FIU
وحدة المعلومات المالية
Financial Intelligence Unit

Misuse of Virtual Assets in Financial Crime

Evolving Trends and Risks

Research and Strategic Analysis Section

December 2025

UAE Financial Intelligence Unit

www.uaefiu.gov.ae

Disclaimer

For any enquiries regarding this document, please contact rsas@uaefiu.gov.ae

TABLE OF CONTENTS

LIST OF ACRONYMS

ADGM	Abu Dhabi Global Market
AI	Artificial Intelligence
AML	Anti-Money Laundering
BTC	Bitcoin
CBUAE	Central Bank of the UAE
CFT	Combating the Financing of Terrorism
CPF	Combating Proliferation Financing
DeFi	Decentralized Finance
DEX	Decentralized Exchange
DFSA	Dubai Financial Services Authority
DIFC	Dubai International Financial Centre
ETH	Ether (the native cryptocurrency of the Ethereum blockchain platform)
FATF	Financial Action Task Force
FIs	Financial Institutions
FIUs	Financial Intelligence Units
FSRA	Financial Services Regulatory Authority
ICO	Initial Coin Offering
IEMS	Integrated Enquiry Management System
KYB	Know Your Business
KYC	Know Your Customer
KYT	Know Your Transaction
LEA	Law Enforcement Authority
LP	Legal Person
ML	Money Laundering
NFT	Non-Fungible Token
NP	Natural Person
NRA	National Risk Assessment
OCG	Organized Crime Group
OSINT	Open-Source Intelligence
OTC	Over-the-Counter
P2P	Peer-to-Peer
RE	Reporting Entity
RFR	Reason for Reporting
R.15	Recommendation 15
SAR	Suspicious Activity Report
SCA	Securities and Commodities Authority
SOF	Source Of Fund
SOW	Source Of Wealth
STR	Suspicious Transaction Report

TF	Terrorist Financing
UAE	United Arab Emirates
UAEFIU	UAE Financial Intelligence Unit
USDC	USD Coin
USDT	USD Tether
VA	Virtual Asset
VARA	Dubai Virtual Assets Regulatory Authority
VASP	Virtual Asset Service Provider

EXECUTIVE SUMMARY

Virtual assets (VAs) are now integral components of modern financial systems, offering high transaction speeds and broad accessibility. Despite these advantages, VAs present substantial risks because their ecosystems are vulnerable to criminal exploitation. As with traditional payment methods, which have been misused by criminal organizations for decades, virtual assets are increasingly used in illicit activities. This trend is primarily driven by the rapid movement of assets, cross-border capabilities, and advanced privacy features associated with VAs.

The second UAE National Risk Assessment (NRA), completed in 2024, assessed that the virtual assets sector faces a high level of exposure to money laundering and is also vulnerable to misuse by terrorist groups. The UAE Financial Intelligence Unit (UAEFIU) employs diverse data sources to identify typologies and trends related to the misuse of VAs and virtual asset service providers (VASPs), as well as other relevant risk factors. Since the 2021 amendment to the UAE legal framework expanded the anti-money laundering (AML) and combating the financing of terrorism (CFT) requirements to the VA sector, registered entities on goAML associated with virtual asset services have submitted over 4,000 suspicious reports to the UAEFIU as of June 2025. The data analyzed in this report includes a comprehensive review of 804 Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) received from reporting entities between 01/07/2023 and 30/06/2025, with a focus on blockchain tracing.

The analysis also reviewed intelligence reports exchanged with counterpart Financial Intelligence Units (FIUs) concerning VA-related crimes, as well as cases disseminated to or initiated by law enforcement authorities (LEAs). Additional insights were gathered from focus group discussions and a questionnaire distributed to VASPs and the banking sector.

The analysis findings identified fraud as the most prevalent risk, encompassing investment and Ponzi schemes, employment and task scams, romance fraud (romance baiting), and website mirroring. Criminals and suspected organized crime groups (OCGs) employed increasingly sophisticated techniques, such as forged identification documents, AI-generated IDs and passports, and the use of stolen or unauthorized bank cards. Third-party control of customer transactions and the use of mule accounts, primarily involving blue-collar workers and students, were also frequently observed in reported fraud cases. Many transactions traced by the UAEFIU were linked to fraud shops and scam wallets on the blockchain.

Online illegal gambling has emerged as a frequently reported concern among VASPs and the banking sector. Analysis of relevant STRs and SARs indicates that a growing number of UAE residents are using virtual assets to make payments to online gambling platforms operating outside the UAE.

Analysis of STRs and SARs also revealed varying levels of exposure to high-risk wallets, including those associated with illicit organizations, stolen funds, and darknet markets. Additionally, several subjects of these reports were suspected of engaging in direct or indirect transactions with sanctioned entities (clusters) or proxies of sanctioned jurisdictions by foreign regimes.

In the context of high-risk wallets, analysis of STRs and SARs reported by VASPs indicated that assets were sometimes routed through several intermediaries to wallets labeled as terrorist fundraising or included on seizure lists, as identified through tracing tools or open-source intelligence (OSINT). However, these instances occurred less frequently than other typologies described above.

It is globally recognized (FATF, 2025) that criminals increasingly favor decentralized exchanges (DEX), which lack the due diligence requirements of centralized, regulated exchanges. UAEFIU analysis of STRs reported by VASPs identified more complex techniques employed by subjects, including the use of decentralized finance (DeFi) platforms,[1] DEXs, over-the-counter (OTC) services,[2] mixers, and cross-chain bridges. In particular, suspected money laundering cases frequently involved structuring and layering of virtual assets through the peel-chain technique[3], as well as swapping and cross-chain services[4] to obscure the origin or beneficial ownership.

The use of unlicensed virtual asset service providers and (crypto) hawala services continues to be observed in the reported STRs/SARs to the UAEFIU. Peer-to-Peer (P2P) transactions were also observed involving individuals using their personal accounts to conduct high-volume crypto trading, either for themselves or on behalf of others. Unlicensed individual brokers may have conducted some of these P2P transactions.

The data analyzed in this report also demonstrate a shift toward the use of stablecoins,[5] particularly USDT on the Tron network,[6] which was the most frequently observed currency in the examined suspicious reports and in responses to the UAEFIU questionnaire. Swapping various cryptocurrencies for stablecoins (USDT and USDC) was common in multiple STRs reviewed.

Data collected from focus group discussions and the UAEFIU questionnaire identified several challenges in effectively disrupting criminal activities. These include inconsistent implementation of Travel Rule requirements globally and a lack of readiness and expertise among VASP counterparts. The report proposes various solutions to address these challenges, emphasizing the need for investment in technology and advanced forensic tools, capacity building, international cooperation, intelligence sharing, and more active public-private partnerships at both national and global levels.

[1] DeFi (Decentralized Finance) is the broad ecosystem of blockchain-based financial services (lending, borrowing, investing) without banks, while a DEX (Decentralized Exchange) is a specific type of application within DeFi that allows peer-to-peer crypto trading via smart contracts, acting as a marketplace for swapping assets without intermediaries, making DEXs a crucial component of the larger DeFi world.

[2] Over-the-counter refers to buying and selling cryptocurrencies directly between parties, often peer-to-peer through private trades, rather than using conventional or centralized exchange platforms.

[3] The peel chain technique is a method primarily associated with cryptocurrency money laundering in which large amounts of illicit funds are broken down and transferred through a long series of transactions across multiple wallets to obscure their origin (similar to layering in traditional finance).

[4] Cross-chain swaps allow users to trade tokens from one blockchain to another in a single transaction. These services enable direct exchanges across blockchains by using smart contracts and bridging protocols.

[5] Stablecoins are cryptocurrencies designed to maintain a stable value, typically by being pegged to a fiat currency (e.g., the U.S. dollar), a commodity, or a financial instrument, offering a less volatile alternative to other cryptocurrencies.

[6] Tron is a decentralized proof-of-stake blockchain with smart contract functionality, designed for building applications focused on content sharing and digital entertainment. Its native cryptocurrency, TRX (Tronix), supports network transactions, payments, and token issuance.

Lastly, the UAEFIU has also developed a list of risk indicators for VASPs, the banking sector, and other stakeholders to facilitate the detection, reporting, and investigation of misuse of virtual assets.

Executive Summary Illustration

Top frequent illegal activities associated with VAs in the examined data

		
Fraud	Illegal gambling	Money laundering

Other observed concerns

			
Sanction circumvention	Market manipulation	TF crowdfunding	Exposure to high-risk wallets

Most frequently observed currency

Stablecoins

Involved techniques and methods (with different frequency levels)

			
Identity theft/fabricated IDs and Passports	Stolen bank cards/credentials	Employment of money mule	Peer-to-Peer (P2P)
			
Unlicensed crypto brokers	Unlicensed VASPs	Over-the-counter (OTC) services	DeFi platforms
			
Mixers	Cross-Chain bridges	Asset swapping	Peel-Chain

1. INTRODUCTION

There is a global perception that by 2028, only 9% of all payments will be made in physical currency (World Economic Forum, 2023).[7] With such apprehension, there is increased interest in shifting to virtual assets (VAs) instead of traditional fiat currency for more convenient and reliable transactions, reshaping how value is created, transferred, and stored outside the traditional financial system. However, the same attributes that make VAs attractive for legitimate investment and trade opportunities also introduce new challenges: a financial system without a central authority allows for the movement of illicit funds, namely proceeds of crime, proliferation, and terrorist financing.[8]

The earliest identified concept of digital money was 'blinded cash' (or eCash) in 1983, which enabled users to receive digital money from banks privately and securely using cryptography. Later, the notion of cryptocurrency was introduced with little success until 2009, when Bitcoin was introduced based on a white paper by an unknown person or group under the alias Satoshi Nakamoto. This paper describes the peer-to-peer (P2P) network and unique blocks that make up the blockchain, overcoming the hurdles faced by other digital assets.[9]

Virtual assets (VAs) are defined as digital representations of value that can be traded, transferred, and used for payment or investment purposes, excluding digital representations of fiat currencies, securities, or other funds. Virtual Asset Service Providers (VASPs) are those natural or legal persons conducting virtual asset activities or transactions as a commercial activity on behalf of or for the benefit of another person (Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing).[10]

In October 2018, the Financial Action Task Force (FATF) expanded its global standards on anti-money laundering and combatting the financing of terrorism (AML/CFT) to include VAs and VASPs by updating Recommendation 15 (R.15). In response, the UAE incorporated specific provisions on virtual assets into its AML/CFT legal framework through Federal Decree-law No. (26) of 2021 to align with FATF requirements.[11] Additionally, the UAE Financial Intelligence Unit (UAEFIU) published its first typology report on the misuse of virtual assets in 2021, highlighting key methods used in financial crime.[12]

[7] World Economic Forum (2023) "By 2028, just 9% of all payments will be made in physical currency – but we may miss it". Available at: https://www.weforum.org/stories/2023/09/digital-currencies-privacy-freedom/

[8] Aldasoro, I., Frost, J., Lim, S.H., Perez-Cruz, F. and Shin, H.S. (2025) An Approach to Anti-Money Laundering Compliance for Cryptoassets. Bank for International Settlements, Basel. Available at: https://www.bis.org/publ/bisbull111.pdf

[9] Bitcoin and Blockchain (2020) History and Current Applications. Available at: https://www.researchgate.net/publication/340682224_Bitcoin_and_Blockchain_History_and_Current_Applications

[10] UAE Legislation (2025) Federal Decree by Law Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing. Available at: https://uaelegislation.gov.ae/en/legislations/3314

[11] Federal Decree Law No. (26) of 2021 was issued amending some provisions of Federal Decree Law No. (20) of 2018. Available at: www.uaefiu.gov.ae/media/qh3kh12e/federal-decree-law-26-of-2021-amending-federal-decree-law-20-of-2018-amlcft-en.pdf

[12] UAEFIU (2021) Strategic Analysis on Virtual Assets. Available at: https://www.uaefiu.gov.ae/en/more/knowledge-centre/publications/trends-typology-reports/strategic-analysis-on-virtual-assets/

Since then, the virtual assets ecosystem has achieved broader acceptance and undergone significant changes in digital infrastructure, financial services, and regulatory frameworks. Concurrently, criminal schemes have evolved, employing increasingly sophisticated methods that exploit technological advancements and sector vulnerabilities worldwide. Subsequently, the UAE updated its legislation on Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT), and Combating Proliferation Financing (CPF) through Federal Decree Law No. (10) of 2025 to address these advanced criminal techniques, including complex illicit activities involving virtual assets.

Furthermore, the UAE has established a comprehensive multi-agency supervisory structure, with various supervisory and regulatory authorities overseeing the virtual assets market and VASP activities through risk-based supervision aligned with FATF standards. The Securities and Commodities Authority (SCA) licenses and supervises investment-related virtual asset activities on the UAE mainland, including exchanges, brokerage, custody services, trading platforms, and other investment services. In Dubai (excluding the Dubai International Financial Centre), the Dubai Virtual Assets Regulatory Authority (VARA) acts as the local regulator for VASPs under a delegated federal framework. The Financial Services Regulatory Authority (FSRA) of Abu Dhabi Global Market (ADGM) and the Dubai Financial Services Authority (DFSA) oversee virtual asset activities within their respective financial free zones. The Central Bank of UAE (CBUAE) regulates tokens used for payment purposes. Collectively, these authorities ensure consistent and coordinated oversight of the virtual asset sector across the UAE.

With the implementation of sound regulation and a crypto-friendly ecosystem, the UAE has emerged as a leading jurisdiction in the MENA, offering comprehensive licensing regimes and advanced compliance frameworks, with an estimated 30% adoption of cryptocurrency in the region.[13] Another estimate indicated that the UAE economy received upward of $56 billion in 2024 to 2025, placing the country at the second-largest market in the MENA after Türkiye. It is also observed that the UAE's cryptocurrency ecosystem shifted from an investment vehicle to a practical payment solution, driven by robust growth in merchant services across retail segments.[14]

Despite attracting substantial investment, the sector remains vulnerable to criminal misuse. In 2020, Chainalysis, as referenced by Interpol, estimated that $11.5 billion in cryptocurrency transactions were linked to illegal activity globally, accounting for approximately 1% of total cryptocurrency transaction volume at that time (Chainalysis, 2020; Interpol, 2020).[15] TRM (2023) reported that criminals may have

[13] Crystal Intelligence (2024) Navigating Crypto Regulation and Risk in the MENA Region: A Guide for Regulators and Compliance Professionals REPORT. Available at: https://crystalintelligence.com/crypto-regulations/crypto-regulation-and-risk-in-mena-trends-risks-and-regional-breakdown/

[14] Chainalysis (2025) The 2025 Geography of Crypto Report. Available at: https://go.chainalysis.com/2025-geography-of-cryptocurrency-report.html

[15] Interpol (2020) Combatting Cyber-enabled Financial Crimes in the era of Virtual Asset and Darknet Service Providers; and Chainalysis (2020) Crypto Crime Report. Available at: https://www.chainalysis.com/blog/cryptocurrency-crime-2020-report/

handled over $34 billion in cryptocurrencies in 2023.[16] Elliptic (2025) estimates that criminals are moving more than $21 billion in cryptoassets globally through cross-chain money laundering techniques, particularly within the DeFi ecosystem, to transfer funds rapidly across assets and blockchains.[17] Chainalysis (2025) further estimated that illicit cryptocurrency addresses received $40.9 billion in 2024, representing a decrease to 0.14% of total on-chain transaction volume.[18]

Earlier typologies of illicit actors in the virtual asset ecosystem included cybercrime, fraud (notably investment and romance scams), the use of dark web markets, and the employment of privacy tools and coins, such as mixers and noncompliant VASPs, to obscure fund flows.[19] Although these typologies remain pertinent, their scale and sophistication have increased significantly, supporting a broader range of threats from national security risks to consumer protection concerns. This evolution has resulted in a more diverse and professionalized landscape, particularly among organized crime groups.[20]

Emerging typologies include the use of artificial intelligence (AI) in virtual asset scams and fraud, increasingly sophisticated incidents of stolen funds and ransomware, the proliferation of stablecoin activity among sanctioned actors, and the growing complexity of cross-chain money laundering. Criminals and organized crime groups (OCGs) continue to employ virtual assets for money laundering and a wide range of predicate offenses, including illegal gambling, drug trafficking, and various fraud schemes.[21] There has been a notable increase in the professionalization of scammers globally, with the rise of investment and romance schemes and the development of scam-as-a-service operations.[22] Additionally, terrorist groups also continue to use virtual assets, particularly stablecoins, to raise and transfer funds across jurisdictions.[23] The Egmont Group of Financial Intelligence Units (2023) reported that 29% of FIUs have identified cases linking virtual assets to terrorist financing.[24]

With the rise in popularity of decentralized finance (DeFi) networks, new coins, tokens, smart contracts, Initial Coin Offerings (ICOs), and Non-Fungible Tokens (NFTs) have emerged, supported by both

[16] TRM (2023) The Illicit Crypto Economy: Key Trends from 2023. Available at: https://www.trmlabs.com/reports-and-whitepapers/the-illicit-crypto-economy-2023

[17] Elliptic (2025) The typologies report: Innovating to fight financial crime in an age of rapid change. Available at: https://www.elliptic.co/resources/the-typologies-report

[18] Chainalysis (2025) The Chainalysis 2025 Crypto Crime Report. Available at: https://go.chainalysis.com/2025-Crypto-Crime-Report.html

[19] FATF (2021, 2023) Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, and Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. Available at: https://www.fatf-gafi.org/en/topics/virtual-assets.html ; TRM (2023) and Eliptic (2020, 2018) Financial Crime Typologies in Cryptoassets: The Concise Guide for Compliance Leaders.

[20] FATF (2025) Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. Available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html; Elliptic (2025), and Chainalysis (2025).

[21] Ibid.

[22] Ibid, Shange Fu, Qin Wang, Jiangshan Yu, and Shiping Chen (2023) FTX Collapse: A Ponzi Story (2022) Available at: https://link.springer.com/chapter/10.1007/978-3-031-48806-1_14

[23] FATF (2025) and Elliptic (2025).

[24] Egmont Group of Financial Intelligence Units (2023) Report on Abuse of Virtual Assets for Terrorist Financing Purposes: Public Summary. Available at: https://egmontgroup.org/wp-content/uploads/2023/12/2023-July-HoFIU-06-IEWG-Project-Abuse-of-VA-for-TF-Summary-1.pdf

decentralized and centralized exchanges. Smart contracts provide essential functionality for virtual assets by enabling decentralized, automated transfers of value based on predefined conditions.[25] DeFi introduces programmable, open-access financial services, including automated lending and trading. The tokenization of real-world assets further broadens investment opportunities by facilitating fractional ownership, enhanced liquidity, and faster settlement. As digital finance evolves, criminals increasingly exploit on-chain services and DeFi innovations. DeFi platforms and peer-to-peer (P2P) networks are particularly vulnerable due to insufficient verification requirements, which facilitate transactions involving fake or stolen identities.

Criminals also continue to use unregistered VASPs, over-the-counter (OTC) traders, mixers and bridges, and swapping VAs for cash. These are in addition to the growth of stablecoins, which have enabled criminals to use more price stable virtual assets and lower volatility than other cryptos in their illicit activities, including money laundering.[26] In this context, FATF (2025) noted a significant increase in the use of stablecoins by illicit actors since 2024, including those linked to the Democratic People's Republic of Korea (DPRK) and terrorist financiers, with stablecoins now involved in most illegal on-chain activity. TRM Labs (2023) reported that approximately 45% of crypto volume associated with illicit acts occurred on the TRON blockchain, followed by Ethereum at 24% and Bitcoin at 18%. Tether (USDT) was identified as the stablecoin with the highest volume of illicit transactions.

The FATF's sixth report, published in June 2025, on the global implementation of standards for VAs and VASPs, indicated that jurisdictions have made progress since the update to R.15 in developing or implementing relevant AML/CFT regulations. However, significant challenges remain in assessing risks associated with VAs and VASPs and in applying effective mitigation measures. As of April 2025, the FATF assessed that, among 138 jurisdictions, only one jurisdiction was fully compliant (C) with R.15, while 29% (40 jurisdictions) were largely compliant (LC), 50% were partially compliant (PC), and 21% were noncompliant (NC) with FATF R.15.[27]

The lack of uniform implementation of FATF R.15, including the Travel Rule requirements (R.16), is considered a major challenge in combating the global misuse of virtual assets for illicit purposes. This issue, referred to in the industry as the 'Sunrise' problem, is discussed further in this report. Additionally, there is a skills gap among AML/CFT practitioners, highlighting the need for specialized blockchain expertise and advanced forensic and analytics tools to identify and investigate criminal virtual assets, particularly those involving mixers, DEXs, cross-chain bridges, and privacy coins.

This report addresses the aforementioned typologies of global misusers of virtual assets, with a focus on the UAE national context. It illustrates the use of various typologies by criminals to exploit the virtual

[25] Bongini, P., Mattassoglio, F., Pedrazzoli, A., and Vismara, S. (2025) Crypto ecosystem: navigating the past, present, and future of decentralized finance. Available at: https://link.springer.com/article/10.1007/s10961-025-10186-x

[26] Krause, D. (2025) The $1.4 Billion Bybit Hack: Cybersecurity Failures and the Risks of Cryptocurrency Deregulation. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5367106; FATF (2025), Elliptic (2025), and Chainalysis (2025).

[27] FATF (2025).

asset ecosystem, highlighting their frequency and identified criminal transactional and behavioral patterns in orchestrating their illicit acts. This report concludes by highlighting the underlying challenges still encountered in preventing criminal schemes and suggests different recommendations to address them, as perceived by practitioners of the AML/CFT regime. These are in addition to a comprehensive list of risk indicators that should assist the UAEFIU's stakeholders in detecting, reporting, and investigating suspicions involving the misuse of virtual assets and local VASPs.

2. OBJECTIVES

In accordance with the Strategic Analysis Plan (SAP) and as part of ongoing efforts to address and identify patterns and typologies of financial crime, the UAEFIU presents its second report on virtual assets for the following purposes:

- Understand the market developments, trends, and emerging risks of financial crime at both global and national levels;
- Reassess previously identified typologies related to the misuse of virtual assets or VASPs in the UAE;
- Evaluate the extent of VASPs' compliance with the UAEFIU reporting system and assess the quality of their suspicious transaction and activity reports;
- Update the previous list of risk indicators;
- Identify current challenges and observed gaps in practice, and recommend appropriate solutions to policy and decision makers;
- Enhance awareness among relevant stakeholders regarding virtual asset-related investigations and risks, in order to proactively detect, investigate, and mitigate suspected financial crime cases involving virtual assets.

3. METHODOLOGY

This report extends previously identified typologies of the misuse of virtual assets in financial crime and addresses associated attributes and characteristics of criminals' schemes. This report is compiled using three different approaches:

3.1. Available data within the UAEFIU's databases and open source (covering a period of two years from 01/07/2023 to 30/06/2025), including the following:

i. Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) received through the UAEFIU's reporting system from VASPs or other reporting entities related to virtual assets concerns.
ii. Cases disseminated by the UAEFIU to law enforcement authorities (LEAs) or initiated by LEAs through the Integrated Enquiry Management System (IEMS).[28]
iii. International intelligence received by the UAEFIU from counterpart FIUs, whether spontaneously or by request.
iv. Open-source data, including media reports, screening results, and relevant articles and documentary data.

3.2. Questionnaire

A questionnaire comprising quantitative and qualitative questions on virtual assets was circulated in July 2025 to all licensed VASPs and to domestic and international banks operating in the UAE, aiming to collect practitioners' insights and perspectives for cross-analysis against the outcomes of the analysis of the previously mentioned data. Said questions included, but were not limited to, the following:

i. Develop an understanding of the virtual assets' ecosystem in the UAE, offered services, (legal and illegal) practices, and market trends and developments.
ii. Most frequent schemes or trends observed by reporting entities (VASPs and banks) concerning their customers' activities and transactions involving financial crime.
iii. Whether red flag monitoring measures were tailored to the observed schemes.
iv. Banks established relationships with VASPs, including their onboarding and monitoring measures, risk appetite, and understanding of virtual asset risks, customers' risks in this regard, whether VASPs or individuals transacting in VAs (e.g., P2P).
v. Identify major challenges in tracing and detecting suspicious activities and transactions, as well as other potential challenges relevant to the nature of virtual assets or to monitoring their risks.
vi. Insights into technological solutions and approaches to enhance financial crime risk mitigation in the virtual asset industry.

Positive responses were received from **69 reporting entities (32 banks and 37 VASPs)** —excluding responses that did not provide details or were not applicable, either because they were newly licensed VASPs or banks that do not maintain a business relationship with VASPs and did not report or observe any relevant financial crime suspicions or schemes.

[28] The Integrated Enquiry Management System (IEMS) is established and owned by the UAEFIU to facilitate communication and the processing of requests between domestic competent authorities, regulated financial institutions, and the UAEFIU.

3.3. Focus Group(s)

The UAEFIU organized **five focus groups** in June 2025 that included members from VASPs, banks, police department investigators, public prosecutors, and senior operational and strategic analysts from the UAEFIU. The first theme focused on understanding the global and national virtual asset ecosystem and VASPs' licensed services and practices in the UAE. The second theme discussed virtual asset-related risks to financial crime and other market and compliance risks. The last theme was dedicated to exploring relevant challenges, particularly in detection, investigation, and monitoring, and to discussing risks and criminal schemes, as well as proposed solutions. Conclusions drawn from the five focus groups were verified with the above-indicated data and integrated into this report.

4. VIRTUAL ASSETS REGULATORY FRAMEWORK IN THE UAE [29]

The UAE has established itself as a leading country in digital finance by adopting virtual assets and implementing a progressive regulatory framework. This approach aims to balance financial innovation with robust safeguards to ensure financial integrity, consumer protection, and market stability.

The supervision and regulation of virtual assets in the UAE is established by Cabinet Resolutions 111 and 112 of 2022, which assign regulatory authority to both national and Emirate-level bodies. This multi-agency structure comprises the Central Bank of the UAE (CBUAE), the Dubai Virtual Assets Regulatory Authority (VARA), the Securities and Commodities Authority (SCA), the Financial Services Regulatory Authority (FSRA) of Abu Dhabi Global Market, and the Dubai Financial Services Authority (DFSA). Collectively, these regulators impose stringent licensing, conduct, and anti-money laundering (AML) requirements on virtual asset service providers (VASPs).

