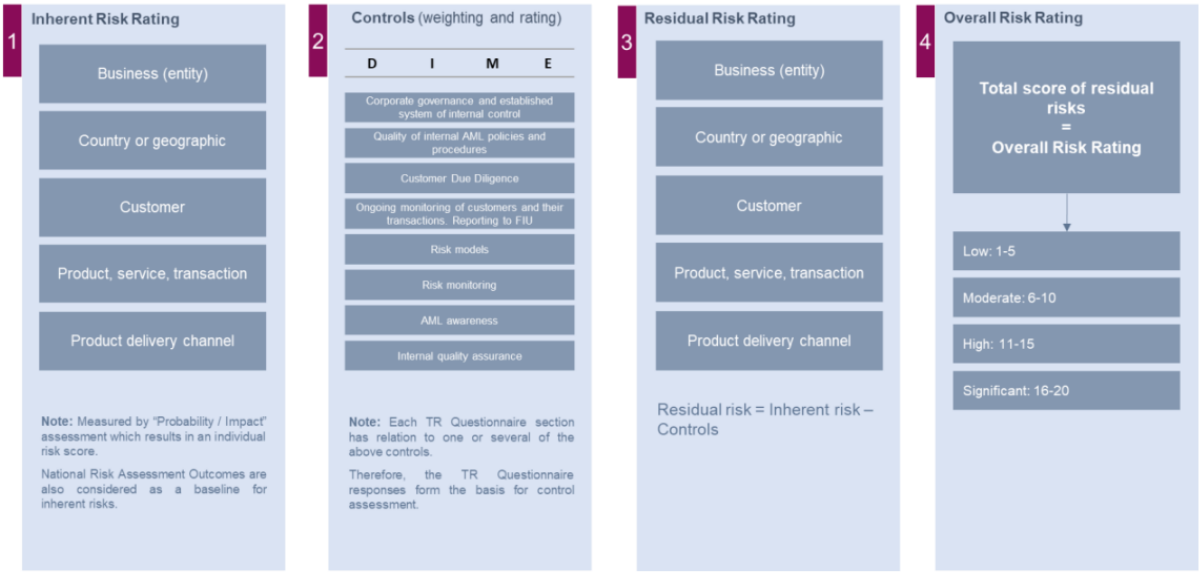
- The share of client transactions rejected due to the inability to identify or verify the owner of a non-custodial (unhosted) digital wallet amounted to 4%.

ONGOING MONITORING OF ML/TF/PF RISKS

In order to ensure adequate and timely supervisory measures, the AFSA (AFSA) conducts continuous monitoring of the risk levels of AIFC Participants. When assessing individual DASPs or specific digital-asset-related products, services, or activities, the AFSA takes into account: the risk level associated with DASP products and services; business models; corporate governance frameworks; financial information; delivery channels; characteristics of the client base; geographical footprint and countries of operation; the degree of implementation by DASPs of ML/TF/PF measures; as well as risks associated with specific DA-based products that may potentially obscure transactions or reduce the ability of DASPs and supervisory authorities to apply effective ML/TF/PF controls.

The AFSA also pays particular attention to the control measures implemented by DASPs, including: the quality of risk management policies and procedures; the effective functioning of internal control mechanisms.

In addition, AFSA takes into account information on: the professional competence and integrity of DASP senior management; the qualifications and independence of ML/TF/PF responsible officers; the existence and effectiveness of compliance functions and internal audit arrangements.



The AFSA applies an AML/CTF risk assessment model (the "Model") designed to identify and assess money laundering and terrorist financing (ML/TF) risks from a supervisory perspective, ensuring the application of a risk-based approach to AML/CTF supervision.

The Model applies a widely accepted international formula for calculating residual risk:

INHERENT RISK – CONTROLS = RESIDUAL RISK,

which is determined and measured using a probability-and-impact matrix.
The Model assesses inherent vulnerability across five (5) key ML/TF risk factors:

- business (legal entity) risk;
- country or geographic risk;
- client risk;
- product, service, or transaction risk;
- delivery channel risk (product or service).

Each factor, in turn, comprises a number of sub-factors (red flags) that influence the final risk assessment. The AML/CTF risk factors within the Model incorporate red flags relevant to money laundering, terrorist financing, fraud, corruption, and sanctions risks.
To arrive at the overall residual risk rating, the Model evaluates the control environment in terms of its:

- Design (D),
- Implementation (I),
- Monitoring (M), and
- Evaluation (E)

(the "DIME" framework).

The Model identifies eight (8) core Controls aimed at reducing the level of inherent ML/TF risk. Each Control is individually weighted using the DIME risk assessment methodology.

For each Control, every DIME criterion is assigned a score from 0 to 3. The scores are then aggregated and expressed as a percentage of the maximum possible control score (12 = 100%). The overall Control score is calculated as the arithmetic mean of the summed values. This process is repeated for each Control, after which the overall Controls score is calculated as the arithmetic means of all Control scores.