Within this context, VARA, which currently regulates the largest share of VASPs in the UAE, was established under Law No. (4) of 2022 as the competent body to regulate, license, and supervise virtual asset activities within the Emirate of Dubai. VARA's mission is to ensure that the virtual asset ecosystem develops within a secure, transparent, and well-governed framework aligned with international best practices and the FATF standards. VARA's supervisory strategy is founded on a risk-based supervision (RBS) model, in which supervisory intensity and frequency are proportionate to each VASP's inherent and residual risks. It follows a structured twelve-month cycle encompassing continuous monitoring, periodic data submission, thematic analysis, and targeted engagements. Each VASP's risk profile is reviewed annually, combining financial soundness, governance, conduct, and AML/CFT compliance indicators into a holistic assessment that guides subsequent supervisory planning.

[29] We thank the Dubai Virtual Assets Regulatory Authority (VARA), the Financial Services Regulatory Authority (FSRA) of Abu Dhabi Global Market, the Dubai Financial Services Authority (DFSA), and the Securities and Commodities Authority (SCA) for providing context on their supervisory models and regulatory frameworks referenced in this section.

VARA's supervisory approach is both data-driven and technology-enabled. The Authority uses Supervisory Technology (SupTech) and on-chain analytics to monitor wallet activity, identify anomalies, and integrate blockchain data with off-chain sources, such as financial reports and complaints. This technological integration facilitates early risk detection and enables prompt supervisory interventions, including desk-based reviews, targeted inspections, and unannounced investigations. The risk-based supervision cycle includes various engagement types: comprehensive AML/CFT inspections (covering governance, sanctions compliance, customer due diligence, and Travel Rule implementation), targeted inspections of high-risk areas such as custody or market conduct, supervisory and compliance meetings to resolve reporting discrepancies, and, when necessary, formal investigations and enforcement referrals. Each engagement results in documented findings, remedial actions, and, if required, recalibration of risk ratings or imposition of sanctions in accordance with the Compliance and Risk Management Rulebook (CRMR).

Before the establishment of VARA, the FSRA introduced its regulatory framework for virtual assets in June 2018. As the regulator of the ADGM, a financial free zone in the UAE, the FSRA recognized within its regulatory framework risks associated with VASPs, including money laundering, terrorist financing, theft and misuse of customer assets, market manipulation, and investment risks. To address these risks, the FSRA implemented a robust, comprehensive framework that adapts traditional finance best practices to the VA sector. This included regulations on AML/CFT, segregation and protection of client assets, investor suitability and risk disclosures, market integrity, anti-abuse provisions, and technology governance. Consequently, the FSRA applied the same regulatory standards to VASPs as to other financial services entities, extending its traditional finance framework to encompass VA-related business activities.

At the same time, on-chain observability and transparency create new supervisory opportunities if regimes ensure regulated firms use traceable assets and implement the Travel Rule effectively. The FSRA's response has been to regulate at both the VASP and VA product levels. To that end, the FSRA adopts proactive due diligence of VAs offered in ADGM, including ongoing monitoring of their market profile, traceability, technology, and security vulnerabilities. The FSRA maintained a tight regulatory perimeter by prohibiting privacy tokens and algorithmic stablecoins.

From the FSRA perspective, regulating only VASP activities is insufficient when virtual asset governance occurs on-chain. New business models increasingly depend on smart contract-enabled services, such as decentralized exchanges and decentralized VA borrowing and lending platforms, which are governed by distributed ledger technology (DLT) protocols. Although the FSRA supervises intermediary activities, the quality of underlying blockchain governance remains essential for maintaining system integrity and preventing financial crime. To address this, ADGM's DLT Foundations framework provides legal structures for decentralized projects, supporting accountability, fiduciary duties, and compliance mechanisms for decentralized autonomous organizations (DAOs). This framework complements the

FSRA's financial and AML/CFT regulations by ensuring legal certainty and operational accountability for blockchain networks supporting virtual assets.

In parallel, the FSRA has invested in digital supervisory mechanisms, such as VA due diligence platforms, continuous monitoring tools, and analytics, to effectively scale oversight capabilities. These enhancements across governance structures, business activities, and AML/CFT measures leverage supervisory technology, from a coherent digital asset approach that is risk-based, outcome-focused, and aligned with the UAE financial crime prevention objectives.

In November 2022, the DFSA implemented a comprehensive legislative framework for regulating VASPs and virtual assets. Under this regime, firms operating within the Dubai International Financial Centre (DIFC) may obtain licenses to offer financial services involving Crypto Tokens, including operating exchanges, providing custody, dealing, advising, and managing investments.

The DFSA framework emphasizes governance, capital adequacy, client asset protection, and comprehensive compliance with FATF-aligned AML/CFT requirements, including blockchain analytics, Travel Rule implementation, and enhanced sanctions screening. The DFSA has identified key risks, including market volatility, technology and cyber resilience, custody and key management failures, and financial crime. To address these, it has implemented targeted mitigation measures, including rigorous token-approval processes, heightened prudential standards, segregation of client assets, restrictions on higher-risk products, and enhanced protections for retail investors. Ongoing supervisory engagement, thematic reviews, and continuous monitoring support these safeguards. As of 30 September 2025, there are no standalone VASPs in the DIFC, but 10 financial institutions have amended their DFSA licenses to include crypto-related activities.

At the federal level, SCA has developed a comprehensive regulatory framework to oversee virtual assets and related service providers across the UAE mainland. Based on Cabinet Resolution No. 111 of 2022, this framework seeks to ensure the integrity, transparency, and stability of the virtual asset ecosystem, protect investors, and mitigate financial crime risks. The SCA employs a technology-neutral approach, regulating activities rather than specific technologies, to provide consistent oversight of emerging virtual asset services.

Within this framework, the SCA licenses and supervises investment-related virtual asset activities on the UAE mainland, including exchanges, brokerage, custody services, trading platforms, and other investment-related services. The SCA's regulatory strategy directly addresses the principal risks identified in national and sectoral risk assessments, including money laundering, terrorist financing, cybercrime, and cross-border misuse. To mitigate these threats, the SCA mandates that all licensed VASPs comply fully with the UAE's AML/CFT/CPF framework, encompassing customer due diligence, ongoing monitoring, suspicious transaction reporting, sanctions screening, and enhanced due diligence for higher-risk clients and products. Additional measures include robust custody controls, secure wallet

management, segregation of customer assets, and transparent disclosure requirements to prevent mis-selling and strengthen investor protection.

Technology and operational resilience are core components of the SCA regulatory framework. Therefore, licensed entities are required to maintain secure infrastructure, implement robust cybersecurity controls, establish incident-response plans, and develop internal governance systems to manage complex digital asset activities. These requirements are designed to mitigate vulnerabilities arising from cyberattacks, system failures, and inadequate key management practices.

From a supervisory perspective, the SCA conducts risk-based offsite and onsite supervision, reviews prudential and conduct requirements, and evaluates the adequacy of each VASP's AML/CFT controls. The SCA also works closely with other domestic regulators, including VARA, CBUAE, and financial free-zone regulators, through structured cooperation and information-sharing mechanisms. These arrangements support coordinated licensing, supervision, and enforcement to ensure national consistency and prevent regulatory arbitrage. Joint initiatives include intelligence exchange and unified approaches to unlicensed activity.

Lastly, the CBUAE is responsible for licensing and supervising payment token service providers under the Payment Token Services Regulation. Payment Tokens are defined as virtual assets pegged to a fiat currency and are classified as either Dirham Payment Tokens or Foreign Payment Tokens. These tokens do not have legal tender status and serve solely as a means of payment, agreed upon by users.

5. OVERVIEW OF THE DATA UTILIZED IN THIS REPORT

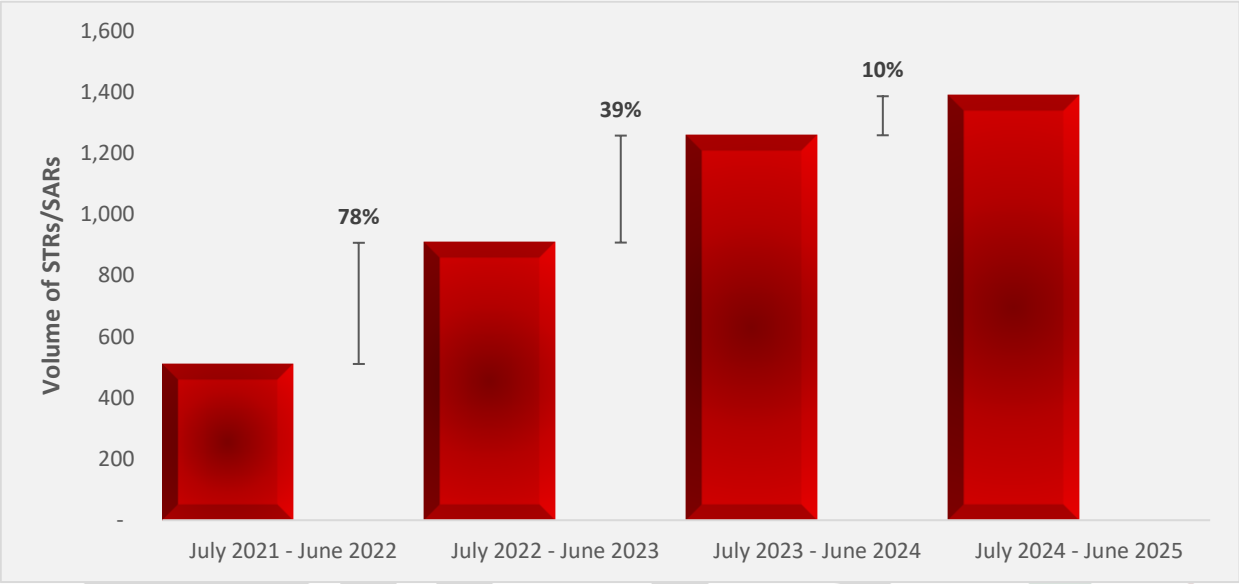
This section provides a descriptive analysis of data from the UAEFIU's databases, which underpins the findings presented in later sections. The analysis includes an overview of registered VASPs within the UAEFIU reporting system and examines STRs/SARs related to virtual assets received from 1 July 2021 to 30 June 2025. A sample of STRs and SARs submitted by VASPs and Financial Institutions (FIs) between 1 July 2023 and 30 June 2025 was selected to identify typologies of virtual asset misuse in financial crime. This section also reviews cases referred to or from LEAs and considers international intelligence exchanged with counterpart FIUs.

During the four-year review period, the number of registered entities associated with virtual asset services on goAML increased **from 7 in June 2022 to 64 in June 2025.** This figure encompasses standalone VASPs and financial institutions providing virtual asset related services, stable coin issuers, and payment token service providers. This substantial increase demonstrates the rapid expansion of the local virtual assets market. [30]

[30] As of November 2025, the total number of registered entities on goAML providing virtual asset services is 73. This figure does not include entities that are not operational and entities that have only obtained in-principal approval from their respective regulatory authorities. Some standalone VASPs have obtained multiple trade licenses to offer different VASP-related services with one or more regulators.

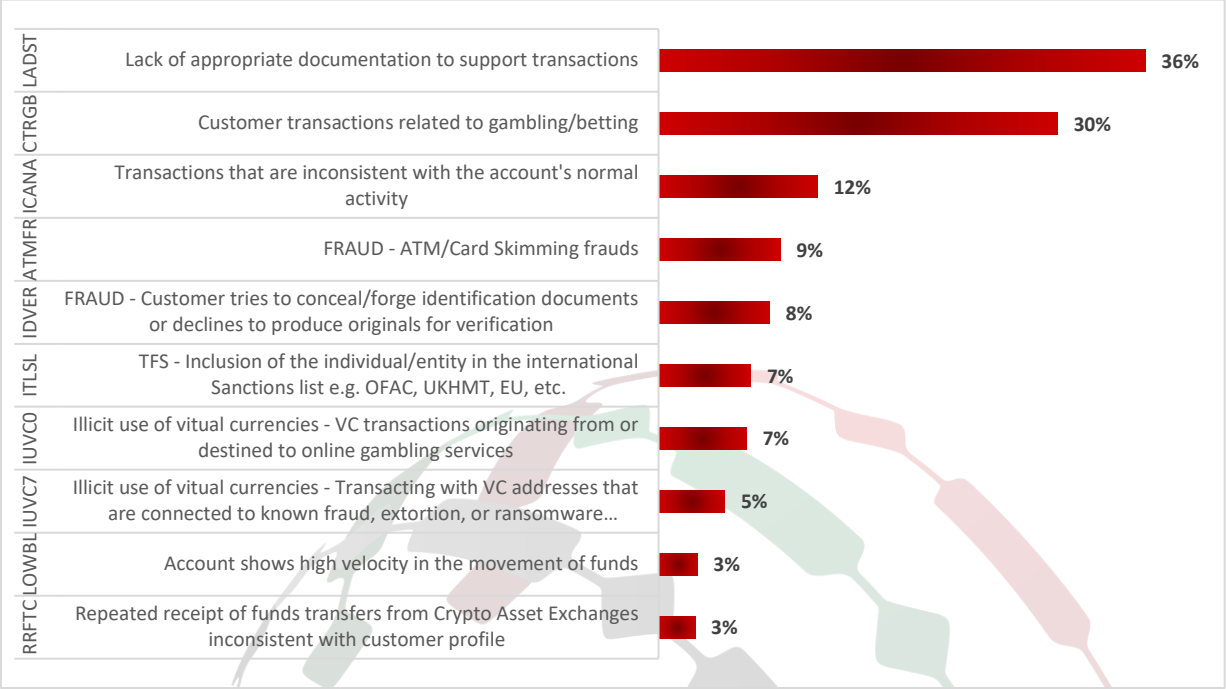
Over the four years, these entities submitted **4,065 suspicious reports** to the UAEFIU. Chart 1 demonstrates a consistent annual increase in report volume, with a 78% rise between June 2022 and June 2023, followed by a more moderate 10% increase in the final year ending June 2025. Nevertheless, this upward trend in reporting should not be interpreted as a risk-mitigation strategy that addresses the inherent risks, characteristics, and vulnerabilities of virtual assets, particularly those associated with criminal techniques aimed at exploiting the sector.

Chart 1: *Volume of suspicious reports received from registered entities associated with virtual asset services during July 2021 to June 2025*



With regards to the reasons for reporting used by VASPs upon submission of STRs/SARs, the following chart demonstrates the top RFRs during the four years.

Chart 2: *Top 10 Reasons for Reporting (RFRs) utilized in the submitted STRs/SARs*

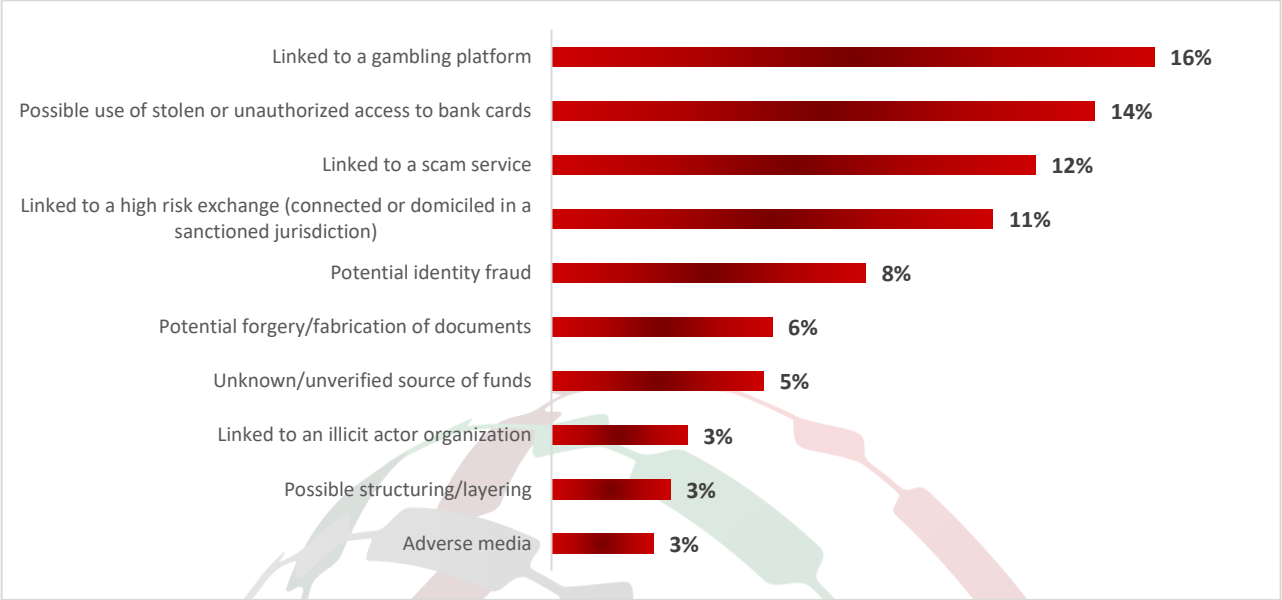


5.1. Examined sample of the suspicious reports filed by VASPs (July 2023-June 2025)

From 1 July 2023 to 30 June 2025, the UAEFIU received 2,645 suspicious reports from VASPs, including 2,025 STRs and 620 SARs. For this report, the UAEFIU reviewed a sample of 458 suspicious reports, covering 287 STRs and 171 SARs.

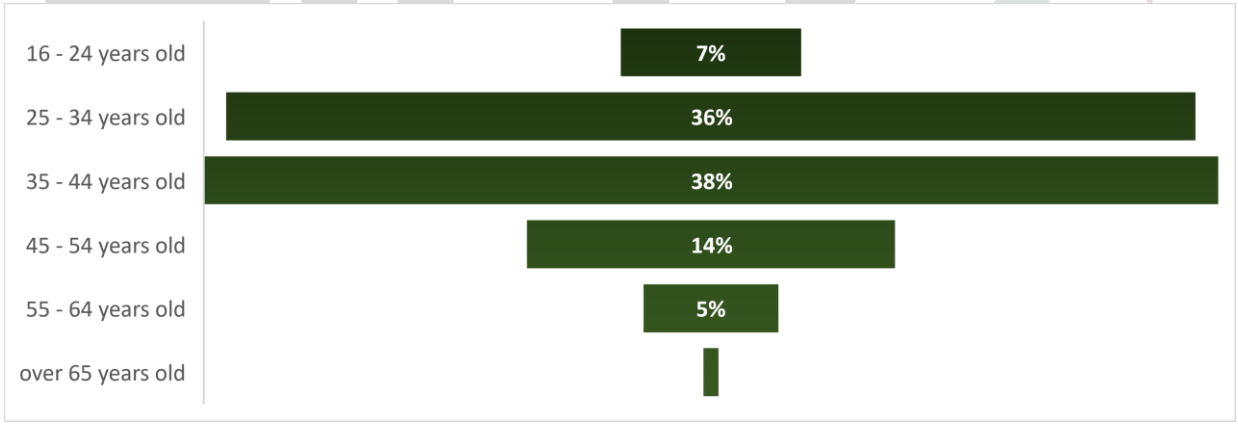
The most frequent triggers for reporting these entities were linked to gambling, stolen or unauthorized use of bank cards, scams, and high-risk exchanges domiciled in or associated with sanctioned jurisdictions, as shown in Chart 3.

Chart 3: *Top VASPs' concerns in the analyzed sample*



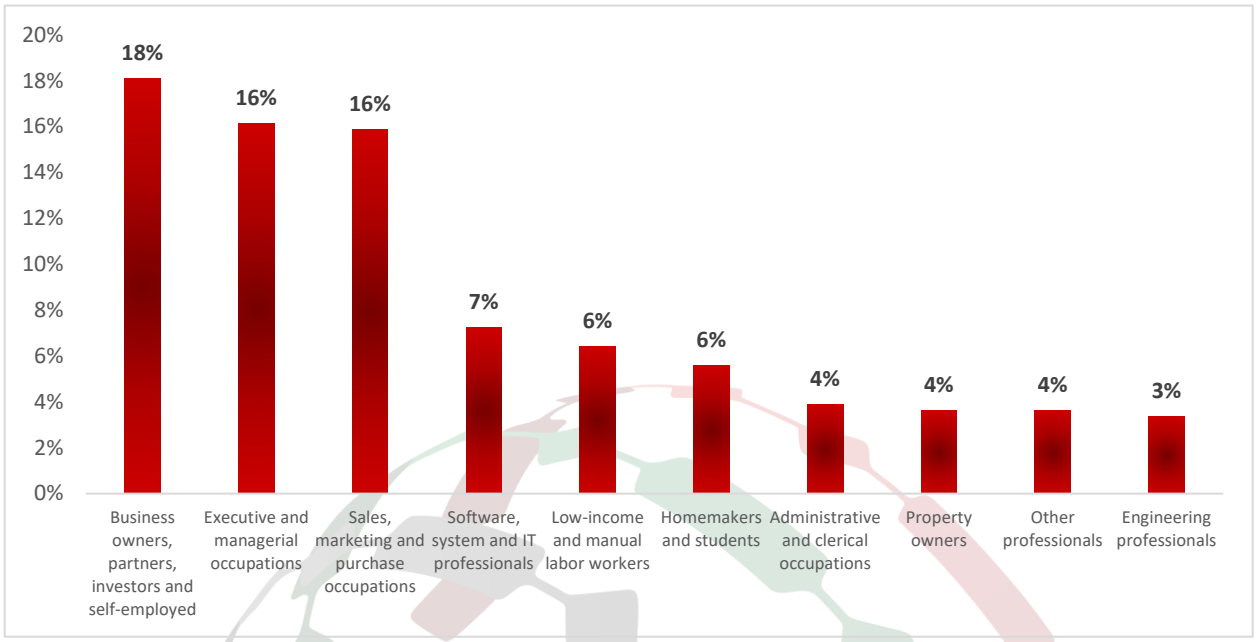
The analysis indicated that 81% of examined suspicious reports involved natural persons, 7% pertained to legal persons, and the remaining 12% involved unidentified subjects due to insufficient reliable data, such as cases of identity fraud, forged documents, or scam activities reported by victims. Approximately 74% of the subject natural persons fell within the young adult and **middle-aged** groups (25 to 44), as illustrated in Chart 4.

Chart 4: *Age of the involved subject NPs*



Analysis of the residence status of the identified natural persons shows that 90% are residents of the UAE, while 10% are non-residents. Occupational analysis indicates that 18% were business owners, partners, investors, or self-employed. Individuals in sales, marketing, and purchasing roles, as well as those in executive and managerial positions, each represented 16% of the sample. Software, system, and IT professionals comprised 7% of the professions, as depicted in Chart 5.

Chart 5: *Top occupations/professions of the subject NPs*



For legal entities, fewer relevant suspicious reports were identified compared to individuals, with only 32 STRs and SARs examined in detail for this sample analysis. Of these entities, 70% were established in commercial free zones, 20% in mainland jurisdictions, and 10% in foreign jurisdictions. The primary business activities of these entities comprised web design, gaming development, computer-related services, data processing, and technology solutions.

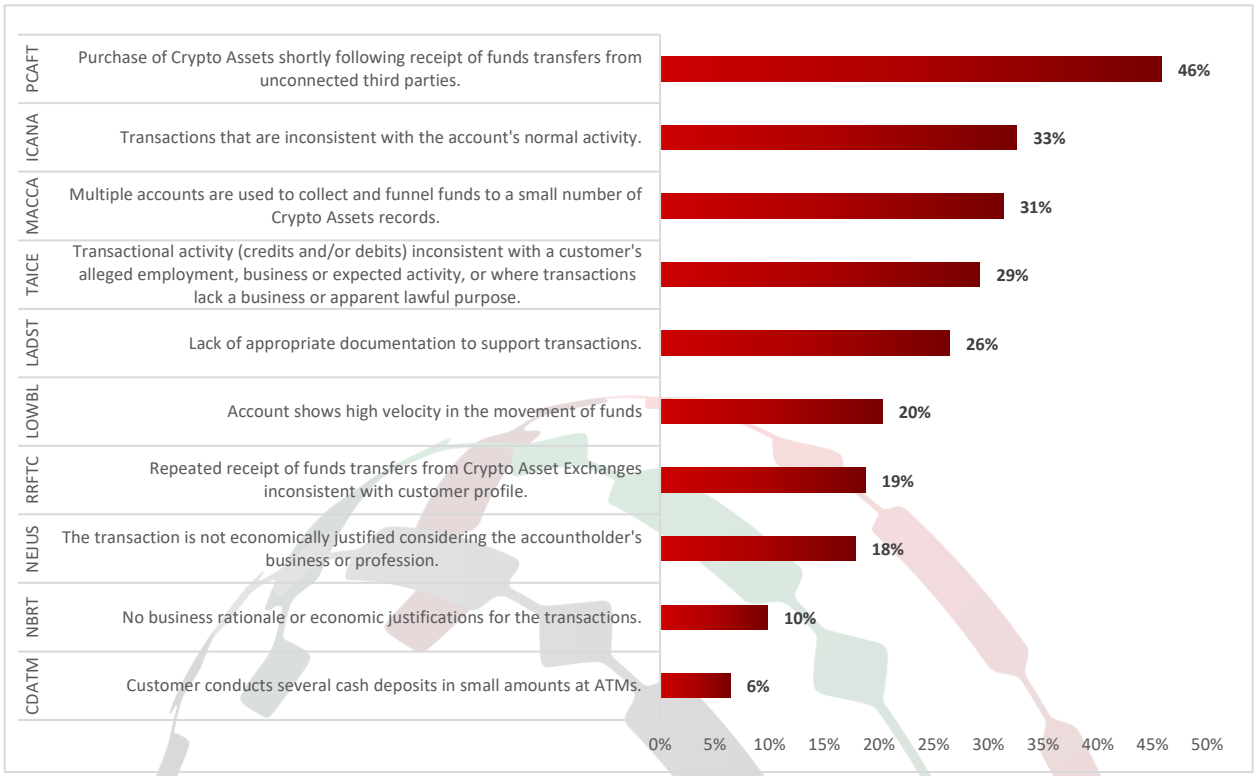
5.2. STRs/SARs reported by other reporting entities involving VAs (July 2023-June 2025)

Between 1 July 2021 and 30 June 2025, the UAEFIU received **512 suspicious reports** from reporting entities (excluding VASPs) and competent authorities, with reporting reasons focused on concerns related to virtual assets. Of these reports, 97% were submitted by financial institutions (FIs), 2% by designated non-financial businesses and professions (DNFBPs), and 1% by competent authorities, specifically regulatory or supervisory bodies.

The UAEFIU has undertaken **a full-scale analysis of 346 suspicious reports** (325 STRs and 21 SARs), encompassing 100% of the reports received from 1 July 2023 to 30 June 2025. Of these reports, 325 were found to be directly relevant to potential misuse of virtual assets and VASPs.

The top 10 reporting entities and the top 10 RFRs in the said reports are illustrated in the following chart.

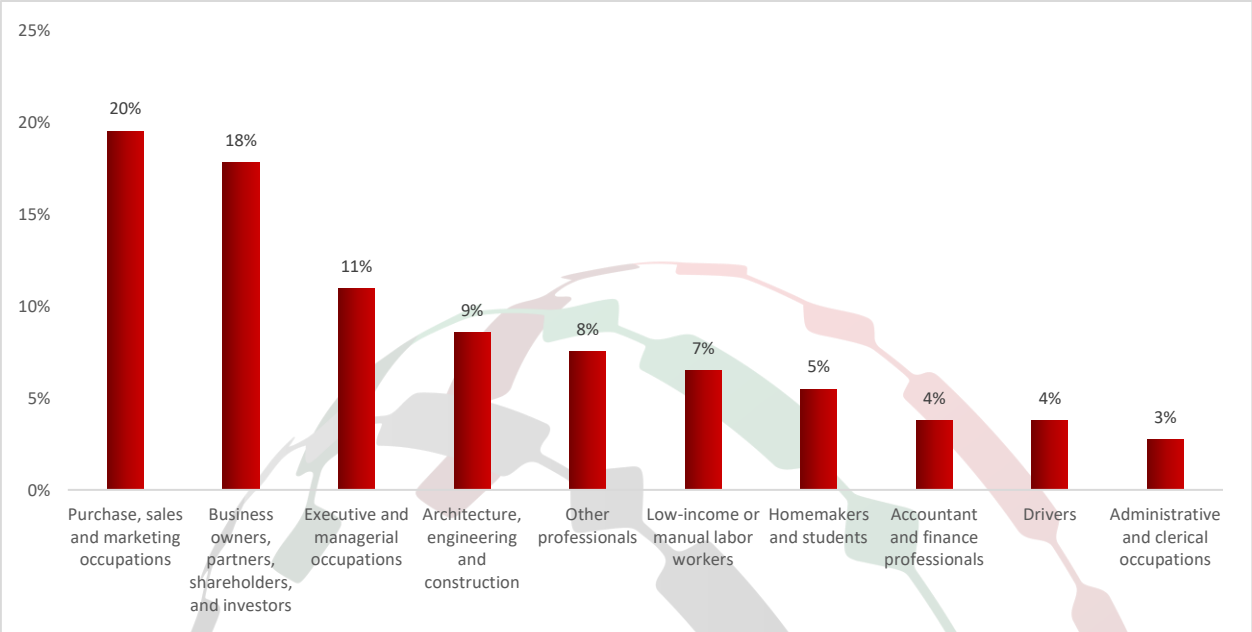
Chart 6: *Top 10 reasons for reporting utilized by other REs and competent authorities*



Analysis of the STRs/SARs indicates that 94% were associated with 292 distinct natural persons, while the remaining 6% involved legal persons. Nearly half (48%) of the subject natural persons were **young adults** aged 25 to 34 years, followed by 34% in the middle-aged group of 35 to 44 years.

With respect to residence status, 97% of the subject natural persons were residents of the UAE, 2.5% were non-residents, and 0.5% could not be determined due to insufficient documentation. Analysis of occupations revealed that 20% were employed in purchase, sales, and marketing, while 18% were business owners, partners, shareholders, or investors, as illustrated in Chart 7.

Chart 7: *Top occupations/professions of the subject NPs*



6. UNDERSTANDING VIRTUAL ASSETS VULNERABILITIES AND THREATS [31]

According to the UAE's National Risk Assessment (NRA), concluded in 2024, the virtual assets sector has a high level of exposure to money laundering. The most prevalent risks remain fraud, unlicensed virtual asset service providers, and geographical risks arising from simplified cross-border transactions. Criminal activities are often facilitated through online marketing campaigns targeting retail investors and exploiting gaps in awareness or cross-border regulatory coordination. The virtual assets sector is also assessed to have a high exposure to be misused by terrorist groups, where terrorist individual terrorists and groups exploit the anonymity of virtual currencies to fund their activities discreetly.[32] Cyberattacks, hacking incidents, and ransomware pose an additional layer of threat, targeting exchanges, custodians, and wallets to steal assets or compromise sensitive information.

The use of mixers, privacy tokens, and decentralized finance (DeFi) platforms adds further complexity, enabling layering and obfuscation of illicit flows. Virtual assets differ fundamentally from traditional financial assets due to their programmability, bearer status, and borderless nature, which introduce distinct regulatory challenges. Features such as pseudonymous wallets, continuous settlement, and

[31] We thank VARA and FSRA for their contributions in this context, relevant to national risks and the sectoral perspective. Thanks are also extended to the practitioners from VASPs, domestic and foreign banks, LEAs, and public prosecutors who participated in the focus group exercise for their time and constructive remarks. Those, in addition to MLROs and participants from VASPs and domestic and foreign banks, who responded to the UAEFIU questionnaire and provided their valuable insights.

[32] Money Laundering and Terrorist Financing Risk Assessment report (2024). Available at: https://www.namlcftc.gov.ae/media/jvejlwgq/nra-annual-report-eng-r13.pdf

composable DeFi compress transaction chains and remove traditional intermediaries that regulators have historically relied upon for oversight. This evolution introduces new vulnerabilities, including risks to private key management, smart contract failures, and emerging financial crime vectors such as mixers, cross-chain transactions, and privacy-enhancing tokens. The anonymity features of certain virtual assets—while offering privacy benefits—increase susceptibility to misuse for illicit financing, including money laundering, terrorist financing, and sanctions evasion.[33]

Regulatory arbitrage at the global level remains another systemic challenge. Some operators attempt to exploit jurisdictional gaps or obtain minimal regulatory coverage while offering services to UAE residents. In parallel, market manipulation and market abuse, including insider trading risks, have emerged due to the decentralized and volatile nature of virtual asset markets, where pump-and-dump schemes or spoofing tactics can mislead consumers and distort pricing.[34]

From the VARA sectoral risk perspective, exchanges and custodians pose the highest risk due to their central roles and high transaction volumes. At the same time, brokers, ICO issuers, and investment managers face medium-to-high risks arising from complex business models and limited transparency. Moreover, infrastructure risks related to smart contracts, such as malware and data theft, further expose the sector to vulnerabilities. The decentralized nature of blockchain networks can impede traceability, making it difficult to attribute transactions to identifiable entities. Variations in cybersecurity resilience across operators expose the industry to systemic risk, while inadequate consumer literacy regarding digital assets increases susceptibility to scams and fraud. Fragmented oversight of legacy operators, inconsistent enforcement of licensing requirements, and limited supervisory resources further exacerbate vulnerabilities.

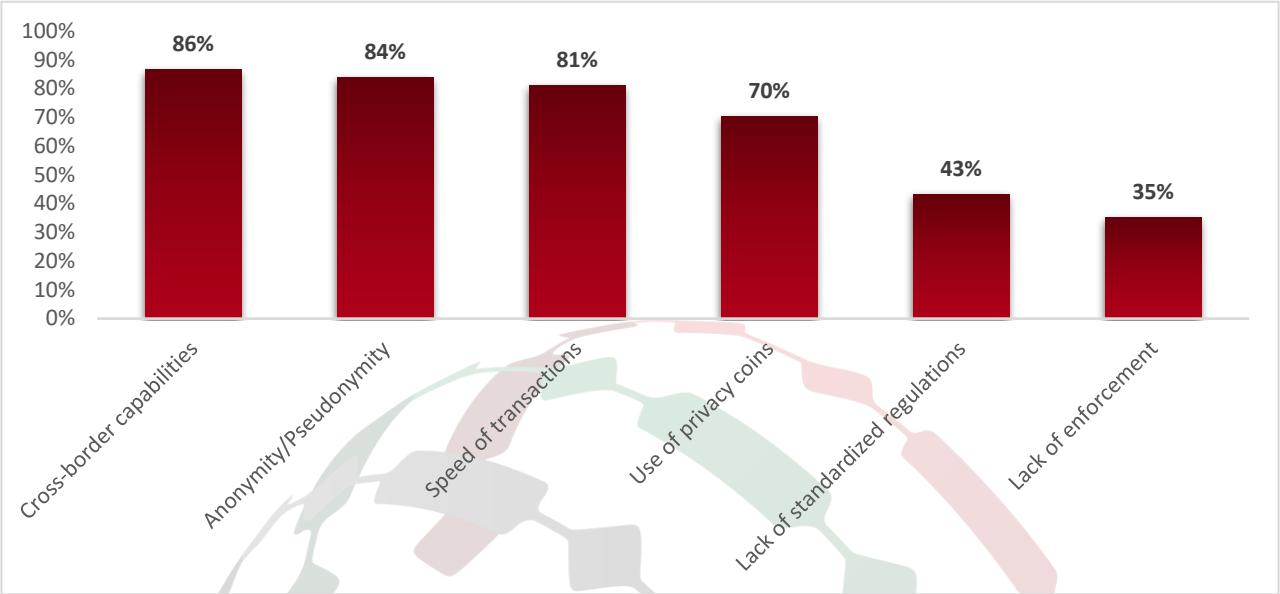
The UAE authorities have addressed these gaps through multiple mitigation initiatives, a robust regulatory framework, and an information-sharing mechanism. For example, VARA launched a grandfathering program to transition legacy operators into the new licensing regime, supported by extensive awareness campaigns, grace periods, and dedicated service centers for compliance assistance. Additionally, coordinated information sharing between registrars, supervisors, and law enforcement ensures that unlicensed activity is detected early.

In addition to the above sectoral risk insights, data collected from the UAEFIU questionnaire and from constructed focus group discussions provided a common understanding of the vulnerabilities and threats of virtual assets as perceived by practitioners in the UAE, including reporting entities (in particular the banking sector and VASPs), LEAs, and prosecutors. Chart 8 below provides some insights into the global features of virtual assets that make them attractive for criminal misuse.

[33] Insights obtained from FSRA and VARA.

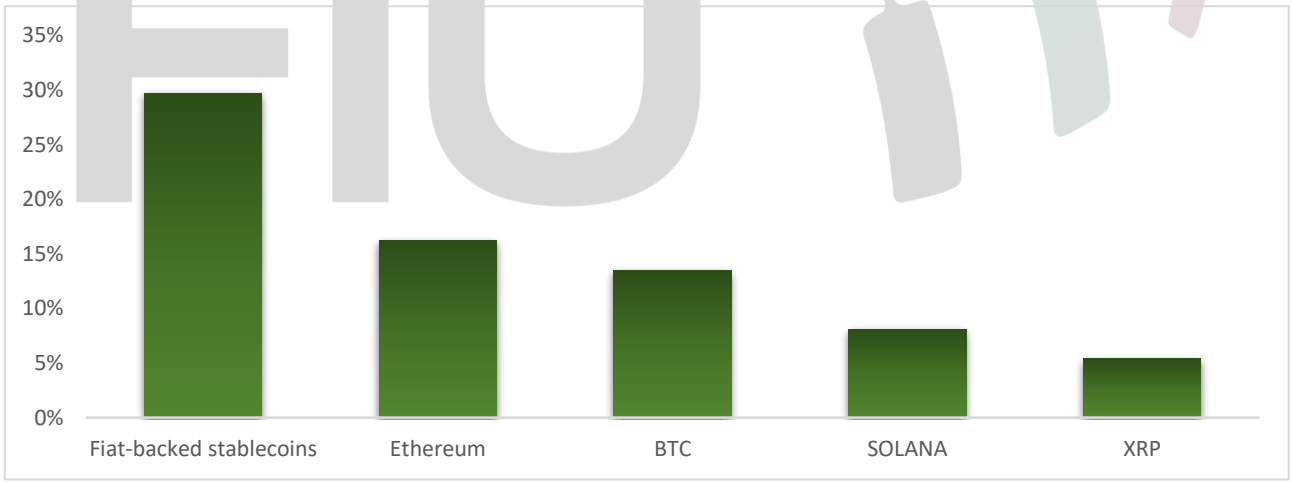
[34] Insights obtained from VARA's sectoral risk assessment.

Chart 8: *Features of virtual assets make them attractive for criminal use, as perceived by VASPs who responded to the questionnaire*



The data used in this report underscored the shift towards **stablecoins** (especially on the Tron network). Chart 9 illustrates the most frequently misused currencies in suspected criminal acts, from VASPs' perspective.

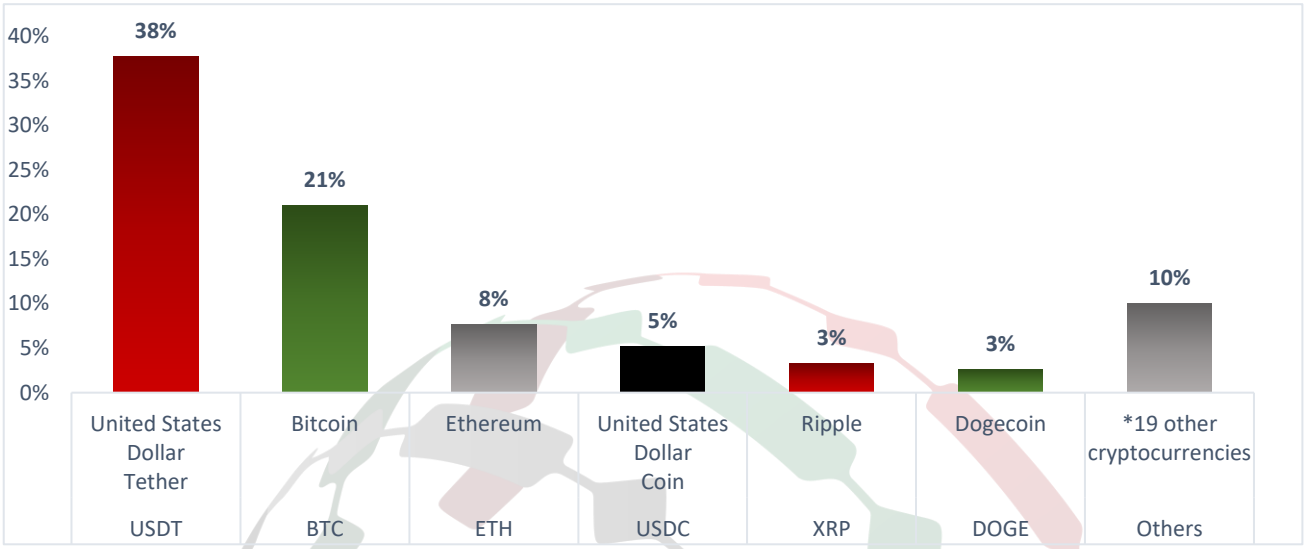
Chart 9: *The most vulnerable cryptocurrency to financial crime, according to VASPs, who responded to the questionnaire*



Discussion of the focus groups highlighted the misuse of BTC in romance scams and stablecoins, notably in sanction evasion and crowdfunding. ETH is also widely used as it is easily transferable, and can also be converted to meme coins.

Analysis of STRs/SARs was consistent with this perception, as the majority of analyzed suspicious reports were associated with stablecoins (USDT, USDC), as shown in Chart 10.

Chart 10: *Frequent currencies involved in the sample STRs/SARs analyzed*



With respect to the misuse of non-fungible tokens (NFTs), including virtual art, music, and NFT gaming, all respondents to the UAEFIU questionnaire reported no evidence of VASPs' customers misusing NFTs. This is primarily because NFTs are not offered or supported by VASPs' services. Similarly, transactions involving privacy coins or cryptocurrencies with anonymity-enhancing mechanisms are prohibited in local VASP services.

As discussed by the focus groups, virtual asset transactions are publicly available on the blockchain, providing a high level of transparency. This transparency is further supported by the industry's evolving compliance culture regarding KYC and KYT.

Data collected from focus groups and the UAEFIU questionnaire were also consistent with the UAE NRA's identified ML/TF risks, as well as with the analysis of STRs/SARs received by the UAEFIU from both FIs and VASPs. As indicated in Charts 11 and 12, **fraud and ML were perceived as the highest threats** by participants from both the banking sector and VASPs.

Chart 11: *Potential financial crime linked to banks identified suspicions or those most concerned to them, according to the questionnaire*

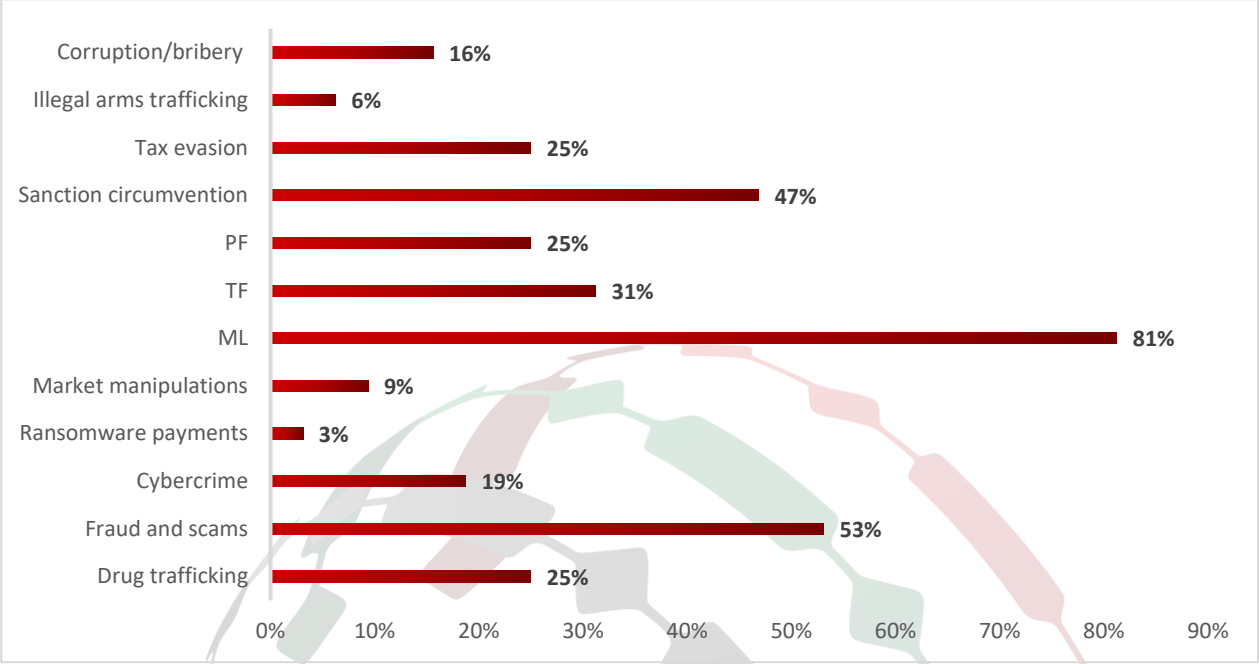
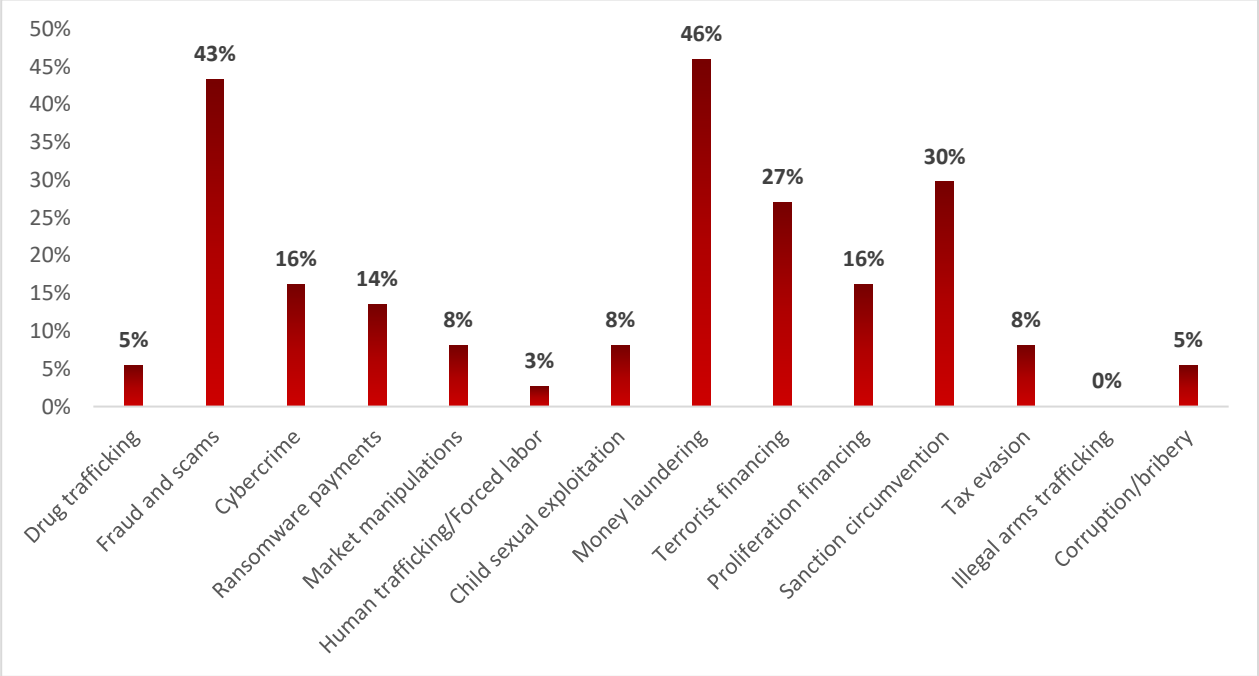


Chart 12: *Potential financial crime linked to VASPs identified suspicions or those most concerned to them, according to the questionnaire*



Simultaneously, analysis of 458 suspicious reports received from VASPs has implied the most prevalent suspected financial crime, with **fraud, illegal gambling, and money laundering** among the top three concerns, as shown in Chart 13. Chart 14 further illustrates the top exposures identified in the analyzed STRs/SARs using a blockchain tracing tool.

Fraud, in particular, according to an analysis of 169 STRs/SARs, was the most prevalent potential financial crime, accounting for 37% of the total sample. This included 48 STRs/SARs associated with unidentified subjects due to the nature of the reported concerns, such as identity fraud (mostly) and investment scams reported by the victims. These are in addition to 56 suspicious reports, in which exposures were found mostly to a scam service (86%) and a fraud shop (7%), with a strong connection of 1 to 2 hops.

Similarly, 11% of the total reports examined were identified as possibly related to money laundering. These reports were filed mostly due to unknown or unverified source of funds (24%) and possible structuring or layering (22%). **USDT** was also the top currency involved (67%) with subject addresses/wallets. Analysis of said reports, considering both REs' reported concerns and the UAEFIU team's analysis using a blockchain analytics tool, further revealed possible structuring or layering activities in 60% of potentially suspected money laundering reports.

Overall, across the examined schemes, fraudulent and fabricated documentation, the use of OTCs, and structuring/layering techniques were among those most frequently used.