Subsequently, the residual risk level for each risk factor is calculated using a matrix combining inherent risks and Controls.

Finally, all residual risk scores are aggregated, and based on these results, the overall risk level of the DASP is determined.

4.4. Measures Aimed at Reducing Vulnerabilities of the Traditional Financial Sector Resulting from Exposure to Risks from Digital Assets and DASPs

Banking Sector

The banking sector of Kazakhstan serves as the primary fiat gateway for the AIFC DASP sector. In order to ensure the safe integration of fiat channels with DASPs, a Pilot Project was implemented to test and validate interactions between DASPs and Kazakhstan's banks. In turn, DASPs participating in the Pilot Project tested their products within the AIFC regulatory sandbox, subject to investment limits, fund custody restrictions, and other regulatory limitations and prohibitions.

Following the successful implementation of the Pilot Project, the AFSA adopted the Rules on Cooperation in 2024. Taking into consideration that banks of the Republic of Kazakhstan are supervised by national financial regulators, the Rules on Cooperation were developed in coordination with the National Bank of Kazakhstan and the Agency for Regulation and Development of the Financial Market (ARDFM).

To mitigate money laundering and terrorist financing (ML/TF) risks, the following key requirements are established for Kazakhstan's banks under the Rules on Cooperation:

- monitoring and control of fiat transactions involving DASPs and DAs;
- assessment by banks of ML/TF risks associated with DASPs;
- application of enhanced CDD for fiat transactions involving digital assets equal to or exceeding USD 1,000;
- a prohibition on third-party deposits and withdrawals;
- information exchange between DASPs and banks to ensure transaction security;
- limitation of cooperation exclusively to Kazakhstan's banks and the National Postal Operator; accordingly, as of the end of 2025, DASPs were not permitted to interact with payment organisations registered in Kazakhstan.

In addition, certain provisions of the regulatory framework further contribute to reducing vulnerabilities within the banking sector:

- resident legal entities of the Republic of Kazakhstan are not permitted to conduct fiat transactions involving DAs through DASPs, except for AIFC legal entities classified as professional clients, as well as miners and mining pools;
- DASPs are required to implement effective systems and controls (including monitoring mechanisms) to prevent retail individual clients-residents of Kazakhstan from depositing more than USD 1,000 within a single calendar month.

Interaction of AIFC DASPs with the banking and payment system of Kazakhstan *(Fig. 6)*

Combination of traditional financial services of AIFC Participants with Digital Asset services

The measures implemented by the AFSA and the measures and controls applied by AIFC Participants to mitigate vulnerabilities and risks related to digital assets DAs and DASPs are consistent with and broadly aligned to the risk-mitigation measures described above with respect to the DA and DASP sector.

5. METHODOLOGY FOR ASSESSING ML/TF/PF RISKS IN THE SECTORAL RISK ASSESSMENT OF THE DA/DASP SECTOR

AFSA applies a risk assessment model based on the classical risk assessment equation:

Inherent Risk *(consisting of threats and vulnerabilities)* **– Controls = Residual Risk**

When conducting this sectoral risk assessment of the DA and DASP sector for 2024 and 2025, the AFSA took into account the FATF Guidance on Assessing Money Laundering Risks Related to Virtual Assets and Virtual Asset Service Providers.[21]

1) Identification of the risk environment:

Risk environment = inherent sector risk, which consists of threats and vulnerabilities.

At the initial stage, the level of risk arising from threats ML/TF/PF and vulnerabilities is assessed separately, including:

- vulnerabilities related to DAs;
- vulnerabilities related to DASPs; and
- vulnerabilities of the traditional financial sector arising from interactions with the DA and DASP sector.

The results of the assessment of threat and vulnerability risk levels are subsequently used to determine the inherent ML/TF/PF risk in accordance with the risk matrix presented in Table 11.

Inherent ML/TF/PF risk matrix

(Table 11)

	Vulnerability			
Threat	**Low**	**Medium**	**High**	**Significant**
Low	**Low**	**Low**	**Medium**	**Medium**
Medium	**Low**	**Medium**	**High**	**High**
High	**Medium**	**High**	**High**	**Significant**
Significant	**Medium**	**High**	**Significant**	**Significant**

2) The second step involves identifying controls or measures aimed at mitigating inherent risks, including threats and vulnerabilities.

[21] Quick guide on assessing the Money Laundering risks of virtual assets (VA) and virtual asset service providers (VASP), https://www.fatf-gafi.org/en/publications/Methodsandtrends/quick-guide-on-assessing-ML-risks-of-VA-and-VASPs.html

3) The results of the assessment of inherent risk levels and controls are then used to determine the residual risk in accordance with the risk matrix set out in Table 11.