Chart 13: *Top potential financial crimes associated with the analyzed sample STRs/SARs received from VASPs*

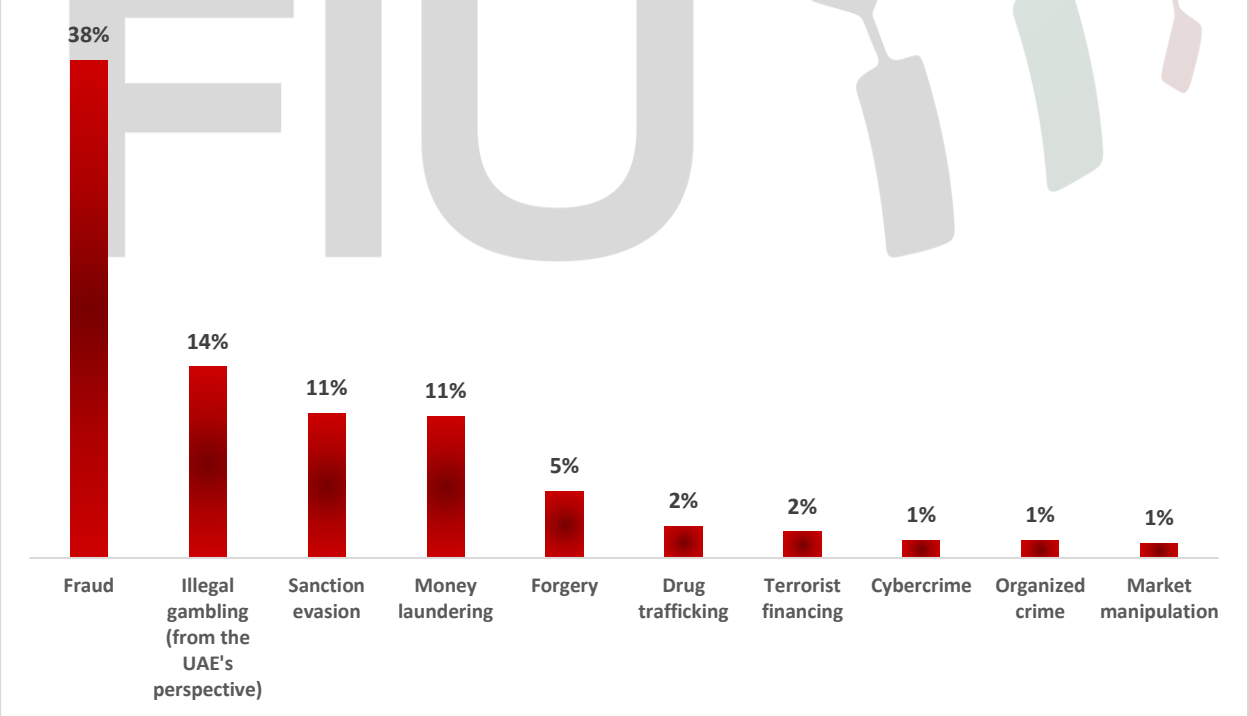
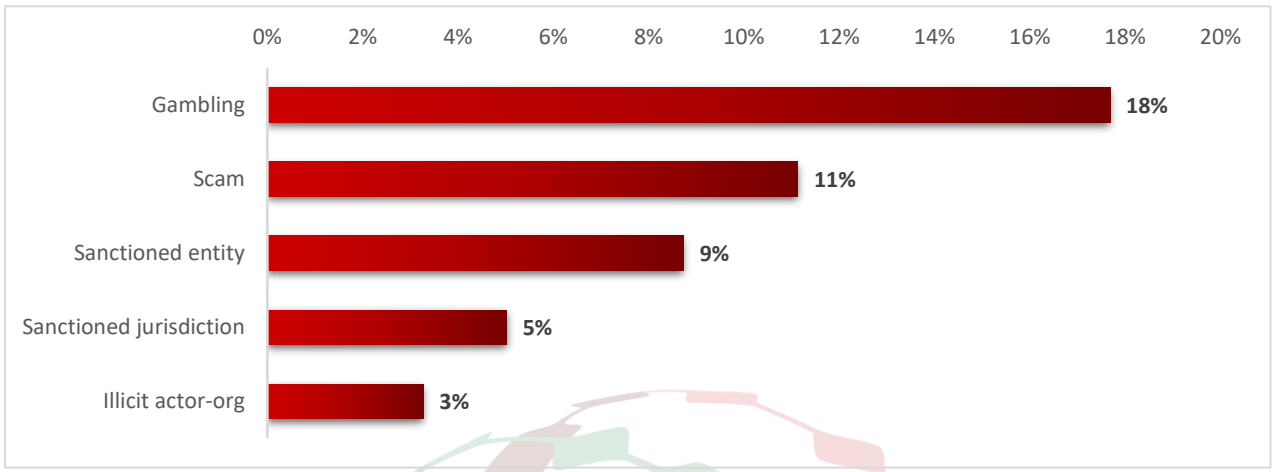
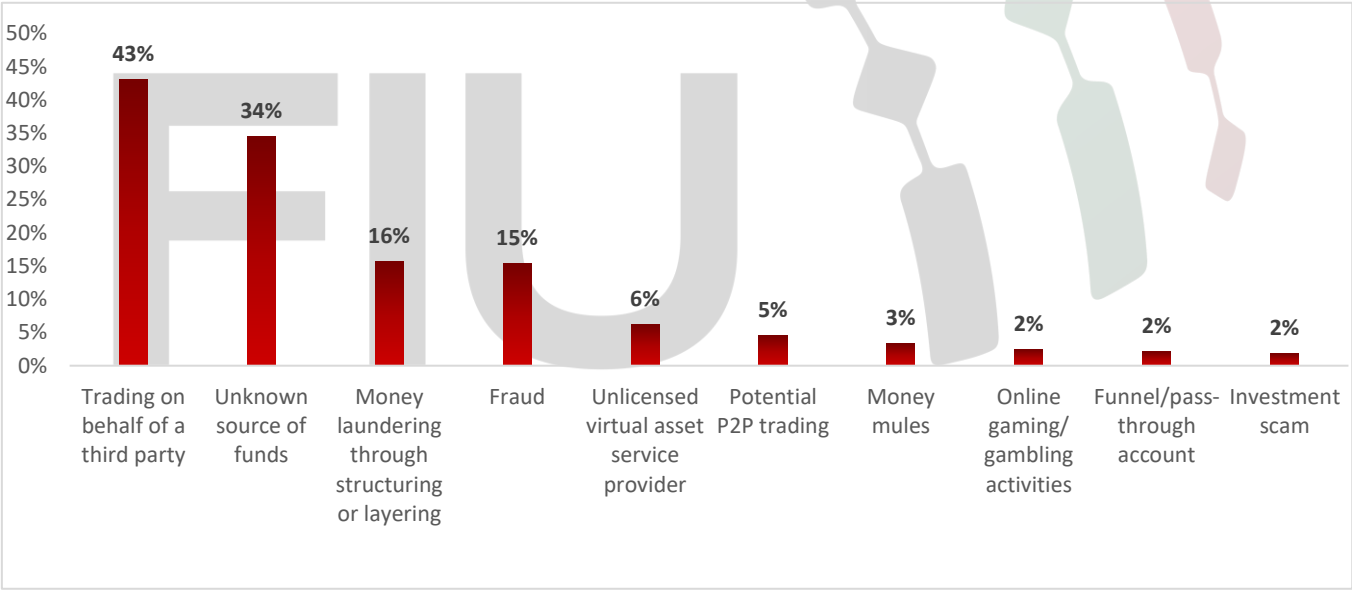


Chart 14: *Top exposures identified in the sample STRs/SARs analyzed*



Further in-depth analysis of the 325 directly related suspicious reports received from other reporting entities and supervisory authorities revealed the top concerns among VA-related STRs/SARs with **trading on behalf of a third party** as the key concern, accounting for 43% of the examined data (as indicated in Chart 15).

Chart 15: *Top concerns identified from the STRs/SARs submitted by other REs and competent authorities*



Within the same context, according to the questionnaire, the most frequent pattern observed by VASPs and FIs in their customer activities associated with potential financial crime was **online gambling**, followed by **acting on behalf of third parties and using money mules**. Fraud schemes, including scams and identity fraud, continued to surface in participants' answers (as indicated in Charts 16, 17, and 18).

Chart 16: *Red flags or unusual patterns related to VA transactions in banks' customer activities, according to the questionnaire*

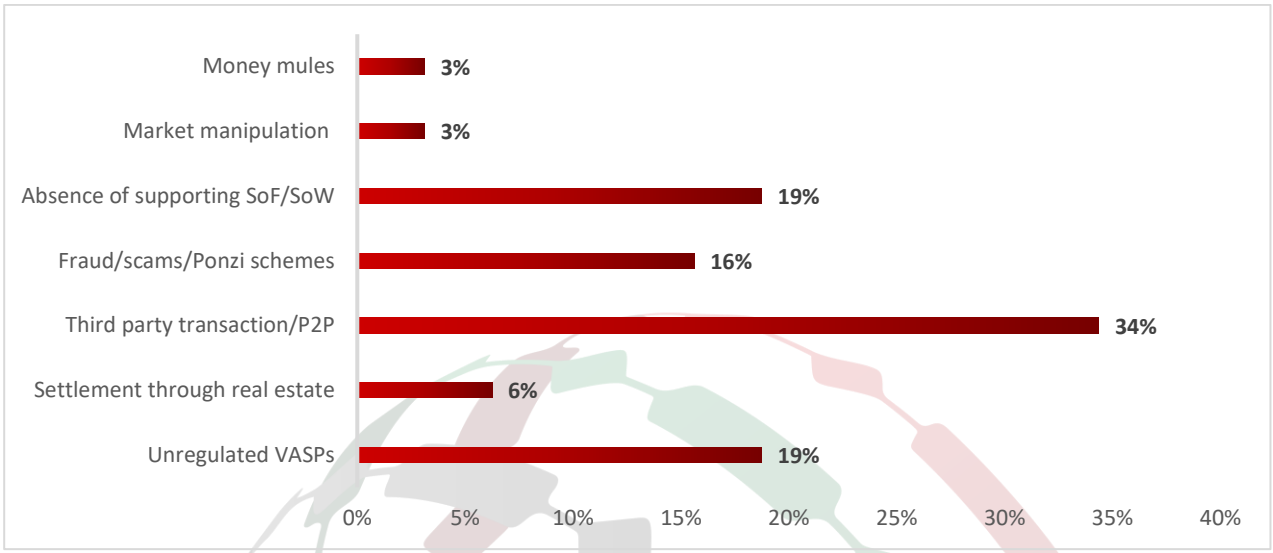


Chart 17: *Identified patterns within VASPs' customer activities/transactions, according to the questionnaire*

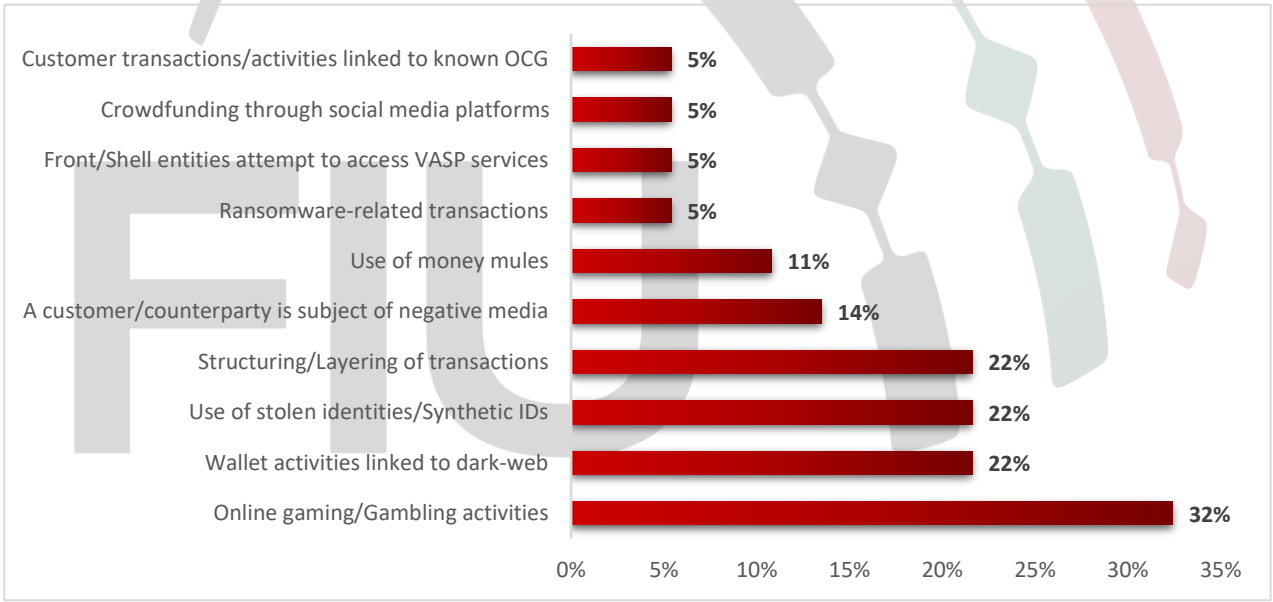
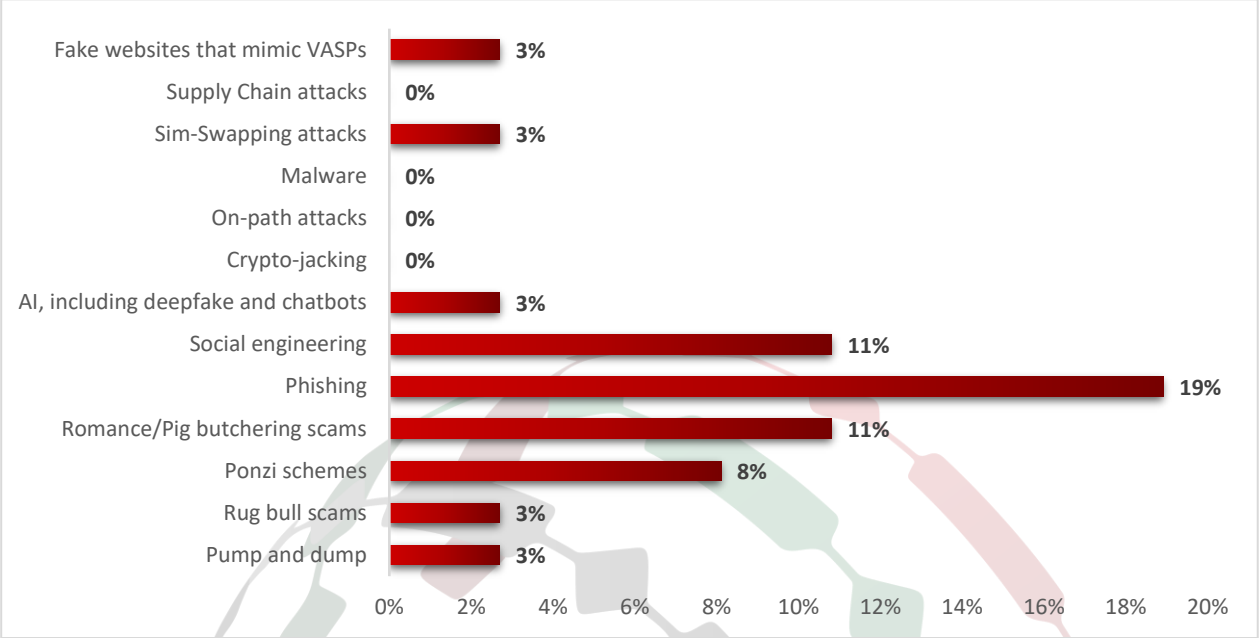
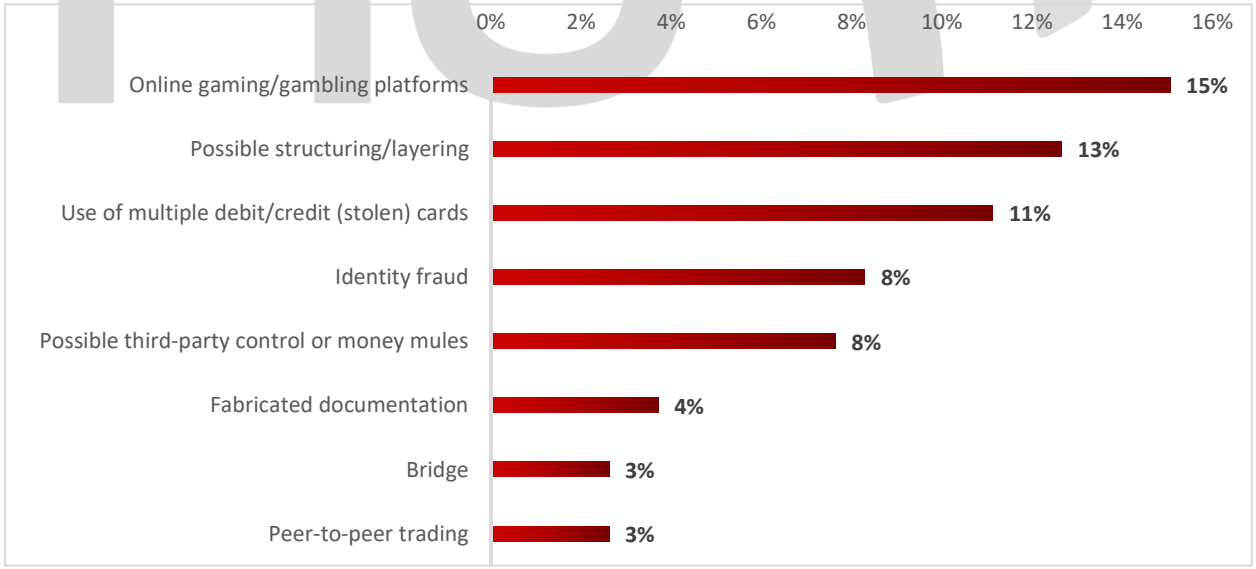


Chart 18: *VASPs' experienced schemes through their platform or customer activities/transactions, according to the questionnaire*



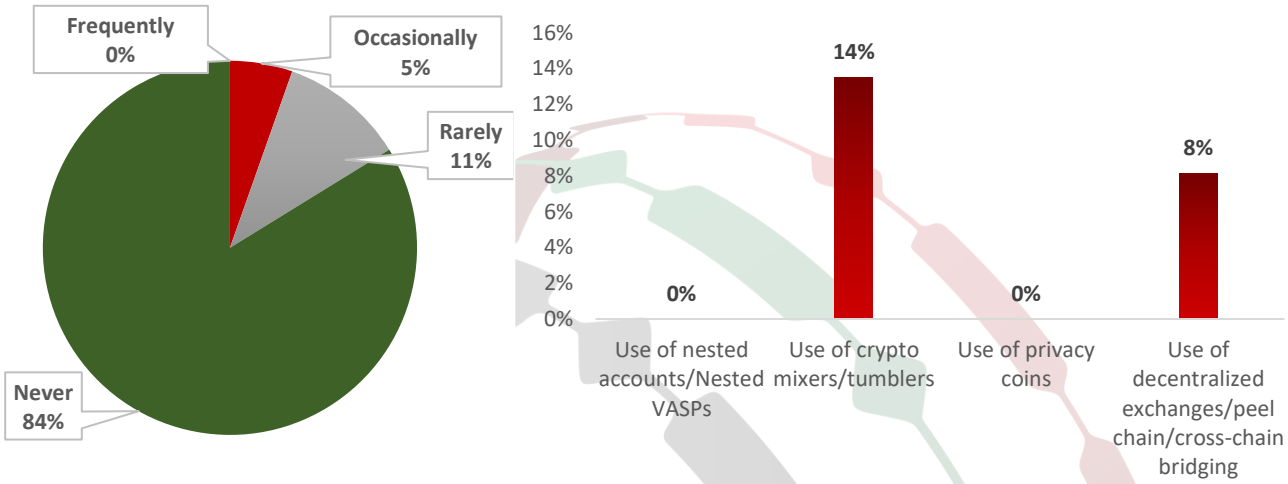
Simultaneously, analysis of a sample of STRs/SARs received from VASPs was consistent with previously mentioned findings. As illustrated in Chart 19, **online gambling platforms** enabled the observed increase in customers gambling using virtual assets. The most frequent approach used in subjects of STRs associated with money laundering suspicion was the use of layering and structuring of assets, followed by fraud schemes, including identity fraud, stolen cards and credentials, fabricated documents, and the employment of money mules.

Chart 19: *Top methods identified in the sample STRs/SARs analyzed*



Lastly, regarding the use of crypto mixers, tumblers, cross-chain bridging, and decentralized exchanges, the questionnaire data confirmed their use. At the same time, analysis of STRs/SARs received from VASPs implied a larger frequency, as indicated later in the next section. As for crypto swapping, while VASPs reported occasional or rare use of this method, swapping among cryptocurrencies was commonly observed in the analyzed STRs/SARs, especially those involving stablecoins.

Chart 20: *Frequent observed methods in VASPs' customer activities, according to the questionnaire*



7. PATTERNS AND TRENDS OF MISUSING VIRTUAL ASSETS

7.1. Fraud schemes and scam clusters

Fraud emerged as a primary concern among reporting entities, as indicated by questionnaire responses and focus group discussions, as well as by STR and SAR analyses. Reporting entities elaborated on different schemes involving their customers on social media (primarily Telegram and WhatsApp). Both VASPs and FIs highlighted various types of fraud they observed, including investment scams, Ponzi schemes, impersonation scams, website mirroring, advance fee scams, part-time online jobs, and social media likes-for-commission schemes. For example, an investment opportunity would be promoted, followed by creating a 'group chat' through a messaging application. The fraudster then targets one or two from a specific group, who will later fall victim to romance fraud or crypto investment schemes.

Another example is a fraudster who would lure individuals under the guise of a job opportunity, ask the targeted individual to open a wallet with a specific VASP, and then transfer the funds, mostly stablecoins, to the perpetrator's mule account(s). Similarly, after joining a social media group and earning commission from task fraud or social media likes, the individual will be onboarded to a fictitious platform where they can invest in misleading returns. The same approach would be employed until the user wants to withdraw the funds, and the user will be asked to provide a card or bank account, which will then be

stolen as part of a broader fraud scheme. Ultimately, practitioners also highlighted that fraud could still be carried out through traditional finance, with the proceeds then converted into virtual assets.

Many of the reported subjects by VASPs were linked to high-risk clusters identified as fraud shops or scams. In several incidents, said clusters involved thousands of addresses, sanctioned entities, P2P addresses, and scam clusters. Investment fraud and Ponzi schemes were also prevalent, according to associated open-source data. These transactions often involved rapid fund movement and large outflows, including immediate off-ramping or withdrawals to different addresses. Some reports illustrated transactions in very small amounts of crypto, but followed by larger outflows later. In certain instances, customers who received funds from scam-related clusters engaged in asset swaps to obscure the origin of those funds. Legitimate trading activity was generally absent in these cases.

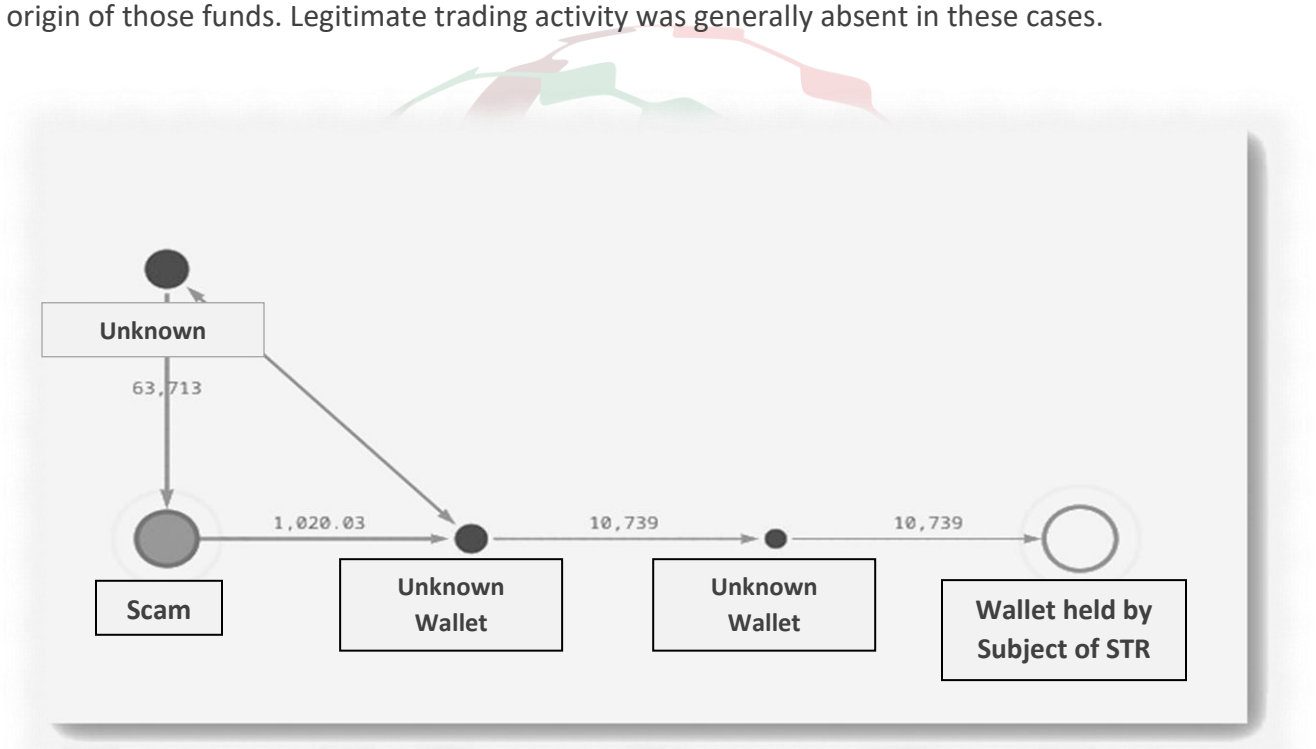


Diagram 1: *An example of a VASP's customer indirectly receiving funds from a scam cluster*

In a related context, numerous suspicious reports involved VASPs' customers who were victims of fraud and transacted with high-risk clusters or online platforms. Unlike the previously described fraudster-driven schemes, these cases lacked layering or complex fund transfers, typically involving direct, single-step connections to scam clusters. Victims were deceived into transferring virtual assets to entities they believed to be legitimate investment platforms. However, the receiving wallets exhibited characteristics of private wallets rather than those of regulated exchanges, suggesting the presence of fictitious or fraudulent investment schemes frequently promoted through online groups or platforms.

Some reports also addressed scams targeting VASP customers through phishing emails mimicking VASP's genuine emails, attempting to deceive users into updating account details or disclosing sensitive information, such as One-Time Passwords ("OTP"). Trusting the legitimacy of these emails, victims clicked the malicious link and provided their personal information (including OTPs), granting scammers unauthorised access to their accounts and facilitating swift fund withdrawals.

Similarly, among the examined STRs/SARs received from the banking sector regarding virtual assets, fraud and investment scams emerged as recurrent patterns. The reviewed reports consistently showed that subjects were either directly involved in fraudulent schemes or served as intermediary recipients that received and circulated the suspected fraudulent funds for layering and integration. Funds were moved across multiple personal and business bank accounts in rapid succession, demonstrating deliberate layering to obscure fund provenance. The analysis of accounts transactional activities frequently revealed possible concealment, transfer, and integration of illicit proceeds, linking investment fraud, social media scams, and Ponzi schemes to high-value asset acquisitions in the UAE (e.g., shares, VAs, and real estate). For example, a report from the banking sector indicated that a UAE-based individual (a student) received substantial inflows suspected to be derived from an overseas Ponzi scheme. The proceeds are alleged to have been laundered through virtual assets and property purchases.

Across other reports, similar mechanisms were apparent. Suspected fraudulent payments were fragmented across several mule accounts (as first or secondary recipient), pooled, and dispersed through unlicensed VASPs or foreign custodians, including cross-border flows.

Case example: Possible money laundering of a fraudulent virtual asset investment scheme

The UAEFIU received multiple STRs from different banks, concerning a foreign national who is a resident in the UAE. The said individual was the subject of adverse media reports and legal action in a foreign jurisdiction arising from a fraudulent virtual asset investment scheme. The subject lured investors to deposit funds intended for trading in cryptocurrency and promised high returns.

The UAEFIU analysis revealed that the subject's funds have been received from the subject's personal bank accounts based abroad. Afterwards, the fund was circulated between multiple domestic entities owned by the subject, in addition to the subject's personal account in the UAE. The transactional pattern indicated rapid inward and outward transfers (domestic and international) to obscure the source of funds.

Furthermore, the subject transferred/received large amounts to/from multiple third parties and family members in the UAE, Europe, and Asia. The funds were found to be integrated through the purchase of luxury vehicles, watches, and real estate, as the subject was also reported to the UAEFIU in different threshold reports (REAR and DPMSR).

Analysis and open-source also uncovered another associate, Subject B, who has the same nationality as the main subject, and was reported to the UAEFIU through STR, showing the same transactional pattern as the main subject.

Ultimately, the UAEFIU raised a request for information (RFI) to a counterpart FIU and disseminated the case to the concerned LEA for further investigation and action.

Risk indicators:

1. Adverse media on the subject linked to financial crime abroad.
2. Rapid movement of funds across multiple personal and corporate accounts without any economic justification.
3. Account turnover does not match the subject's profile as per the available documents.
4. The subject set up several legal entities in a short period of time without any clear economic purpose.
5. Lack of cooperation from the subject in providing the required supporting documents when asked by the reporting entity.
6. The source of funds, destination, and reason for transfers remained unjustified to the reporting entity.

7.2. Fraudulent documents to gain credentials and forgery

Within the same context as the previous concern, many reports received from VASPs showed a dominant pattern of customers using forged or fabricated documents during onboarding to the reporting entity to bypass KYC controls. Examples of these include IDs, passport copies, tampered trade licenses, forged proof-of-address documents, fabricated source-of-funds statements, and bank statements with modified balances, misspellings, typographical errors, and inconsistent dates. This is in addition to AI-generated passports.

Such documents often displayed inconsistencies and anomalies during registration, such as mismatches in gender, date of birth, or place of birth, or inconsistencies in the customer's selfie and passport photo or information. This scheme also included fabricated nationality (mostly of UAE citizens), in which the Machine-Readable Zone would show a nationality other than the UAE, a different ID number on the ID front, different signatures on the passport and ID, and low photo quality.

Many instances involved applicants submitting selfies that did not correspond to the photos on the identity documents provided, uploading passports or Emirates IDs belonging to unrelated individuals, or attempting to register multiple accounts under different names, nationalities, or dates of birth.

The analysis showed that reported attempts to onboard customers using fraudulent identities or forged documentation failed and were countered by VASPs, demonstrating strong early-stage detection. Other reports indicated more structured attempts, in which users initially registered under someone else's identity and later switched to their own documents after the reporting entity verification. More sophisticated or organised behaviour was indicated by applicants who reused the same selfie across multiple onboarding attempts with different identification documents, or attempted to create duplicate profiles using altered or modified IDs. Other incidents revealed the intersection between such a scheme and broader financial crimes, such as a job scam.

Ultimately, these instances strongly suggested an organised fraud scheme by criminal groups utilising fraudulent identifications and possibly constructed mule networks. Still, the use of forged documents or AI-generated IDs complicates tracing real individuals.

7.3. Unauthorized use of third-party banking cards

One of the most dominant patterns reported by VASPs was the unauthorized use of bank cards by third parties. Customers mostly purchased virtual assets using cards that did not match their names, followed by rapid withdrawals to external wallets.

It was noted that subjects attempted multiple deposits using several credit or debit cards issued by different banks, often within very short time windows. Many of these transactions were successfully blocked by VASPs before being processed on the blockchain, or flagged by fraud-detection solutions as suspected card-testing behavior. Nevertheless, some transactions were successfully processed. In all cases, customers were unresponsive or unable to validate card ownership and the source of funds. Analysis also indicated that some had ongoing ML or fraud cases recorded by UAE law enforcement authorities, in addition to subject's link to fraud suspicions reported by financial institutions to the UAEFIU.

Moreover, different reports suggested the use of money mules, particularly blue-collar workers. At the same time, only one incident indicated third-party transactions in which the source of funds was linked to a PEP during due diligence, based on the bank statement provided by the VASP's customer.

Discussion of the focus groups was consistent with the above-mentioned outcome of STRs/SARs analysis. VASPs noted the use of IDs owned by unrelated individuals to open accounts with VASPs, mainly orchestrated by gang leaders (controllers). These accounts are then used to steal funds from compromised credit cards and convert them into virtual assets. Virtual phone SIM cards (operated by a gang) are used to authenticate and control accounts opened under different individuals' names, mostly those of blue-collar workers. FIs highlighted that typical transactional activity in this scenario includes a sudden spike in amounts credited to the account, which is claimed to have originated from a P2P transaction, without presenting supporting documents.

7.4. Acting on behalf of a third party through P2P

One of the most frequently reported patterns, especially in the banking sector, involved individuals using their personal accounts to conduct high-volume crypto trading transactions, either for themselves or on behalf of others. These accounts typically exhibit rapid, high turnover, including cross-border activity, with total credits nearly matching debits, leaving minimal balances. Transactions were mainly characterized by credits from multiple unrelated individuals, self-to-self transfers from other banks, and cash deposits, followed by rapid outward remittances, ATM withdrawals, and payments to crypto-related merchants or exchanges.

In the majority of examined suspicious reports from the banking sector, the account activity was inconsistent with the customers' declared profiles. Many reported subjects were students or employees with modest monthly incomes, yet their accounts processed a significant volume of inflows and outflows, of which the source of funds remained unknown. For instance, a student's account received inflows from unrelated individuals, followed by immediate payments to a VASP-linked payment processor and large-value cash withdrawals, suggesting account trading in virtual assets. Similarly, an account of a low-income cleaner recorded large remittances from a multi-asset trading and crypto platform, which were swiftly dispersed to multiple beneficiaries.

Justifications such as 'personal investment', 'crypto salary', 'freelancing income', or 'crypto trading for friends' were common. However, with poor documentation, in many cases, it is limited to screenshots of exchange pages, chat messages, or informal statements rather than verifiable exchange records or proper transaction identifiers. More importantly, the actual source of the funds used to acquire or trade virtual assets was often unsubstantiated and remained unknown.

Simultaneously, other subjects acknowledged selling virtual assets on behalf of others, showing significant third-party inflows, or trading in general on behalf of relatives or associates. References such as 'buy USDT', 'crypto', 'P2P', and 'investment' appeared frequently in these transaction details.

Similar to the banking sector concern, multiple reports received from VASPs indicated transfers from subjects to P2P exchanges. The most common reason for filing suspicious reports is the inherent risk of P2P exchanges, which are frequently associated with crypto-money laundering typologies and lack of regulatory KYC requirements.

For example, a customer was reported for suspected structures of crypto-to-fiat off-ramping transactions. The subject appeared to be engaged in legitimate P2P trading but attempted to open multiple accounts with the reporting entity. Afterwards, the customer opened an account using a different identification document and was ultimately linked to many devices. Despite the customer's low income, the account witnessed significant USDT deposits and withdrawals within a couple of months of opening, suggesting the subject was employed as a mule using different pass-through addresses. At the same time, unusual activity involving deposits and P2P purchases was linked to fraud, and the customer had multiple accounts in violation of the VASP terms of service. Although the user had no risk exposures, a high volume of stablecoins passing through the account to exchanges was perceived as a high potential ML risk.

7.5. Virtual assets payment for online gambling

In the UAE, commercial gaming is regulated by the General Commercial Gaming Regulatory Authority (GCGRA), established by the 2023 Federal Law. Commercial gaming encompasses lottery, internet gaming, sports wagering, and land-based gaming facilities. All stakeholders and players should be aware of social repercussions and the regulatory, legal, and financial risks before engaging in, conducting, or facilitating commercial gaming activities in the UAE without a license.[35] The absence of licensing in gaming activities increases the risk of money laundering and other illicit financial activities.

Cryptocurrencies were noted to be used for gambling activities on a large scale, as gambling was the most prevalent concern reported in the examined STRs received from reporting entities (be it VASPs or FIs), wherein their customers, predominantly individuals, were linked to gambling clusters and platforms.

Among the examined suspicious reports received from VASPs, USDT was the most frequent currency, followed by BTC with lower frequency. The transaction pattern often shows rapid inflows and outflows,

[35] GCGRA (no date) Activities We Regulate. Available at: https://www.gcgra.gov.ae/en/commercial-gaming/activities-we-regulate/

and in many incidents, involves multiple wallets. It was noted that a customer would have multiple wallets with several local VASPs.

While the majority of the subjects had direct or close exposure to gambling clusters (often one to two hops), the use of multiple intermediaries, merchant services, decentralized exchanges, and 'no KYC exchange' was also common in different reports, and 'mixing service' in a few others. The majority of the reports suggested individual gambling behavior, but the latter implied a complex transaction chain that could be both linked to gambling or money laundering.

Some instances revealed further concerns filed on VASPs' subjects for other suspicions. For example, fraud involving multiple credit cards, with transactions subsequently flowing through private blockchain wallets acting as intermediaries. Those intermediary clusters were suspected, based on the analysis, to be used to obscure the origin and nature of funds before they reached gambling clusters.

Simultaneously, several banking sector reports confirmed the same concern, reporting transactions linked to online gaming and gambling involving virtual assets. The reviewed STRs showed that multiple individuals' accounts received credits from entities associated with digital payments and gaming services, along with inflows from several unrelated individuals, which the subjects described as 'gaming prizes' or 'online winnings'. In these instances, the accounts were also funded through high-value cash deposits and third-party transfers of unclear origin.

Transactional analysis indicated immediate outward transfers to other individuals, wallet payment processors, or VASPs, as well as dispersals through point-of-sale (POS) transactions linked to crypto trading and other gaming-related payments.

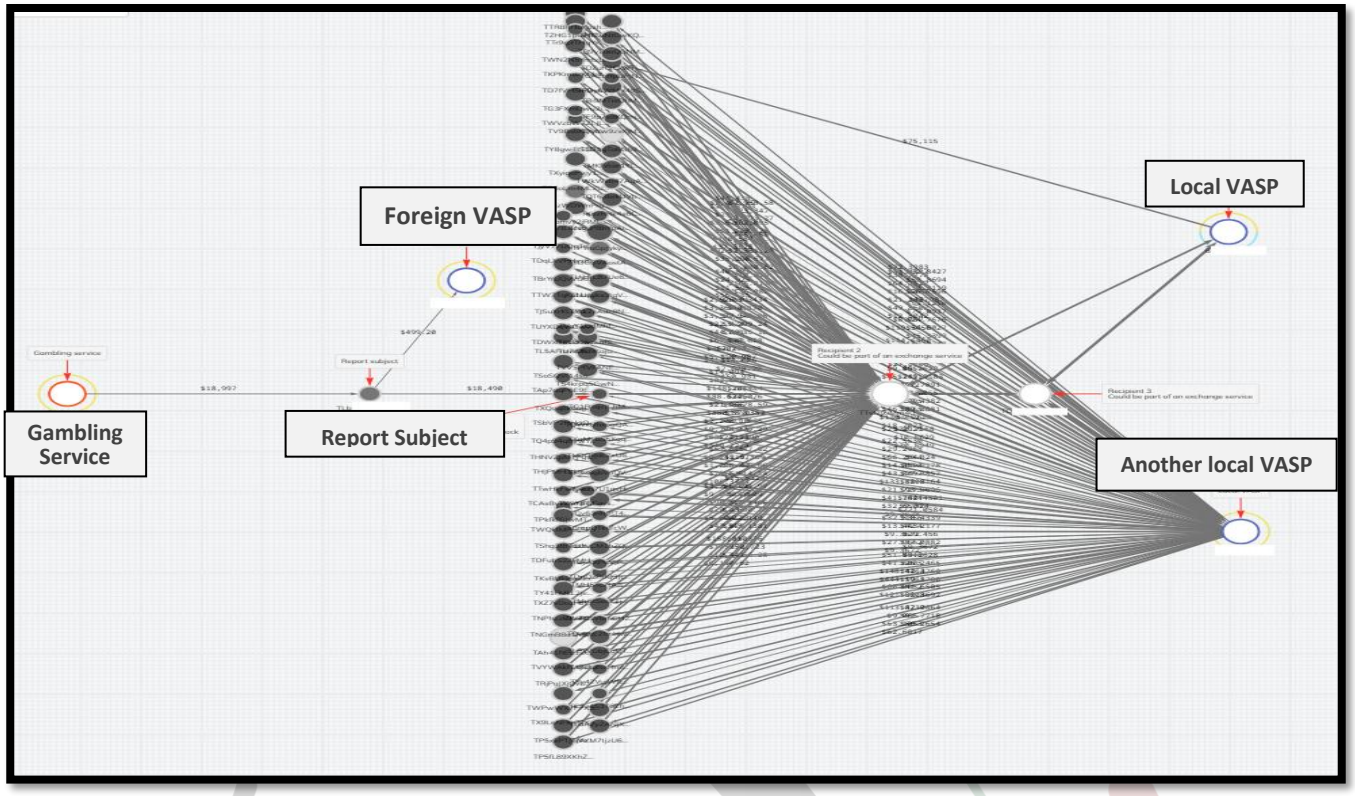


Diagram 2: *An example of the subject's multiple wallets linked to local and foreign VASPs, ultimately linked to a gambling cluster*

7.6. Exposure to high-risk clustered wallets

Analysis of multiple STRs linked the reported subjects to exposure with 'illicit actor organizations' (especially those that operate on Telegram channels), whether indirectly through multiple-hop chains that potentially obfuscate the origin of assets or directly through outgoing payments to labelled illicit payees. A frequent pattern observed in this context is the aggregation of small- to medium-sized funds through exchanges and high volumes of intermediary wallets, combined with rapid cross-asset conversions (e.g., BTC, LTC, DOGE, and stablecoins).

Similarly, multiple subjects were linked to high-risk clustered wallets such as 'Stolen Funds', 'Darknet Market', 'Fraud Shop', and 'Mixing Services', showing the same transactional pattern of small-to-medium transfers (mainly BTC or stablecoins). The majority of these reports related to scams or stolen funds had a moderate to weak connection. While some of these subjects were linked to adverse media, e.g., Ponzi schemes or other financial crimes, others could be knowingly or unknowingly associated with said clusters of criminally linked nodes.

An example of this is indicated below, where a customer conducted transactions towards a darknet market and a wallet heavily associated with stolen funds. Virtual assets moved through an intermediary address and wallet, which ultimately transferred to an identified 'stolen funds' address and 'stolen funds' wallet with multiple addresses within a short period of time. The addresses within the same wallet moved the assets rapidly and were observed to have made one deposit and one or two immediate withdrawals, indicating potential layering activity.

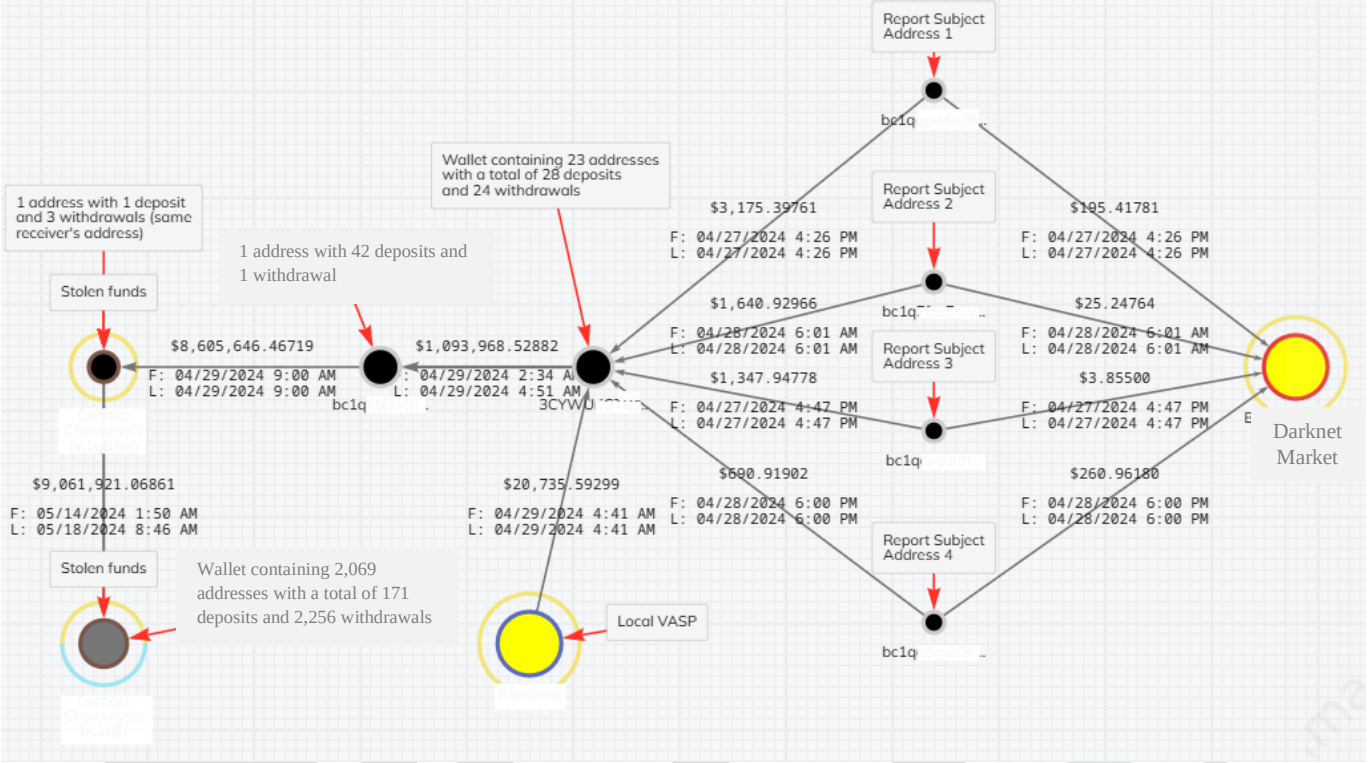


Diagram 3: *An example showing customer transactions linked to a darknet market, as well as multiple addresses and intermediaries linked to stolen funds*

7.7. Exposure to sanctioned entities and jurisdictions

Multiple reported subjects by VASPs were engaging in direct or indirect transactions with sanctioned entities/VASPs, or were potentially proxies of sanctioned jurisdictions by foreign regimes.

In most scenarios, structuring and routing patterns were observed through intermediaries, commonly with multiple hops, along with the use of decentralized exchanges, no-KYC exchanges, mixing services, and intermediary private and self-controlled wallets. Transacting in stablecoins was more common than in other currencies, but BTC and XRP were also observed with lower frequency, potentially enabling high liquidity through OTCs and cross-border value movement.

Case example: Using Fake IDs in Sanction Evasion

The UAEFIU received an STR from a local VASP concerning two customers (possibly spouses), Subject A and Subject B, for using fabricated UAE IDs to open digital wallets. These wallets were subsequently used to conduct multiple transactions, which were ultimately transferred through a crypto platform known for enabling sanction evasion in high-risk jurisdiction Country X.

The reported subjects mainly conducted large, rapid deposits in multiple cryptocurrencies, immediately followed by transfers and withdrawals to Country X. A significant amount of funds moved to Country X. The involved wallets were subsequently suspended by the VASP.

Following the UAEFIU investigation, it was concluded that the details of purportedly used UAE IDs were not found in government databases and were therefore determined to be fake. Based on the above, the UAEFIU has disseminated the case to the relevant LEA for further investigation and action.

Risk indicators:

1. High-velocity activity on large deposits and withdrawals within the same day with different cryptocurrencies.
2. Deposit a large amount of crypto from external wallet addresses, then swap to another crypto in a virtual asset exchange, and withdraw immediately.
3. Direct exposure to a virtual asset exchange located in a high-risk jurisdiction.
4. Unknown source of funds.
5. Forged official ID documents for the purpose of opening digital wallets.

In a few examined reports, the use of companies' accounts was also observed, showing an indirect link to incorporated cryptocurrency exchange(s) in a sanctioned jurisdiction. The VAs' withdrawals were made to the customer's external wallets, sourced from regular trading activities within the UAE. VAs used were mainly USDT on the TRON network. In such a scenario, it was common for the company also to be a subject of STR from financial institution(s) besides VASPs, highlighting a significant inward remittance from the company's UBO or a shareholder's personal account.

7.8. Market manipulation

Several suspicious reports received from VASPs highlighted transaction behavior that often indicates wash trading. One of the methods is for an account to be used repeatedly in buying and selling crypto against the same counterparty, which is the account holder themself. As a result, the individual artificially inflates the public volume of the cryptocurrency through cross- and wash trades, a form of market abuse and a prohibited trading practice.

Such concerns involved the misuse of legal persons and the use of multiple intermediaries and counterparties, transacting through both decentralized and centralized crypto exchanges and OTC purchases. An example of these scenarios is a licensed entity in a different line of business trading high-volume tokens, with an associated network of individuals and other UAE trading platforms. Significant internal transfers were observed between a subject (UBO) and its owned entities (including offshore entities), involving large amounts of crypto exchanges and OTC purchases of a particular token that operates on the Ethereum platform. The subject main entity frequently appeared in both buying and selling of its own trades, with significant, repetitive, and synchronized trade volume.

Similar examples involved general trading companies associated with other investors and DeFi platforms that aim to make cross-chain trading easy. An additional risk was the potential co-mingling of investors' funds with the client's personal wealth, as observed in relevant STRs reported by the banking sector.

Ultimately, virtual assets were sent to wallets and exchange accounts controlled by a subject entity and its associates, followed by distributions across numerous sub-accounts. The trading scale suggested a coordinated network of multiple accounts on the reporting entity platform, as well as a similar pattern on other licensed VASP platforms. The timing of conducted trades, detected device sharing, and IP addresses overlapped with the change in said token price, OTC inflows, large distributions, and circulated transactions among coordinated sub-accounts suggests deliberate intent to influence market price and liquidity.

Other reports indicated similar deliberate behavior with coordinated trade among counterparties, suggesting pre-arranged transactions. A common observed pattern was that traders were transacting at prices with greater variation than the market price, with consistent losses on one side while the other profited.

7.9. Money laundering

Different reports received from VASPs indicated potential money laundering involving virtual assets, primarily through layering and structuring. These assets were suspected to be proceeds of corruption, tax evasion, stolen tokens, and drug trafficking,[36] based on analysis of suspicious reports, open-source research, and the focus group discussions. In such cases, layering of funds is typically observed through multiple exchanges and intermediaries, decentralized platforms, and no-KYC exchanges, as well as extensive use of cross-chain swaps.

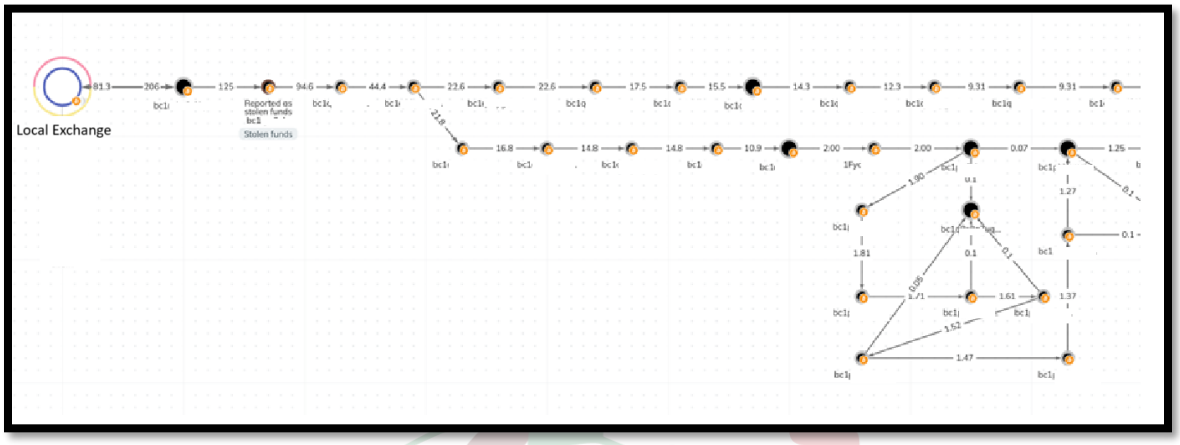
The analysis of STRs illustrated high-velocity layering and large deposits followed by rapid withdrawals in a structured manner, including repeated round-amount deposits or split withdrawals. Several transactions also involved intermediary clusters that were suspected of functioning as pass-through wallets. Some of the subjects involved in this scheme were also linked to sanctioned entities and were suspected of being beneficiaries of fraudulent proceeds.

Another observed approach involved non-customers transacting with each other at different market prices (similar to TBML over/under pricing, but in crypto) while sharing the same IP addresses, suggesting using the same VPN service. Other observed concerns across multiple reports included the use of high-value funds with unknown source of fund (SOF) or source of wealth (SOW) and the use of intermediaries, prompting reporting entities to enhance due diligence due to suspicions of potential money laundering.

In the majority of examined transactions, structured fiat-to-stablecoin cycling was observed, with most subjects rapidly converting between fiat (often via card-funded deposits) and stablecoins over a short period (e.g., minutes or hours), leaving their accounts in a zero balance. Similarly, the user would execute a sale transaction on the platform, converting crypto to stablecoins. Subsequently, the stablecoin will be transferred to an external, unidentified wallet. In some cases, wallets at certain VASPs appeared to be used solely to deposit fiat to acquire VAs or to receive VAs and then convert them back into fiat, in significant amounts. Ultimately, this pattern showed multiple originators and the involvement of intermediaries, while maintaining the same beneficiary.

A few STRs linked VASPs' customers to funds identified as hacked or stolen on the blockchain. Involvement of unhosted wallets and cross-chain swaps was a common technique in these transactions. An example is highlighted below, illustrating the passage of stolen funds from a local VASP through an intermediary, followed by a series of peeled transactions, and finally reaching another local VASP.

[36] The next section provides additional information on potential drug trafficking (vendors).



Peel chain continues …

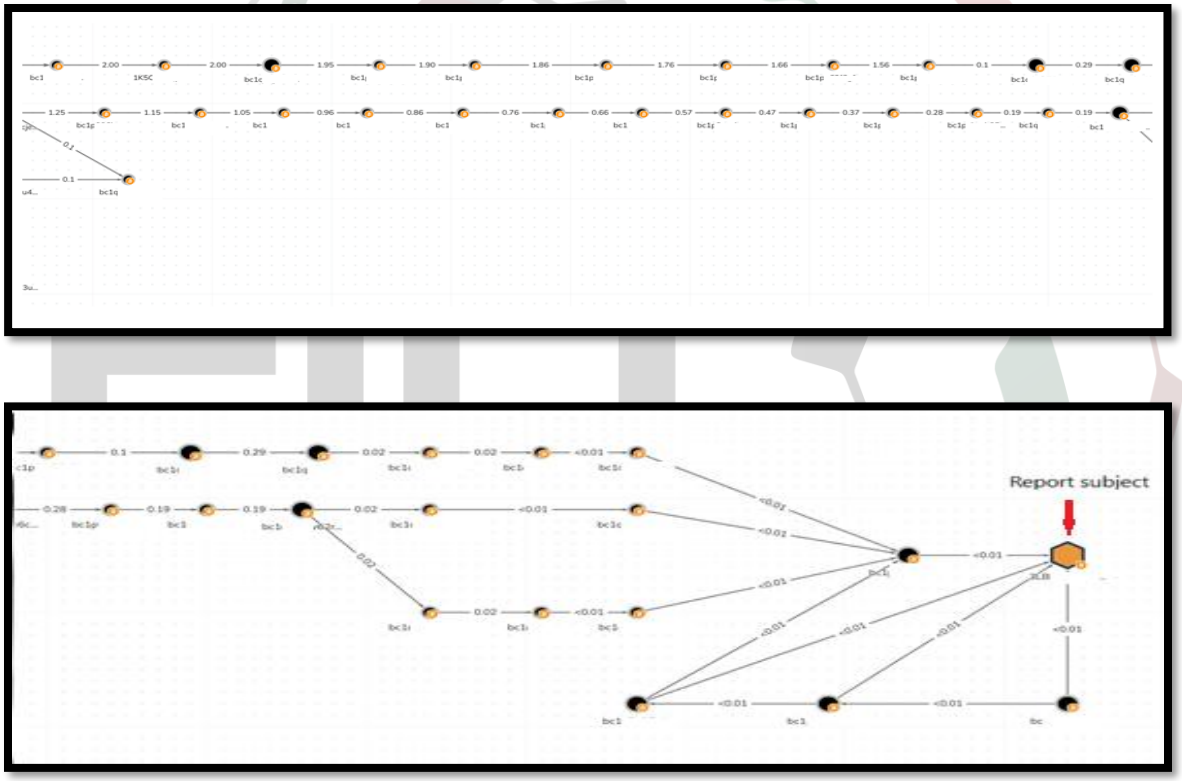


Diagram 4: *An example of a peel chain of stolen funds*

Overall, the majority of reviewed transactions had indirect exposure with high-risk wallets. Additionally, the use of multiple cards to purchase the virtual assets was also frequently observed, often with non-cooperative or non-responsive customers. Open source also enabled, in multiple cases, linking the

customer to financial crime or money laundering schemes. An unknown source of funds was common in the examined reports, with multiple reporting entities (FIs and VASPs) raising the same concern on the same subject.