Residual ML/TF/PF risk matrix

(Table 12)

	Control			
Inherent risk	**Efficient**	**Sufficiently effective**	**Partly efficient**	**Inefficient**
Significant	**Medium**	High	**Significant**	**Significant**
High	Medium	Medium	**Significant**	**Significant**
Medium	**Low**	Medium	High	**Significant**
Low	**Low**	**Low**	Medium	High

Hierarchy of evidence and level of assurance in the assessment

In conducting the sectoral assessment, the AFSA applies a multi-source approach and differentiates sources by their degree of reliability. The highest weight is assigned to: (i) regulatory and supervisory data of the AIFC; (ii) official materials of the competent authorities of the Republic of Kazakhstan; (iii) STR/SAR/TTR reports and other data from reporting entities; (iv) international standards and reports of FATF, IOSCO, the World Bank, and other international organizations; (v) analytics from blockchain analytics providers and publicly available industry reports; and (vi) media and other open-source materials.

For each final risk rating, a level of data reliability is additionally determined, depending on data completeness, the availability of local case studies, the consistency of statistical data, and the degree to which the assessment relies on external typologies. This is particularly important for cross-border risks, offshore reporting entities, terrorist financing, proliferation financing, non-custodial risks, and other areas with limited observability.

Limitations of the assessment

This sectoral assessment assumes that certain risks within the DA/DASP sector are cross-border, concealed, and rapidly evolving in nature. This applies, in particular, to offshore DASPs, transactions involving non-custodial wallets, OTC intermediaries, transactions using multiple blockchains (chain hopping), and obfuscation services. Accordingly, the absence of identified local cases should not automatically be interpreted as indicating gaps in the assessment.

Furthermore, the assessment of certain risks may be complex or subject to limited reliability due to, for example, the decentralised nature of blockchain technology. In addition, some quantitative indicators of the sector are constrained by the fact that a significant number of licensed DASPs are not yet fully operational. For this reason, the

results of the assessment are subject to regular updates as supervisory data, STR/SAR/TTR reports, law enforcement data, and international typologies continue to accumulate.

6. OVERALL ASSESSMENT OF THREATS, VULNERABILITIES, AND RISK LEVELS

Thus, based on the analysis of the current situation, the **inherent risks** related to achieving ML/TF/PF objectives in the DA and DASP sector, taking into account the **level of threats and the existence of vulnerabilities**, are assessed as **significant**. DAs possess a number of attractive characteristics that may be exploited by criminals for ML/TF/PF purposes. The use of DAs is widely accessible, can be carried out through various means and/or at relatively low cost, and is considered attractive and relatively safe, while requiring limited planning, knowledge, or technical expertise.

At the same time, the risk-mitigation measures implemented-both through preventive and supervisory procedures of the AIFC and through DASPs' compliance with AIFC internal control requirements-allow for a substantial reduction of inherent risks. Consequently, taking into account the **effectiveness of risk-mitigation measures**, the vulnerability of the AIFC to involvement in ML/TF/PF schemes is assessed as low, while the **residual risk** level of DASPs operating within the AIFC is assessed as **MEDIUM.**

Within the scope of the activities considered, the AIFC has established deterrent measures and control mechanisms that enable effective prevention of money laundering and terrorist financing. In addition to the measures outlined above, the following characteristics contribute to reducing risks in the DA sector within the AIFC:

- the presence of continuous supervision over the activities of companies;
- restrictions on cash transactions;
- a significant number of licenced DASPs that had not commenced DA operations as of the end of 2025;
- reliance primarily on secure and/or controlled delivery channels;
- effective management of new technologies and/or new payment methods;
- a client base consisting predominantly of residents of Kazakhstan;
- a relatively small number of clients located in jurisdictions identified as high-risk.

Conclusion

The scale of the AIFC DA sector, the identification and understanding of existing threats and vulnerabilities, and the application of measures aligned with international best practices and FATF requirements, support the conclusion that the sector is characterised by a **significant level of inherent risk**, **effective controls**, and an overall **medium level of residual risk** related to the potential use of the DA sector for ML/TF/PF purposes.

The results of the sectoral risk assessment are used by the AIFC in the context of its ongoing supervisory activities. Specifically, based on the findings, measures are developed and implemented to eliminate and mitigate ML/TF/PF risks, including determination of the scope and frequency of supervisory actions, the development of risk management strategies, and the adoption of measures encompassing risk prevention, deterrence, and mitigation, as well as remediation plans.

Such measures include, inter alia: increased frequency of updates regarding the number and quality of company clients; enhanced regulatory oversight; implementation of risk-based supervision (desk-based reviews, on-site inspections, and thematic reviews); initiatives to enhance the awareness and expertise of ML/TF/PF and compliance-responsible personnel; regular engagement with supervised entities; delivery of training and awareness-raising activities; regular dissemination of typology reports and ML/TF/PF risk indicators to sector participants; strengthened cooperation with law enforcement authorities, and other relevant measures.