Similar to VASPs, analysis of STRs/SARs received from FIs revealed recurrent structuring and layering techniques possibly used to disguise the source and trail of funds, with many instances linked to unlicensed virtual asset trading and/or fraud-related activity.

The reviewed transactions in many reports highlighted multiple structured, small, or rounded cash deposits via CDMs/ATMs by multiple depositors, frequently using different Emirates IDs, followed by rapid internal transfers and outward remittances to unrelated third parties or crypto exchanges. These flows typically left minimal balances and lacked a legitimate economic rationale, suggesting the accounts were being used as temporary conduits for placement and layering rather than genuine purposes.

The layering stage was frequently executed through domestic fund transfers or cross-border movements, creating a multi-jurisdictional trail that fragmented traceability. Several other reports demonstrated similar circular fund flows, using fintech intermediaries and payment gateways, as well as foreign investment or trading platforms, to move value between jurisdictions. Funds were often dispersed to or through high-risk destinations with oversight gaps and limited traceability. In parallel, broad and random transaction references were used, such as 'charitable contributions', 'good luck', and explicit crypto references like 'For USDT', or 'crypto income'. Explanations provided by subjects in most reports were unsupported by documentation or fabricated, while many subjects failed to respond to due diligence requests initiated by the reporting entities.

7.10. Crowdfunding through VAs with TF link

The UAEFIU issued its strategic analysis report on terrorist financing typologies and trends in May 2025, wherein all reported TF-related STRs/SARs received by the UAEFIU during 2021-2024 were analyzed. While no strong pattern was identified regarding virtual assets, there were indications of links between some reporting entities' customers and terrorist individuals/networks, or high-risk jurisdictions of conflict. Observed scenarios included suspicions that a cryptocurrency address/wallet (owned by a subject of STR/SAR) may be controlled by a designated terrorist individual/group or used to transfer funds in the form of digital currency within the network/counterparties.[37]

For the purpose of this report, further examination of the TF link to virtual assets continued. As a result of this analysis, a few STRs/SARs reported by VASPs showed funds routed via a few or multiple hops to

[37] UAEFIU (2025) Terrorist Financing: Typologies and Facilitators. Available at: www.uaefiu.gov.ae/en/more/knowledge-centre/publications/trends-typology-reports/strategic-analysis-report-on-terrorist-financing

labelled terrorist fundraising and seizure-list wallets, whether through the tracing tool or OSINT. Transactions were noted in low value, with direct outbound transfers from customers or intermediaries in the UAE to those labelled wallets (mostly in USDT on the TRON network). Limited scenarios also showed a customer's counterparty linked to a potential TF-related cluster, while the cluster itself was receiving from another TF-related (sanctioned) cluster. In rare incidents, a link to a gambling cluster was also observed. However, no concrete relationship or pattern could be established.

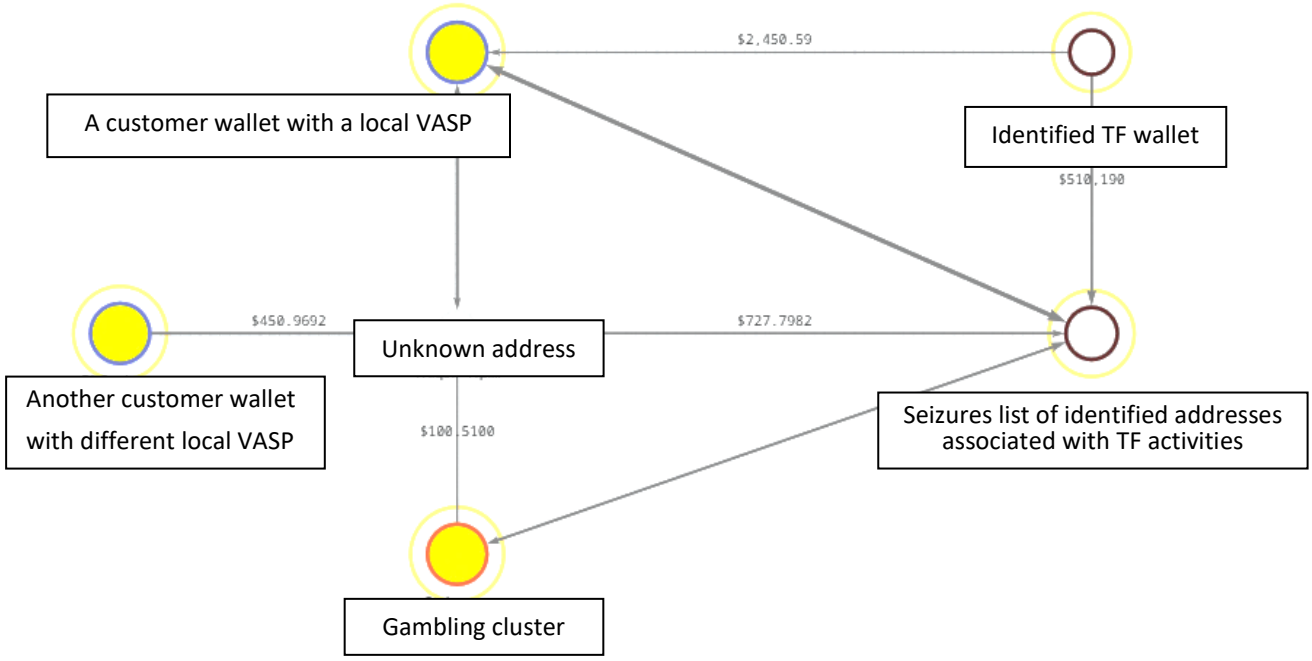


Diagram 5: *An example of transactions associated with two customers of two different local VASPs linked to the TF wallet*

7.11. Drug vendors

The UAEFIU published in August 2023 its strategic analysis report on drug trafficking and the laundering of its proceeds, in which a sample of STRs/SARs reported by VASPs was examined to explore a potential link between drug trafficking and virtual assets.[38] The sample was found to be indirectly relevant, indicating transactions with indirect links to dark web markets known for drug trading. However, the

[38] UAEFIU (2023) Patterns of Abusing Financial Institutions in "Drug Trafficking and Laundering its Proceeds". Available at: www.uaefiu.gov.ae/en/more/knowledge-centre/publications/trends-typology-reports/patterns-of-abusing-financial-institutions-in-drug-trafficking-and-laundering-its-proceeds

analysis could not establish whether the subjects were actually trading in illicit drugs or were merely transferring or receiving virtual assets without being aware of any criminal activity, as the transaction amounts were insignificant, and the customers' accounts had no balance. The majority of said dark websites were also shut down globally by law enforcement authorities in different jurisdictions.

For the purpose of this report, the UAEFIU continues to explore the probability of such a link between drug trafficking and the misuse of virtual assets in such trade. Nevertheless, the results remain inconclusive. Only a few suspicious reports showed customer indirect exposure to clusters identified as 'drug vendor' or a strong connection with an 'online pharmacy' entity, suggesting a resident customer of a local VASP potentially purchasing drugs while abroad for personal use. Others were linked to possible drug trafficking based on adverse media and screening, or transactional behaviour. For example, an applicant attempted to complete onboarding through an on-ramp partner of a VASP, but was found to be a subject of an open source signifying a criminal case involving possession with intent to supply drugs and production of cannabis.

7.12. Piracy and copyright infringement

No pattern was identified in this regard. However, few reported incidents involved transfers to clusters associated with unauthorized Internet Protocol Television (IPTV) services[39] that enable illegal access to copyrighted content. While the primary behavior may relate to digital piracy, such operations are frequently linked to broader fraud and cybercrime suspicions and, in some cases, to money-laundering risk, particularly where clusters show large volumes of activity.

7.13. Kidnapping and hacking

No suspicious reports were received, but the focus group participants discussed international fraud scheme scenarios at the global level, including some media articles published about the kidnapping of VASP members or account holders and hacking their accounts.

[39] IPTV services are unauthorized streaming services that provide access to copyrighted content without proper licensing or permission, often at a lower cost than legitimate services.

8. SUBJECTS PROFILE AND INVOLVED SECTORS

8.1. Individuals acting on behalf of third parties

A frequent pattern observed in many suspicious reports received from both VASPs and the banking sector highlighted reporting entities' customers acting on behalf of third parties in relation to virtual asset trade. In some incidents, customers acknowledged that they had transacted on behalf of others or that the funds originated from a relative. In such a scenario, the customer would receive repeated inbound crypto deposits from multiple exchanges and transfers routed through major centralized exchanges.

8.2. Third-party control

Within the context of previously identified individuals, a similar pattern emerged from a few reports suggesting unauthorized third-party control, in which individuals other than the customer appeared to be operating or influencing the account. While some customers explicitly confirmed to the reporting entities the involvement of third parties, other cases often surfaced when users attempted to change critical security credentials, such as registered email addresses or authenticator settings.

Additional concerns stemmed from device-level and behavioral anomalies, including devices linked to multiple unrelated accounts previously frozen for suspicious activity, login attempts from foreign jurisdictions inconsistent with the customer's stated residence, and device time zones set to geographically distant regions — indicators of remote access, session spoofing, or shared-device usage within organized networks.

8.3. Money mules

Money mule activity was observed in multiple suspicious reports and was addressed by the participants of the focus group discussions. These mules primarily involved low-income and young individuals with limited financial capacity and no experience with virtual assets (e.g., blue-collar and non-resident students), whose personal accounts were used to receive and transfer funds on behalf of others, most often engaged in P2P transactions and unlicensed crypto-trading, or served as intermediaries for ML/Fraud.

The reviewed reports received from the banking sector revealed repeated credits, both cash and wire transfers, from multiple unrelated individuals and, in some cases, trading platforms, where the account holder (the mule) acted as a temporary receiver of funds, followed by immediate withdrawals or outward remittances. These recurrent inflows and rapid outflows indicate that the accounts served as intermediary channels while concealing the true beneficiaries of the funds. The lack of balance retention

further revealed that these accounts were not used for legitimate personal or business purposes but rather served as transit points.

In several reports, involved individuals (mules) appeared to have been recruited or compensated to move funds, as reflected in transaction narratives such as 'assisting friends'. Others claimed ignorance or were unable to justify the sources or purposes of transactions, offering explanations that were either ambiguous or contradictory. For instance, one report involved two counterparties: one described the purpose of the transfers as 'luxury goods trading', while the other claimed they were crypto-related transactions. In another report, a freelance coordinator used their personal account to collect funds locally from multiple individuals and forward them to a high-risk jurisdiction, after which the funds are purportedly sent to various beneficiaries for crypto purchases.

Similar transactional and behavioral patterns were also observed in another set of reports showing pass-through or funnel account activity, in which accounts exhibited rapid turnover, small, structured deposits, and immediate outflows. While not always explicitly recognized as money mule cases, the accounts demonstrated the same functional characteristics, serving as temporary conduits for third-party funds.

Regarding suspicious reports received from VASPs, different STRs suggested the potential use of money mules (blue collars) or other individuals in relation to fraud shops or clusters identified as scams, mostly linked to known fake trading platforms. These accounts with VASPs illustrated account behavior as a pass-through and the layering of assets. Some of these transactions had direct exposure to the scam entities, and the funds were ultimately withdrawn to multiple external addresses. Other transactions showed VASP's customers receiving funds from the scam entity via intermediaries (multiple hops via on-chain deposits), which were subsequently transferred to other external addresses.

Transactions were also observed to be conducted from multiple IP addresses located in different jurisdictions. Moreover, other accounts/wallets transacting through the same virtual asset service providers also exhibited the same suspicious behavior, including a scam using the same device.

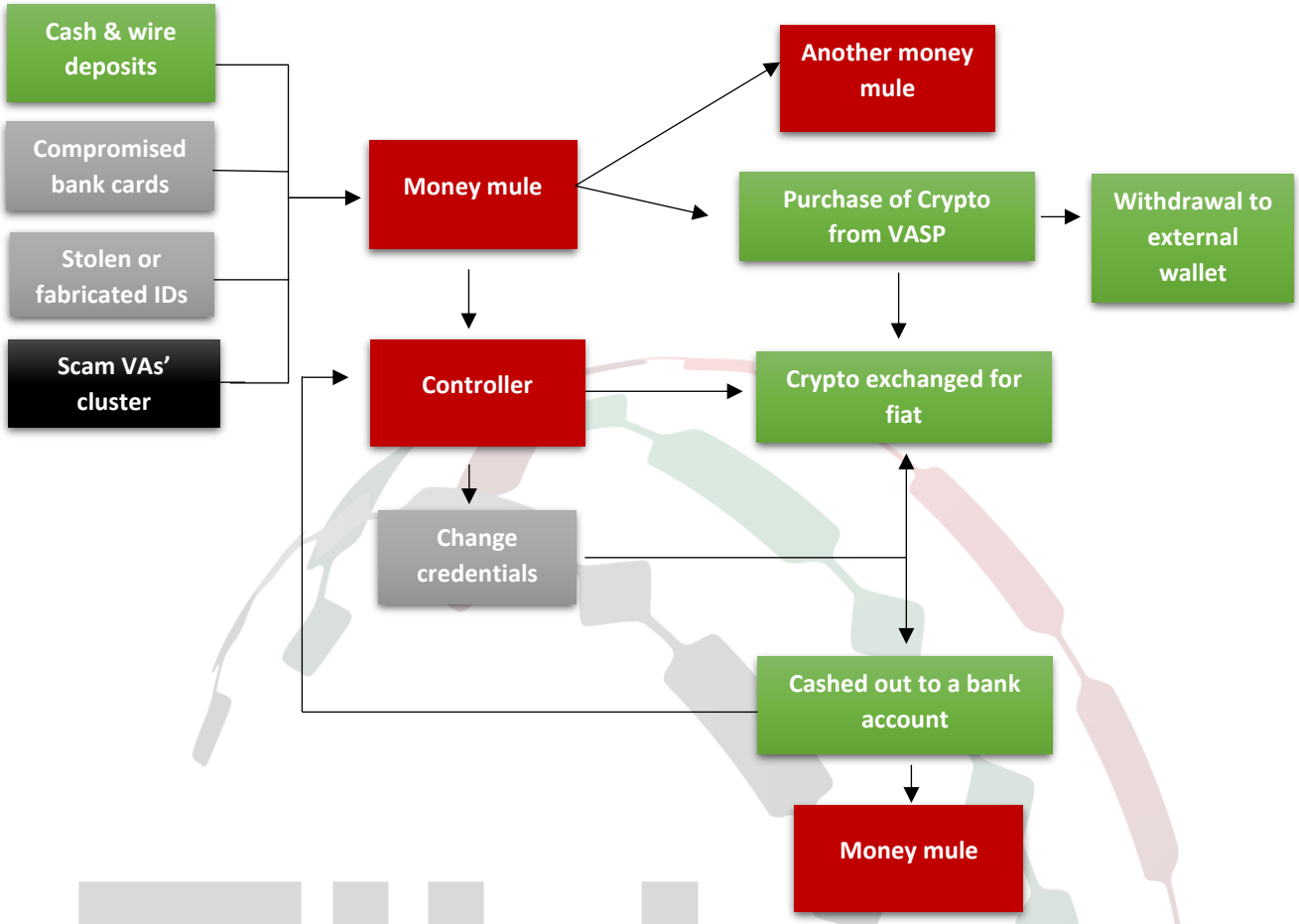


Diagram 6: *An illustration of money mule patterns observed in the examined VA-related STRs*

8.4. Organized Crime Groups (OCGs)

Organized crime groups were mostly suspected of involvement in the layering of illicit proceeds, fraud and scams, and the recruitment of mules, among other activities.

8.5. Politically Exposed Persons (PEPs)

No pattern was observed in the analyzed data relevant to PEPs and the misuse of virtual assets, except for only one incident, indicating a pass-through pattern (deposit and immediate withdrawal) within a close timeframe (e.g., same day) of unexplained high-volume of exchanges, combined with the use of decentralized exchanges, bridges, and OTCs.

8.6. Individuals with high-risk profiles linked to financial crime

Multiple suspicious reports illustrated the involvement of high-risk customer profiles who were subjects of adverse media and criminal investigations abroad. Concerns raised by these reports included links to corruption, crypto Ponzi schemes, investment fraud, other scams, and allegations of money laundering.

The majority of these subjects could not explain the source of funds to the reporting entity, and stablecoins were commonly used in reported transactions. Moreover, some of these subjects were found to have dual nationalities, and others had family-linked transactions to designated persons.

8.7. Unlicensed practice of trading in virtual assets

One of the most prevalent patterns in the analyzed data involved both individuals and legal entities providing virtual asset services and activities without obtaining the required regulatory license or authorization. The related bank accounts typically received inflows referencing 'buy/sell USDT', 'crypto trading', 'commission', or 'financial services', followed by immediate outward transfers to multiple virtual asset exchanges or merchants, indicating facilitation rather than personal investment or regular business activity.

A. Unlicensed Crypto traders and brokers

Several customers revealed to the reporting entities engaging in brokerage trading of virtual assets on behalf of others, often describing themselves as 'crypto traders' or 'merchants' despite not holding any regulatory license. These individuals facilitated 'fiat to crypto' conversions and the settlement of third-party crypto trades, frequently comingling prospective client funds with their personal balances.

A frequently observed pattern showed subjects receiving funds from multiple unrelated parties, immediately converting them into virtual assets, and rapidly withdrawing or transferring them to multiple external wallets linked to major exchanges, along with occasional involvement in high-risk P2P transactions. These transactions often showed unidirectional flows toward large centralized exchanges and multiple output addresses, with no legitimate commercial rationale.

B. Unlicensed VASPs and misuse of legal persons

Overall, the majority of reviewed suspicious reports involved NPs rather than LPs. However, several reports involved LPs and were commonly relevant to entities licensed for other business activities, such as IT and software services, digital media and internet services, marketing and management services, and, occasionally, other retail-related activities registered in both free zone and mainland jurisdictions. These legal persons engaged in high-value flows beyond their declared business scope, and transacted

heavily with individuals rather than other businesses, indicating that these accounts were being repurposed for unlicensed payment processing or crypto-related brokerage functions rather than legitimate commercial activities.

Typical profiles involved entrepreneurs or free zone companies receiving frequent third-party deposits, executing high frequency outward transfers, and maintaining minimal operational expenditures, consistent with payment-processing activity. An observed example involved a free zone entity that channeled a large volume of funds through a combination of personal and corporate accounts under the label 'crypto trading'. Although this pattern shares similarities with the previous concern about unlicensed individuals trading in crypto, it differs in legal persons' practices, with significantly higher transaction volume and a larger number of counterparties and third parties. It also often shows higher frequency and instant transaction processing.

Furthermore, several legal persons continued conducting virtual asset-related transactions/activities despite the expiry or suspension of their trade licenses. In addition, some foreign-based online platforms were found to market in or offer cryptocurrency exchange services in the UAE without obtaining the required approvals or authorizations from the competent regulatory authorities.

Data also highlighted inconsistencies in business activities for some reported subjects. For example, oil and gas, foodstuffs, restaurants, general trading, and other retail businesses, possibly providing unlicensed OTC services (e.g., mirroring unlicensed hawala practices in crypto) or operating within broader schemes such as sanction circumvention. Focus groups also highlighted the observed practice among participants of holding companies to hold assets on behalf of others and trade in cryptocurrencies (however, this was not observed in the analyzed STRs/SARs).

Lastly, it was noted that misuse of legal persons occurred when the UBO of an entity was the subject of a suspicious report, the entity served as the SOF/SOW, and other employees within the same entity provided a salary as the SOF.

Case example: Unlicensed Virtual Asset Service Provider

The UAEFIU received multiple reports from banks and VASPs concerning Subject A, a UAE resident. Subject A is also the sole owner of an entity licensed for digital services on the mainland, Company A. The subject is running an unlicensed virtual asset service, wherein both personal and company accounts received funds from multiple individuals based in Country X. Concerns also raised about Subject A's sibling, Subject B, due to similar activities.

The UAEFIU's analysis of the subject's personal and business accounts revealed several inward transactions from Country X, made by different individuals. A portion of the funds was transferred to a UAE-licensed VASP and to foreign VASPs. Funds were noted to be moved circularly to Subject A and Subject B's personal accounts, in addition to other third parties in the UAE and abroad.

The turnover in both business and personal accounts significantly exceeded the customers' declared income. Several reporting entities also raised fund recall requests regarding some inbound fund transfers received in Subject A's personal and business accounts, due to suspected fraud.

Furthermore, the subject's transactions through the UAE-based VASP highlighted indirect sending exposures to a cryptocurrency exchange based in a high-risk jurisdiction. As a result, the UAEFIU disseminated the case to the concerned competent authority for further investigation and action.

Risk indicators:

1. Multiple inbound transactions of unknown source of funds from multiple third parties.
2. Fund recall requests related to possible fraud.
3. Rapid movement of funds through multiple personal and business accounts without any economic rationale.
4. Turnover does not match the customer profile.
5. Exposure to high-risk cryptocurrency exchanges.

8.8. Correlation with real estate transactions

The UAEFIU published its strategic analysis report on real estate money laundering typologies in December 2023, highlighting suspicious transactions involving inward funds that ultimately directed toward purchasing both real estate and virtual assets, wherein outward remittances to both real estate firm(s) and VASPs (licensed or unlicensed) were noted. The analysis also reported a pattern of customers' tendency to buy several off-plan properties using cryptocurrency (e.g., via P2P cryptocurrency transfers) without disclosing the source of funds, even though the property values are inconsistent with the clients'

ages and professions. Therefore, the possibility of a customer acting on behalf of another person to purchase a property in the UAE using virtual asset payments was concluded.[40]

Analysis conducted for this report, in addition to the focus group discussion, supported the correlation between the real estate sector and VASPs across multiple reviewed transactions, combined with the misuse of manager cheques and the involvement of unlicensed services, such as unlicensed (crypto) hawala services. For example, some transactions were potentially flowing to a real estate developer from a customer, while the customer's wallets exhibited an exposure to sanctioned jurisdictions, entities, or a known scam address. In such a scenario, the risk was not linked to the involved developer, but rather the on-chain counterparties' exposure.

Analysis also showed that some real estate developer(s) were using crypto mixers. Account transactions were significant in volume and total value, which might indicate accepting customer crypto in VAs or investing in the field. Nevertheless, using a mixer that involves a high amount of funds appears suspicious.

8.9. Dealers in Precious Metals and Stones (DPMS)

No pattern was observed in the analyzed STRs/SARs regarding the misuse of DPMS in potential financial crimes involving virtual assets, except in the focus group discussions, where some participants described an emerging practice of DPMS involvement in converting fiat into virtual assets for a commission.

9. IDENTIFIED CHALLENGES IN TACKLING THE MISUSE OF VIRTUAL ASSETS

This section outlines the primary challenges identified through a questionnaire and focus group discussions, as previously indicated in this report's methodology. The following factors focus on different operational and technical obstacles discussed by practitioners in the field of financial crime prevention. Proposed solutions and recommendations will be addressed in the next section.

9.1. Difficulty in tracing and identifying beneficiaries

Responding to whether VASPs are facing difficulty in tracing the ultimate destination of their customer transactions, 35 out of the 37 respondents to the UAEFIU questionnaire confirmed that they have not encountered any challenges in this regard. As for the remaining two VASPs, they highlighted different scenarios in tracing the ultimate destination of their customer transactions, such as:

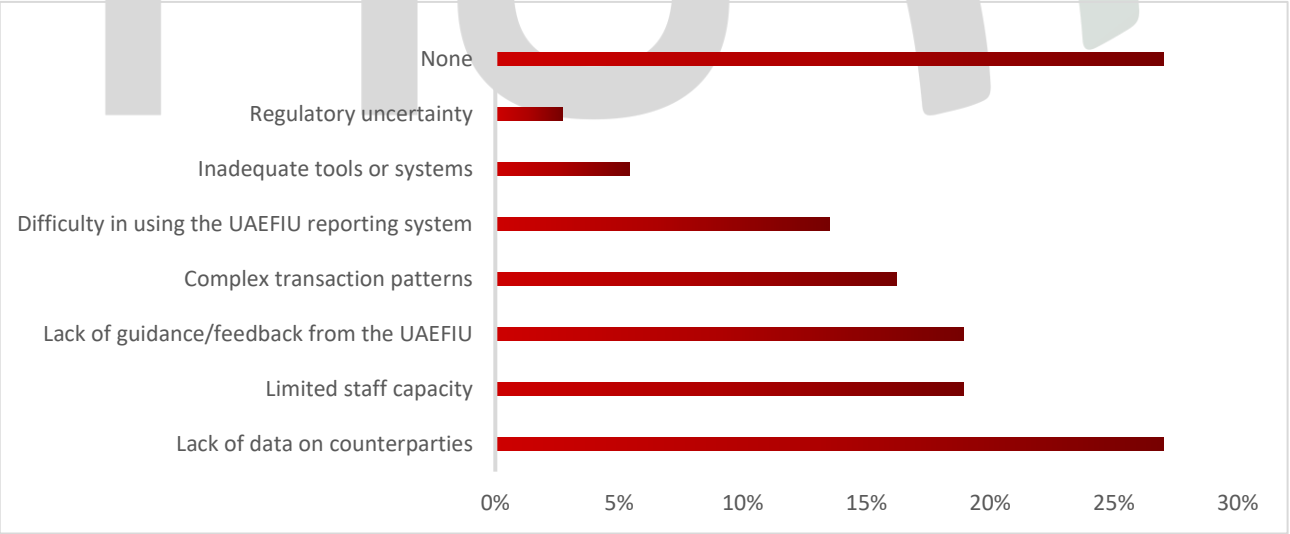
[40] UAEFIU (2023) Real Estate Money Laundering. Available at: www.uaefiu.gov.ae/media/omqb4a1z/real-estate-money-laundering-typologies-and-patterns-dec-2023.pdf

- Use of non-custodial wallets: When transactions are routed to self-hosted wallets, it makes it difficult to identify the end beneficiary or determine whether the destination is associated with a regulated entity.
- Cross-Chain swaps and bridging protocols: Customers increasingly use DeFi platforms and blockchain bridges to move assets across chains, creating fragmented audit trails and complicating end-to-end traceability.
- Layering via multiple exchanges: Funds are often moved through a series of centralized and decentralized exchanges, sometimes across multiple jurisdictions, which delays or limits VASP's ability to trace ultimate destinations without external cooperation.
- Use of obfuscation tools: In some cases, customers use mixing/tumbling services or privacy-enhancing technologies specifically designed to conceal transaction flows.

9.2. Challenges in Reporting

Concerning challenges facing VASPs in reporting suspicious activities and transactions of their customers, Chart 21 highlights that the lack of data on counterparties is the most significant challenge in providing effective suspicious reports that enable the UAEFIU to act, followed by staff capacity and the lack of sufficient guidance or feedback from the UAEFIU. The UAEFIU has acknowledged these issues and, through its operational plan, aims to enhance engagement with VASPs by increasing outreach sessions and meetings, both individually and in roundtable formats. These efforts complement the ongoing roles of supervisory and regulatory authorities in providing guidance and feedback to VASPs. Additionally, this report offers feedback to VASPs on their suspicious reports in the conclusion section, followed by scheduled face-to-face sessions.

Chart 21: *Challenges in identifying and reporting suspicious activities/transactions, as responded by VASPs*



9.3. Challenges in applying the FATF Travel Rule

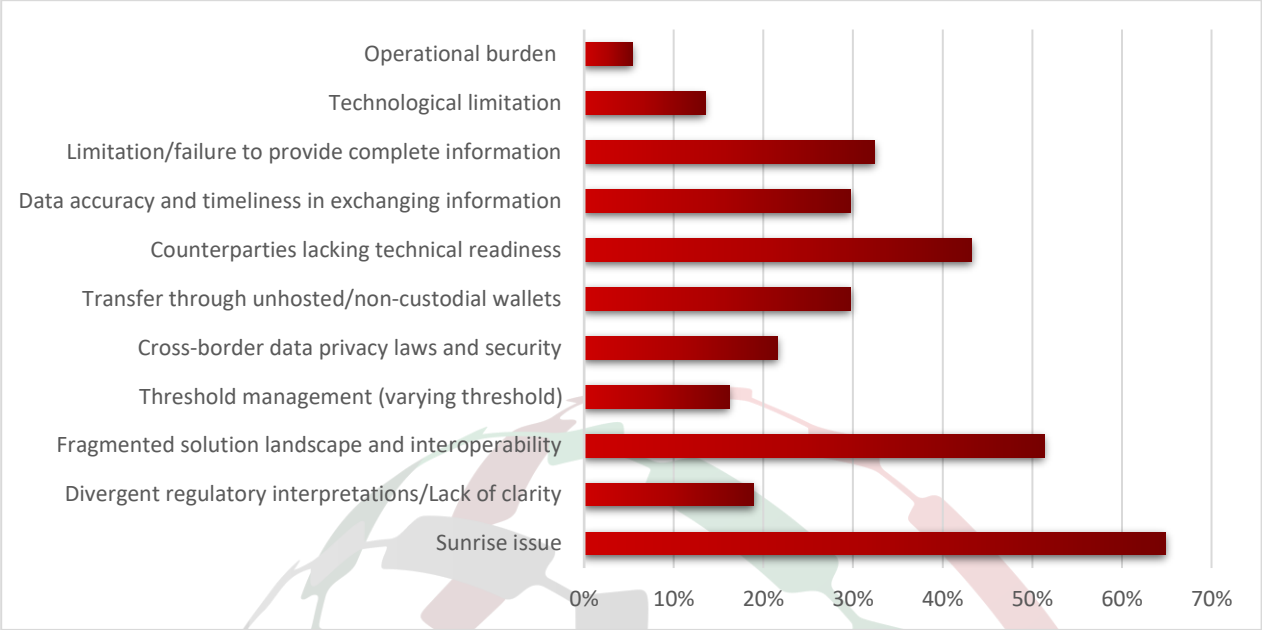
Applying the FATF Travel Rule remains a challenge to VASPs, whether domestically or globally. According to VASPs, there are still various obstacles to fully and effectively complying with all aspects of the FATF Travel Rule. Among these obstacles, the global regulatory mismatch (known as the "sunrise issue") is highlighted by VASPs in their responses to the UAEFIU questionnaire, as it creates uncertainty and compliance gaps when one jurisdiction requires information sharing, while another does not. In contrast, the counterparty jurisdiction does not yet mandate or support such requirements.

Another obstacle in this context is the fragmented landscape and the need to ensure interoperability between different VASP systems and protocols when dealing with counterparties in jurisdictions that have not yet implemented or enforced the Travel Rule. Moreover, VASPs highlighted the lack of interoperability between Travel Rule solution providers and the absence of a universally adopted technical standard, leading to the use of different technical protocols and systems, causing interoperability issues, delays in information sharing, and barriers to compliance.

The above-mentioned obstacles were also linked to challenges with VASPs' counterparties, which vary in compliance and capacity. As indicated by VASPs, in several cases, counterpart VASPs are either not Travel Rule-compliant or operate in jurisdictions where Travel Rule enforcement is limited, which results in manual processing of certain transactions. Additionally, regulators across jurisdictions have adopted varying interpretations and requirements regarding the Travel Rule, e.g., with different thresholds and data requirements. This lack of harmonization leads to inconsistencies in compliance obligations, creating significant operational complexity for VASPs operating internationally.

Furthermore, variations in data privacy and security requirements add another layer of concern for VASPs, especially given the absence of a universally accepted technical standard for sharing personal information when required to transmit personal data cross-border with VASPs in jurisdictions that might have inadequate data protection laws. These requirements may be complex, as privacy expectations and legal frameworks vary.

Chart 22: *Challenges in applying the FATF Travel Rule, as responded by VASPs*



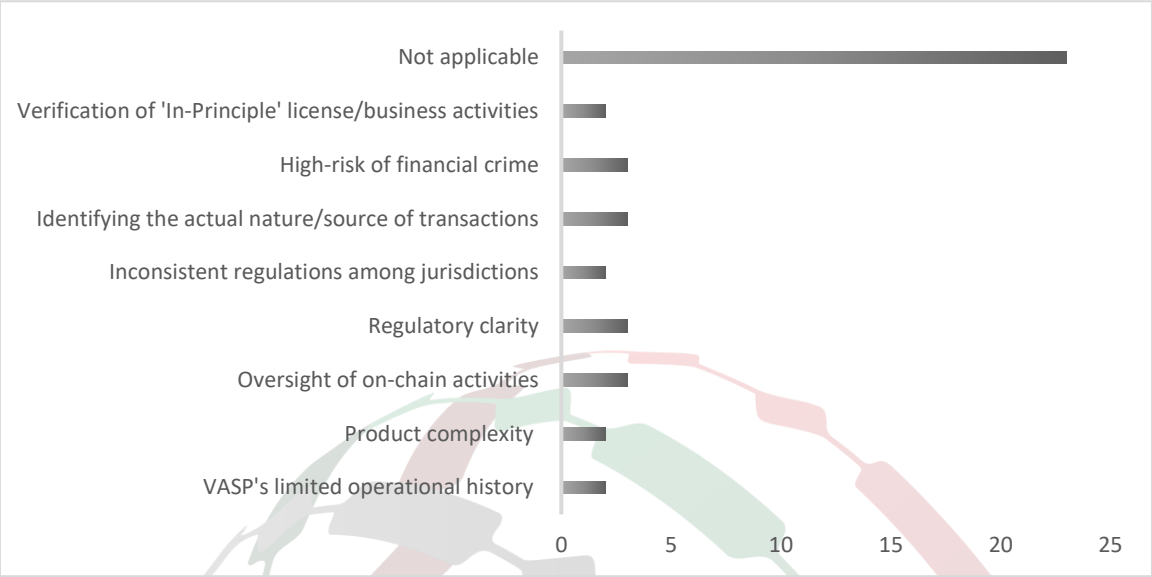
9.4. Business risks and challenges

VASPs highlighted that different market risks are not treated or prioritized at the same level of compliance risk, such as operational, cyber, credit, fraud, and pump-and-dump risks. Consumer protection must also be considered.

Both VASPs and banks identified core challenges inherent to the virtual assets ecosystem. One key business barrier is the establishment and maintenance of relationships between VASPs and banks. During focus group discussions, VASPs highlighted the tendency of some financial institutions to de-risk VASPs, despite regulatory requirements mandating that VASPs maintain on-ramp and off-ramp mechanisms. Consequently, relationships with financial institutions are essential.

On the other hand, banks explained the high risk associated with the virtual asset sector, which impacts their internal policies for onboarding VASPs. Data collected from the questionnaire indicated that 86% of respondents in the banking sector (55 out of 64) do not maintain a business relationship with VASPs due to bank policy, which is not aligned with their risk appetite. The remaining 14% hold limited Client Money Accounts (CMAs) for UAE-regulated VASPs, or maintain VASP accounts for administrative and operational purposes, such as rent, salaries, and utility bill payments. Chart 23 further explores perceptions of risk from the banking sector's perspective, including operational maturity, risk management, and regulatory uncertainty.

Chart 23: *Challenges in maintaining banks' relationship with VASPs*[41]



9.5. Main challenges encountered in effectively disrupting criminal activities

VASPs and banks' practitioners illustrated several challenges currently encountered in effectively disrupting suspicious activities and transactions potentially misusing virtual assets in financial crime schemes:

Features of virtual assets that make tracing their final destination difficult, especially once they are withdrawn into unhosted wallets or layered across multiple on-chain hops. Additionally, the speed of transactions makes it difficult, in many cases, to reactively stop the misuse of assets, as by the time a transaction is detected, the funds may have been used several times or moved to cold wallets. Therefore, systematic alerts should be prompt, VASPs should react rapidly, and the monitoring system should constantly adapt to criminal trends and tactics.

The use of privacy-enhancing tools such as mixers, cross-chain bridges, and decentralised exchanges adds further complications, making it harder to obscure its provenance. Decentralized platforms, in particular DeFi and DEXs, fall outside traditional regulatory reach and are used to move and launder funds without interacting with regulated entities, reducing oversight and accountability. As such, with no central operator, no KYC, and instant global access, these platforms might give illicit actors a frictionless way to launder and transfer value. Similarly, in terms of using self-custodied wallets and unregulated P2P platforms to bypass compliance controls.

[41] Not applicable in the chart refers to banks that do not have a business relationship with VASPs.

All of these features, and the rapid evolution of tactics used by criminals, are acknowledged to be increasingly sophisticated in their layering and movement of criminals' funds. Additionally, products such as NFTs, DeFi protocols, privacy coins, and the darknet markets, fraud shops, and online gambling sites that facilitate the movement and laundering of illicit funds often operate in jurisdictions with lax regulatory environments. Nation-state hackers (e.g., North Korea) also pose major investigative challenges due to advanced obfuscation as they move funds quickly and efficiently.

Other factors illustrated by VASPs addressed the limitations of real-time intelligence sharing and cross-border cooperation and data-sharing between regulators, law enforcement, and industry stakeholders, which could reduce the ability to act swiftly and disrupt ongoing criminal activity if shared in real time. This is in addition to the inconsistent implementation of regulations across jurisdictions, as previously mentioned, and the lack of uniformity among the enforcement regimes. In particular, freezing and recovery of assets, and securely managing seized virtual assets, are perceived by practitioners as among the most complicated challenges at the global level. Therefore, it requires active cross-border cooperation, enhanced analytics tools and investigative capabilities, and timely action.

At the same time, respondents from the banking sector illustrated different factors relevant to managing their customer risks associated with virtual assets, including the operational burden represented in the required ongoing staff training and updating internal tools and systems to meet the rapid evolution of the virtual assets sector and its products, as well as the sophistication and swiftness of the money laundering techniques. Furthermore, maintaining a robust risk posture, which often requires alignment across multiple internal stakeholders and governance forums, can be resource-intensive.

Respondents from the banking sector also highlighted the same challenge as VASPs: the lack of regulatory clarity at the global level and variation in the application of Travel Rule requirements.

Chart 24: *Challenges in disrupting criminal activities as indicated by VASPs*

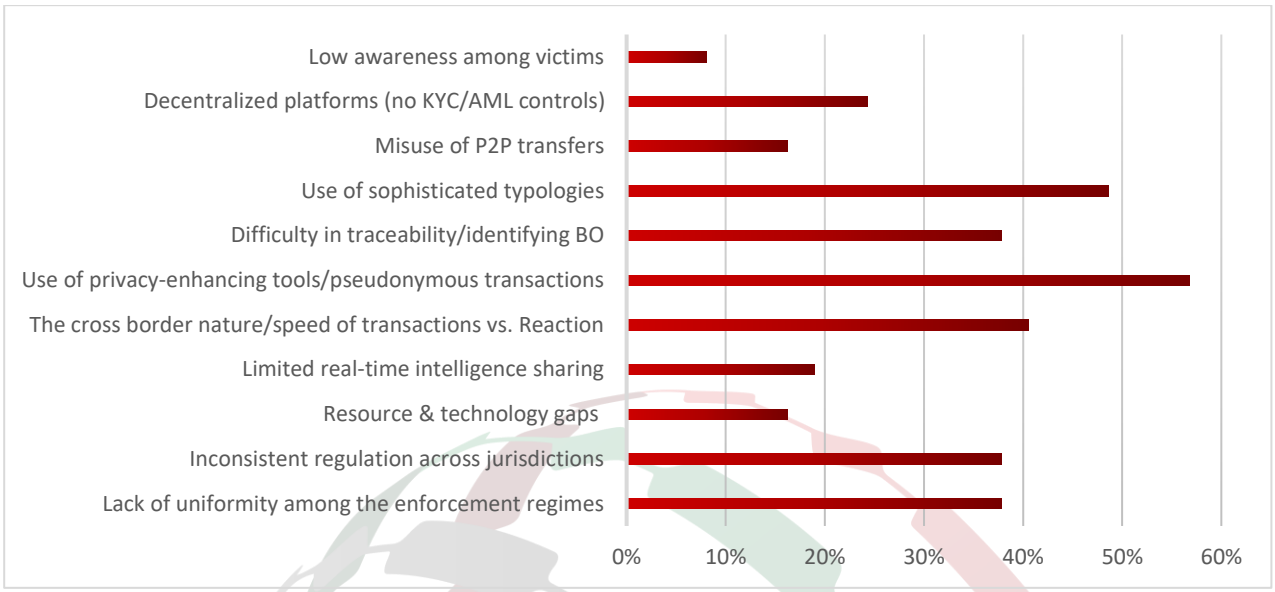
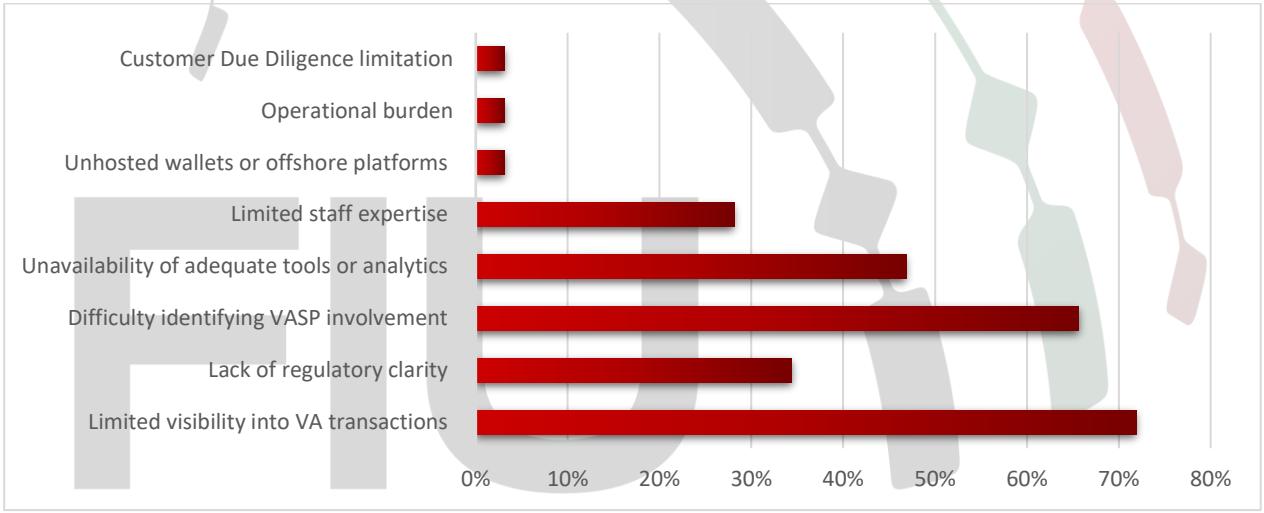


Chart 25: *Challenges banks face in managing VA-related risks*



10. PROPOSED SOLUTIONS AND RECOMMENDATIONS

Within the context of previously discussed challenges, the following were proposed as action points that need to be considered in the national approach by both the public and private sectors to disrupt the misuse of virtual assets in financial crime effectively:

In addressing the challenges faced in P2P transactions and unhosted wallets, both banks and VASPs highlighted the roles of monitoring systems, 'Know your Customer/Transaction' (KYC/KYT), enhanced due diligence, and the use of blockchain analytical tools. However, according to banks' responses on how they detect customer engagement with virtual assets, adopting blockchain analytics tools was identified as an area for improvement (Charts 26 and 27).

Chart 26: *VASPs' approaches to address decentralized, peer-to-peer cryptocurrency activity and unhosted wallets, according to the questionnaire*

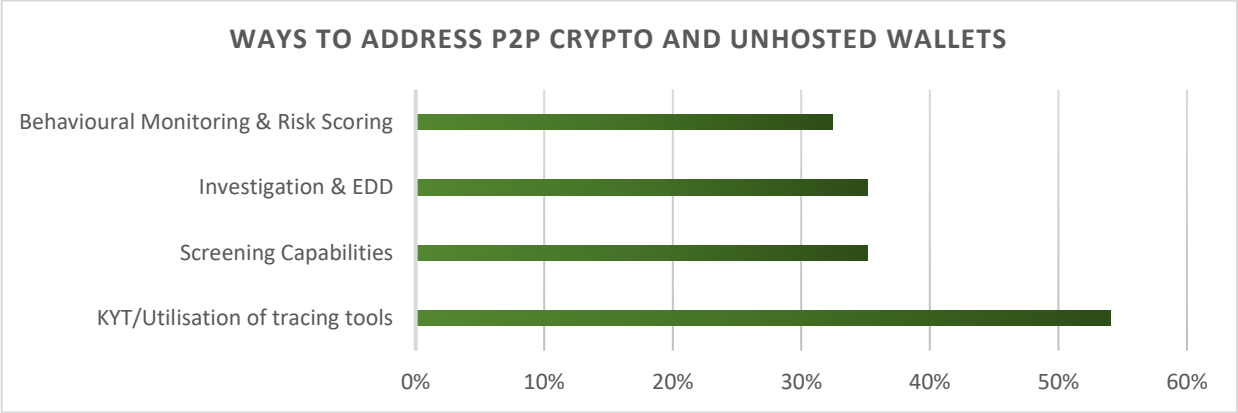
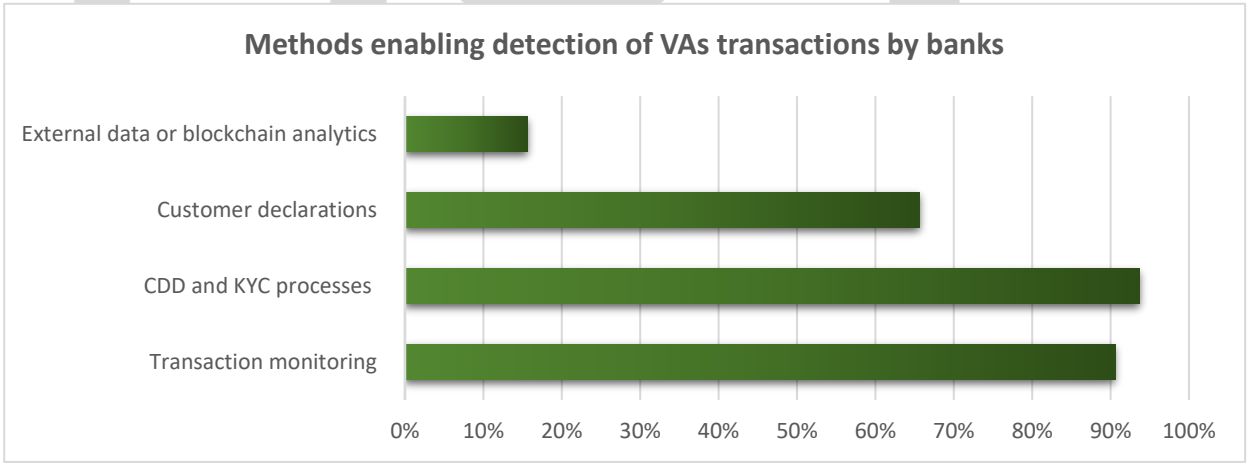


Chart 27: *Banks' approaches in detecting their customer engagement with virtual assets or VASPs, according to the questionnaire respondents*



With regard to enhancing the overall financial crime risk mitigation in the virtual asset industry, the following recommendations were common in both the questionnaire and the focus group discussions:

1. Fostering international and domestic Intelligence sharing through the Egmont Group, FATF networks, joint task forces of investigations, and prompt response to foreign requests for information between counterparties. This should also include broader, active public-private partnerships and collaboration to establish secure real-time data-sharing platforms, typologies and emerging threats among VASPs, the UAEFIU, law enforcement, and other stakeholders to facilitate early detection and disruption of coordinated criminal activities.
2. Unified and mandatory technical standards for the FATF Travel Rule, that mandate a minimum and common regulator-approved messaging standard for all licensed VASPs to ensure seamless, secure sharing of originator and beneficiary information domestically and across borders. Additionally, promoting interoperable technical solutions and clear guidance to enable effective compliance with the Travel Rule, particularly for cross-border transactions.
3. Consider standardizing a national rulebook for virtual assets, with a focus on prudent risk-taking for complex virtual asset products.
4. Explore approaches aiming to harmonize regulatory overlaps with an established baseline regulatory standards by continuing to align UAE regulations with FATF standards and requiring all VASPs to implement robust, standardized due diligence procedures. Furthermore, ensuring that all virtual asset service providers implement comprehensive compliance programs, including KYC, global sanctions screening, transaction monitoring, staff training, and governance oversight.
5. Strengthen supervisory oversight and targeted monitoring of P2P, OTC activities, decentralized applications, and DeFi interfaces, in addition to update on new typologies and applying key performance indicators among VASPs; prohibiting privacy coins, algorithmic stablecoins, and tokens that fail custody standards or facilitate high-risk activities without appropriate licensing, as part of a robust token listing and review process.
6. Supporting the establishment of clear risk appetite statements, with defined metrics and key performance indicators, to guide compliance and risk management activities.
7. Timely and high-quality reporting STRs/SARs for an effective investigation cycle, while updating the UAEFIU reasons for reporting relevant to virtual assets.
8. Investment in blockchain analytics and forensic tools, including exploring the possibility of establishing a UAE-led, regulator-managed blockchain analytics and intelligence centralized hub accessible to all licensed VASPs for real-time addresses, screening, typology sharing, and red flag alerts.

9. Capacity-building and training on blockchain analytics and forensic tools for the involved actors to enable more sophisticated detection, analysis, and prosecution of virtual asset-related crimes. Within the same context, it was recommended that regulators mandate the use of industry-leading blockchain analytics and transaction monitoring tools, enabling the detection of suspicious activities.
10. Within the same context of the investment in technology, adopting blockchain-integrated digital identity systems and eKYC platforms (e.g., UAE Pass) are recommended to support user verification across financial platforms, minimizing impersonation and fraud, and onboarding and ongoing monitoring. Additionally, RegTech Integration streamlines KYC/AML processes with digital identity verification, biometric solutions, and automated risk scoring to strengthen onboarding and ongoing monitoring.
11. Strengthen AI-Driven monitoring capabilities to monitor activities occurring outside traditional VASP channels, such as DEXs, cross-chain bridges, and smart contracts. This is in addition to leveraging machine learning models to identify behavioral anomalies, layering patterns, typologies, and predictive risk assessment.
12. Supporting the development of regulatory sandboxes to test new AML technologies and foster innovation, in addition to smart contract audit tools to assess smart contract vulnerabilities and risky DeFi protocols.
13. Promoting consumer awareness and guiding them to trade and invest through official and regulated VASPs to strengthen the integrity of and confidence in the VA sector, in addition to educating them about fraudulent schemes, Ponzi structures, phishing platforms, and social engineering tactics.

Chart 28: *VASPs' recommendations to enhance financial crime risk mitigation*

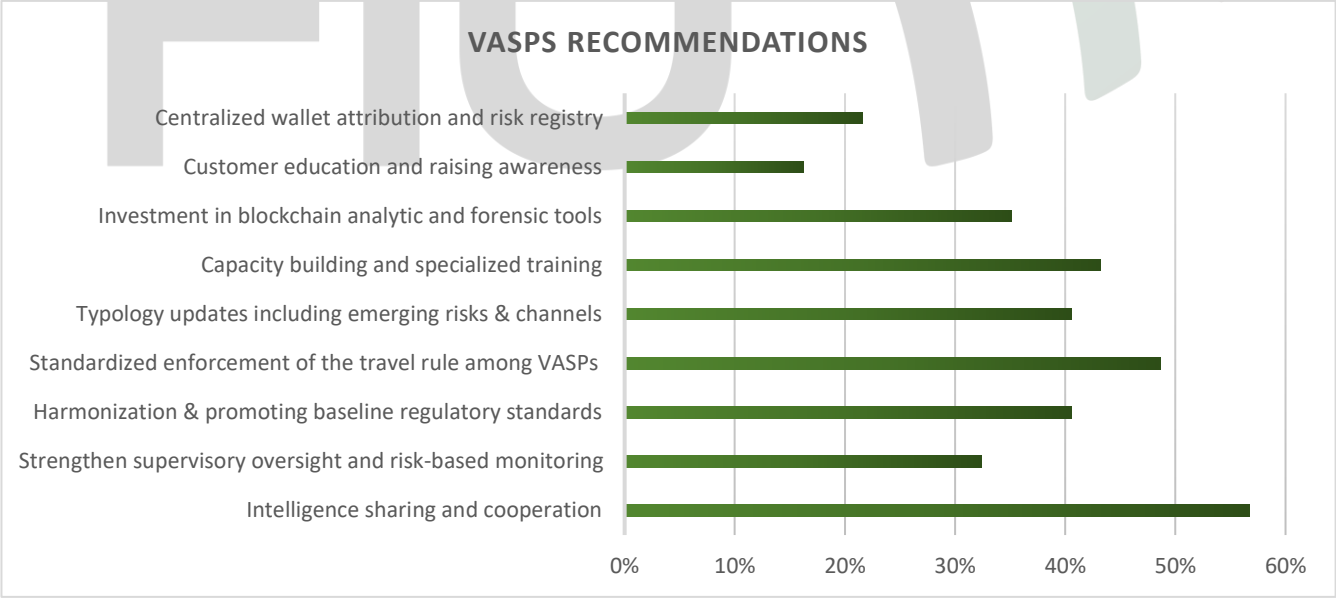


Chart 29: *Technology solutions enhancement as proposed by VASPs*

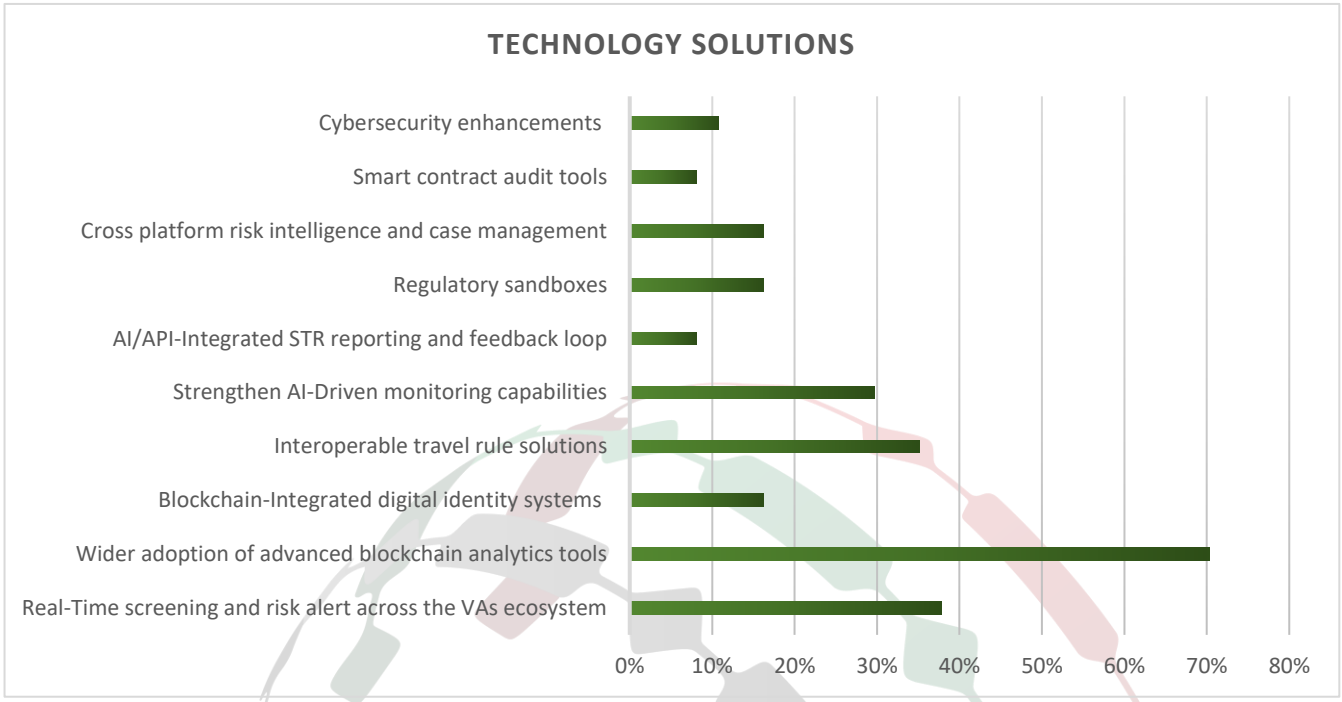
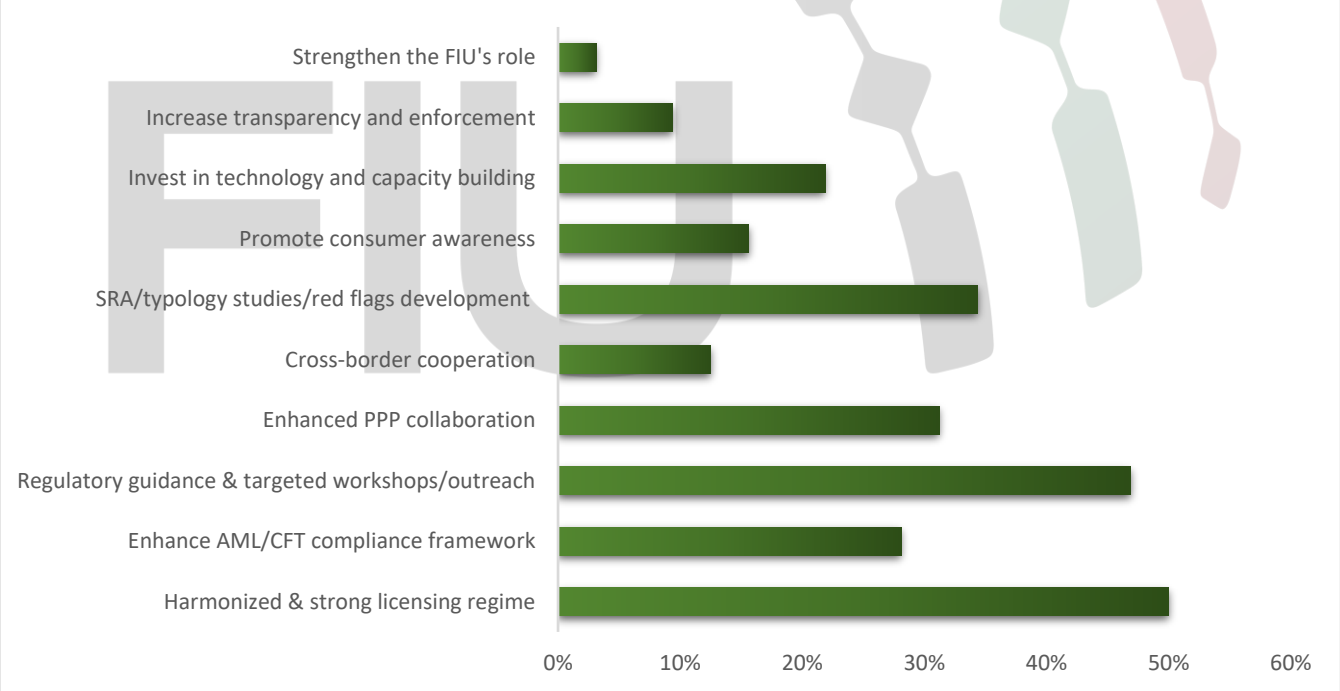


Chart 30: *Recommendations proposed by the banking sector*



11. DEVELOPED RISK INDICATORS

At the end of this analysis, the UAEFIU developed a list of relevant risk indicators specific to the nature of VAs and their associated financial crime schemes. These indicators are not exhaustive, but they are crucial for UAEFIU stakeholders, including VASPs, financial institutions, and LEAs, in detecting and investigating unusual transactions and behaviors relevant to the misuse of virtual assets. It should be noted that criminal activity cannot be conclusively determined based on a single indicator; rather, it requires a combination of indicators to ascertain such suspicion. Furthermore, risk indicators should always be considered in context. The following indicators should be read and understood together with the FATF virtual assets red flag indicators for money laundering and terrorist financing issued in September 2020. [42]

11.1. Risk indicators relevant to VASPs

Account activity and behavior

1. A customer attempts or completes a virtual asset purchase by depositing fiat using multiple credit or debit cards, especially cards not in the customer's name, suggesting stolen card or payment fraud.
2. The payment method used to fund the account is registered to an individual other than the customer, with no legitimate connection to the customer.
3. Small initial deposits are made, followed by significantly larger inbound and outbound transactions once the account or wallet is validated.
4. Funds are received from multiple unrelated individuals and pooled in the customer's account before outward transfer(s).
5. A suspicious account is linked to other wallets within the virtual asset service provider through the same device, all exhibiting similar suspicious behavior.
6. Multiple deposits into the customer wallet within the same day or over consecutive days, followed by a withdrawal to fiat.
7. Multiple transactions are conducted just below the reporting thresholds, whether on/off-ramping virtual assets or on-chain deposits/withdrawals.
8. No actual trading occurs on the account, and the balance remains low as funds are withdrawn shortly after receipt, either on-chain or via fiat withdrawals.

[42] FATF (2020), Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets. Available at: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html

9. Accounts are opened by numerous individuals (often of the same nationality) within a short period of time using shared addresses, mobile devices, IP addresses, and other common identity indicators.
10. An individual with low income suddenly receiving large virtual asset transfers that are inconsistent with the declared profile.
11. Device or IP address showing that the same device has been used to onboard or access other account(s).
12. Login attempts or live checks from unusual geolocations inconsistent with the user's declared residence.
13. Multiple login attempts occur from remote or unexpected jurisdictions without explanation of travel or relocation.
14. Users entering the VASP platform who have registered their internet domain names through proxies or using domain name registrars (DNS) that suppress or redact the owners of the domain names.
15. Users entering the VASP platform using an IP address associated with darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs.
16. Requests to change e-mail, phone number, or other credentials, immediately followed by suspicious login or transaction attempts.
17. Trading addresses, phone numbers, and other business information change frequently and for no apparent reason.
18. Presentation of documents that appear to be forged, falsified, or stolen.
19. A customer insinuates that another individual manages or directs activity on the account or wallet, suggesting potential third-party control.
20. Multiple third-party deposits to a single wallet without any established relationship.
21. Transaction paths show exposure to services or platforms previously linked to fraud or money laundering networks.
22. Making multiple high-value transactions in short succession, such as within 24 hours or in a staggered and regular pattern, with no further transactions recorded during a long period afterwards—ransomware to a newly created or previously inactive account.
23. A customer accepts funds suspected or identified as originating from stolen or fraudulent sources.

24. Use of language in VA message fields is indicative of the transactions conducted in support of illicit activity or in the purchase of illegal goods.
25. Lack of transparency or insufficient information on the origin and owners of the funds, such as those involving the use of shell companies or those funds placed in an ICO, where personal data of investors may not be available.

Transactional behavior and movement of assets

26. Funds pass through multiple wallet hops or intermediaries before reaching their final destination.
27. A customer uses multiple obfuscation techniques in combination, such as mixing pools, cross-chain bridging, peel-chain transfers, OTC settlements, and rapid off-ramping, within the same transactional cycle, creating a multi-layered pathway that significantly reduces transparency and traceability of asset origin or destination.
28. An address that receives multiple low-value virtual asset transfers, aggregates, and sends them to a single wallet destination.
29. A customer who purchases crypto assets, followed by immediate swapping to another asset to be ultimately transferred to a bank account.
30. High-volume fragmentation and consolidation patterns, such as funds moving through numerous intermediate wallets before arriving at the customer account.
31. Assets are transferred across multiple blockchain networks through cross-chain bridges without any stated investment strategy or reasonable purpose, indicating potential traceability evasion.
32. The customer regularly deposits and withdraws virtual assets on the same day, without engaging in trading or using any platform services.
33. The customer conducts rapid chain-hopping by moving the same value across several protocols or networks in a short period.
34. Funds are transferred from high-risk blockchains or privacy-focused networks before being immediately integrated into mainstream assets or exchanges.
35. A large incoming transfer is followed by a sequence of small outgoing transactions to multiple wallets, consistent with peel chain methodologies.
36. The customer primarily uses the VASP as an entry or exit point (fiat on-ramping or off-ramping) with no trading, investment, staking, or platform interaction.

37. Virtual assets are regularly off-ramped into sectors known for high cash turnover (e.g., real estate deposits, luxury goods brokers, vehicle exporters) without supporting documentation.
38. Assets routed through the account are traced to platforms known for pig-butchering and hybrid social engineering schemes targeting expatriates and migrant workers.

High-risk wallets and entities

39. A customer's source of wealth is disproportionately drawn from VAs originating from other VASPs that lack AML/CFT controls.
40. Multiple customers make high-value onward transfers to common accounts in high-risk jurisdictions with no clear apparent purpose.
41. A customer transacts with a cryptocurrency exchange or network that is sanctioned or known for enabling sanctions evasion and cybercrime.
42. The ownership structure of the customer's business appears opaque and involves shell companies in multiple jurisdictions.
43. An account receives funding from a politically exposed person (PEP) or from a party categorized as high-risk before engaging in virtual asset activity.
44. The customer receives assets from OTC providers linked to scam clusters, darknet markets, or high-risk exchanges/platforms.
45. Transferring virtual assets immediately to multiple VASPs, especially to those operating in another jurisdiction where there is no relation to where the customer lives or conducts business, or with lax AML/CFT controls.
46. Exposure to high-risk channels, including scam addresses, P2P merchants with weak KYC controls, or gambling platforms.
47. Direct or indirect exposure to sanctioned jurisdictions or entities.
48. Multiple small payments are collected and routed to a wallet associated with conflict-zone or extremist activity.
49. Transfers involve exchanges located in high-risk jurisdictions with known terrorist activity or jurisdictions associated with sanctions evasion.
50. Customer transactions are frequently conducted through peer-to-peer merchants that operate with limited identity verification.
51. Funds move to or from platforms associated with restricted, illicit, or unregulated services.

Market manipulation indicators

52. Multiple sub-accounts (or/and offshore accounts) showing synchronized and overlapping trading patterns around critical price points or off-market pricing.
53. A customer transacts at a potential loss with no logical business explanation, for example, when the value of VA is fluctuating, or when commission fees are abnormally high compared to industry standards.
54. Non-resident customers trade exclusively with each other under a trade agreement provided to the reporting entity, despite significant market price variations or use of the same or similar IP addresses.
55. An account simultaneously buys and sells the same financial instrument with the same counterparty, who is linked to the account holder, to create a false or misleading appearance of market activity and engage in wash trading.
56. Large withdrawals or sales coincide with rapid market fluctuations connected to the customer's trading activity.
57. A group of wallets appears to strategically accumulate a significant supply of a token in a coordinated manner.
58. Tokens circulate in repetitive patterns among customer-controlled wallets to simulate liquidity or trading activity.

Profile and documentation irregularities

59. Unclear source of funds or assets linked to a non-responsive customer who does not provide the required information or supporting documents to the reporting entity.
60. The customer becomes evasive, uncooperative, or defensive when asked to provide information required for due diligence.
61. The scale, frequency, or timing of the customer's transactions does not align with their stated financial profile, activity, or purpose.
62. High-value transfers are conducted without documentation that supports the customer's financial profile or declared purpose.
63. Transaction complexity exceeds what would be reasonably expected from the customer's knowledge, background, or experience.
64. The customer describes investment activities but cannot provide the source of funds, contracts, or receiving party details.

65. Selfie and/or ID mismatches during live checks, including gender, age, or facial discrepancies indicating impersonation or document misuse.
66. Submission of multiple identity documents in rapid succession, purportedly issued from different jurisdictions or showing different personal details, but the same or similar photograph.
67. Submission of forged or manipulated documents, including bank statements, proof of address, passports, or business licenses showing editing, pixilation, or invalid verification codes.
68. Sender/recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty.
69. The customer's personal details conflict with KYC information or records obtained during due diligence.
70. The customer states a source of funds or wealth, but is unable to provide documentation that sufficiently supports the stated origin.
71. The customer delays, avoids, or repeatedly submits incomplete information during KYC or enhanced due diligence reviews.
72. Open-source or media research associates the customer or UBO with allegations of financial crime, corruption, or illicit activity.
73. Absence of legitimate transaction purpose or economic rationale, combined with attempts to engage with high-risk clusters.

11.2. Risk indicators relevant to financial institutions

Customer profile and behavior

1. A customer account exceeds its declared income, with a high frequency of transfers involving crypto platforms inconsistent with their profile (e.g., low-income earners or students).
2. Declared occupations or business activities bear no relation to the transactional behavior observed (e.g., a tailor or student transacting in significant amounts of crypto-related payments).
3. Use of multiple personal accounts across different banks to fragment the flow of funds and conceal the overall transaction volume, or avoid reporting thresholds.
4. Customer reluctance to provide supporting documents or screenshots indicating crypto trading or investing, as required for the reporting entity's due diligence, including verifiable proof of income or the source of funds/wealth.

5. Individuals with limited financial literacy demonstrate activities of crypto platforms and P2P trading structures inconsistent with their profile.
6. Young individuals without a valid source of income handling high-volume crypto transactions.
7. A customer account shows a high volume of crypto-related transfers, combined with property and luxury good purchases, which are inconsistent with the declared income or profile.
8. A UAE-based corporate customer licensed for Information Technology activities or other similar business activities shows high turnover, primarily from crypto-related transactions, with unexplained sources or economic rationale, and a large volume of debits to its own accounts.
9. A positive result on the screening tool for name, photo, birthplace, or nationality indicates a potential financial crime.

Transactional activity

10. Customer is dealing in virtual currencies on behalf of third parties.
11. Multiple failed card deposits followed by crypto purchases.
12. Large cash deposits followed by immediate debit card usage on VA/cryptocurrency platforms and exchanges.
13. Immediate outflows to virtual asset exchanges or crypto payment gateways after receiving credits from unknown parties, with no economic purpose.
14. Account of a legal person that is not licensed for a virtual assets service provider or an individual showing an excessive movement of funds and transfers explicitly referenced to crypto-related keywords within fund transfers or remittance text fields.
15. Concentrated spikes in account activity followed by dormancy periods are a hallmark of structured laundering cycles tied to specific crypto or scam cash-outs.
16. High volume/value of transactions involving multiple unrelated third parties, indicative of the customer's personal account being used to route third-party proceeds or potentially involving crypto trading activities.
17. Customer accounts funded with cryptocurrency proceeds (from the sale of VAs) and subsequently used for real estate industry activities.
18. Customers using personal savings accounts for trading on the VASP platform or for third-party transactions (P2P) with high turnover.

19. Customer accounts are funded through peer-to-peer (P2P) transactions by multiple unrelated individuals, followed by outward transfers to various beneficiaries, cash withdrawals, or towards their own accounts maintained with another bank.
20. An account receives a high volume of funds from multiple parties.

Counterparty profile and behavior

21. Inflows originate from multiple unrelated individuals or businesses in relation to VAs with no logical connection to the account holder's personal or commercial activities.
22. Repeated interactions with known high-risk virtual asset exchanges, offshore wallets, or PSPs operating.
23. Outbound transactions directed to accounts of other individuals have been reported in prior STRs/SARs for similar activity.
24. Regular fund movements to or from 'Fintech' intermediaries that facilitate virtual asset or forex trades outside the customer's declared profile.
25. Accounts showing repeated inbound transactions from crypto platforms known to have compliance deficiencies, negative media, or sanctions-related concerns.
26. Counterparties linked to known fraudulent platforms or Ponzi schemes.
27. Accounts receiving micro-credits from numerous unrelated senders, later identified as victims of investment or social media scams.
28. A customer engaged in transfers with high-risk VASPs or PSPs without local licensing or registered under unrelated business activities to virtual asset service providers.
29. Engagement with unlicensed or high-risk VASP.
30. Transactions involving seemingly unrelated counterparties, either remitter or beneficiary, where the funds are potentially linked to virtual asset (VA) conversions, indicating engagement in VA exchange services as a business on behalf of other parties.
31. A customer is dealing with an exchange with no KYC/AML policies in place, and it is also located in a country associated with high levels of organized criminal activity.

Transaction transparency and verification

32. A customer fails to provide complete details of a transaction involving VAs.
33. Absence of supporting documentation for transactions to/from VA exchanges (related to the purchase or sale of VAs), raising concerns around the legitimacy of the transaction and

customers' dealings with unlicensed VA exchanges or high-risk VA exchanges (low/no KYC exchanges).

34. A crypto exchange that advertises for providing fiat currency and P2P trading, for which no verification is required. For example, 'Get your X currency for fiat swiftly without KYC'.
35. Involvement in an exchange that engages in high-volume trading involving fiat currencies associated with sanctioned jurisdictions.
36. Numerous parties are engaging in transactions involving the purchase or sale of virtual assets where the origin, intended purpose, or relationships among the participants are not clearly defined.

12. CONCLUSION

This report provided a thorough analysis and insights crucial to the UAEFIU stakeholders' understanding of the typologies associated with the misuse of virtual assets and VASPs, including criminals' evolved techniques and the transactional and behavioral patterns used in their schemes.

The report illustrated more than ten frequent risk areas in the analyzed STRs/SARs related to virtual assets or VASPs, consistent with the UAE NRA (2024). Furthermore, the analysis constructed criminal profiles for the examined subjects, enabling the UAEFIU's stakeholders to detect and investigate those illicit actors.

Among the identified typologies in this report, fraud remains the most reported concern, including identity theft, stolen bank cards and credentials, and fabricated or AI-generated identification documents, followed by illegal gambling, money laundering, and sanction evasion. Unlicensed VASPs, DeFi, and OTCs were frequently observed in the analyzed STRs, alongside mixer services and more complex techniques such as peel chains and cross-chain bridges. Swapping cryptocurrency for stablecoins was also common in many of the examined suspicious reports.

Data collected from the focus group discussions and the UAEFIU questionnaire circulated to VASPs and the banking sector addressed different challenges faced by reporting entities in responding to the misuse of virtual assets. These include regulatory mismatches at the global level and a fragmented landscape, as well as challenging compliance with the FATF travel rule and the need to obtain accurate, timely data on counterparties, and ensuring interoperability between different VASP systems and protocols. Staff capacity and skills are also another challenge. More importantly, there are limitations on real-time intelligence sharing, cross-border cooperation, and global data sharing among regulators, law enforcement, and industry stakeholders.

The same data sources proposed different solutions to tackle these challenges, highlighting the importance of reporting entities (both banks and VASPs) monitoring systems, enhanced due diligence,

and investment in blockchain analytics and forensic tools, enabling 'Know your Customer/Transaction' (KYC/KYT) and tracing of suspected funds. Fostering international and domestic Intelligence is also crucial, including public-private partnerships to address the identified risks and typologies, and the sharing of information in real time.

Good governance and future-proof, risk-based policy frameworks remain central to addressing the persistent vulnerabilities within the DeFi ecosystem. The annual FATF plenary meeting, under the headline "Back to Future," assessed opportunities in risk management to address rising challenges, highlighting the need for a global regulatory approach that utilizes new technologies, namely artificial intelligence and big data, to further mitigate potential risks.[43] Strengthening global regulatory frameworks, enhancing supervisory capabilities, and promoting public-private collaboration will be crucial to closing existing gaps. Only through such coordinated efforts can jurisdictions fully harness the benefits of virtual assets while protecting the financial system from illicit activity.

The presence of advanced technology tools and language-specific platforms used by criminals adds further challenges for investigative authorities, necessitating specialized blockchain expertise, investment in AI technology, and advanced forensic tools. Training all involved actors in the AML/CFT/CPF regime in blockchain forensics enhances the ability to detect complex laundering and terrorist financing techniques.

Furthermore, strengthening international supervisory and FIU cooperation is essential, including broader use of Egmont information-sharing channels and bilateral intelligence exchange. This should also include sharing best practices among FIUs, efforts to address virtual asset risks, and communication with stablecoin issuers to explore approaches that enable advanced monitoring and the freezing or blocking of assets.

Lastly, public awareness campaigns can educate customers of reporting entities and the public on how to avoid falling victim to criminals' schemes, in addition to continuing to provide targeted outreach and awareness sessions to AML/CFT/CPF practitioners.

Concluding Guidance on the Reporting of Suspicious Activities:

The UAEFIU has identified a range of risk indicators to facilitate the detection of suspicious activities involving the misuse of virtual assets in financial crime. Reporting entities are strongly encouraged to incorporate these indicators when detecting and reporting relevant cases.

Reporting entities should evaluate multiple risk indicators alongside other relevant factors, such as customer risk profiles and overall activities throughout the duration of the business relationship. In addition, entities should utilize available open-source information, screening tools, and advanced technologies to trace funds and identify high-risk activities.

[43] ECOFEL (2025) Outcome document Governance for Web 4.0 and Virtual Worlds.

Reporting entities must ensure that STRs and SARs are actionable to the UAEFIU and contain high-quality, accurate, and complete information. All supporting documents that substantiate the established suspicion should be included. **The following considerations are particularly relevant for VASPs:**

1. Select the correct report type: an STR should be submitted when a suspicious transaction has occurred, whereas an SAR is used to report suspicious activity that does not involve a specific transaction.
2. Include all information and documentation relevant to the customer's KYC/KYB record, such as customer/UBO identification documents and account details.
3. Provide the wallet address and the transaction hash (TXID) associated with the reported suspicion.
4. Include references or links to previous related transactions, where applicable.
5. Specify the nature and type of the asset involved (e.g., whether it is an on-ramp or off-ramp transaction, the asset type, and the transaction amount). Additionally, provide the exact timestamp and date of the transaction.
6. Ensure that the report contains a well-structured narrative that clearly and explicitly describes the concern or suspicion related to the subject of the report. The narrative should articulate the rationale for submitting the report to the UAEFIU.
7. Clearly indicate any high-risk clusters when reported, including the name and type of risk, as well as details of all relevant transactions within the suspect's activity cluster. (e.g., scam, sanctioned entity, etc). Avoid only mentioning "high-risk wallet" without further details.
8. Provide both the source and destination wallet addresses associated with the reported transactions, when known.
9. Describe the nature of the customer relationship, where applicable.
10. Include the results of screening processes and any relevant open-source intelligence.
11. Attach a screenshot of the traced transaction(s) to facilitate consistency and verification of findings during the UAEFIU tracing process.