Supervisory subcommittee

Virtual Asset Service Providers (VASPs) - Emerging ML/TF/PF Risks, Threats & Vulnerabilities in the UAE Relating to Stablecoins

Table of Contents

Virtual Asset Service Providers (VASPs) - Emerging ML/TF/PF Risks, Threats & Vulnerabilities in the UAE relating to Stablecoins

1. Context and Overview

The global financial landscape is undergoing a significant transformation, driven by the rapid innovation and adoption of virtual assets (VAs). While these technologies offer significant opportunities for economic growth and financial inclusion, they also present new and complex challenges related to money laundering, terrorist financing and proliferation financing globally. In particular, the unique characteristics of virtual assets, such as their pseudonymity, speed, and cross-border nature, have made them attractive to illicit actors for money laundering, terrorist financing, and proliferation financing.

The United Arab Emirates (UAE), through its comprehensive sectoral risk assessments and continuous supervisory reviews, has identified a notable increase in risks associated with activities involving the virtual assets ecosystem or Virtual Asset Service Providers (VASPs). The primary areas of concern revolve around stablecoin-led financial flows, particularly those involving Tether (USDT), the use of cross-chain obfuscation techniques such as bridges, mixers, and decentralized exchange (DEX) routers, and the growing exposure to unlicensed VASPs and peer-to-peer (P2P) “merchants.”

These emerging patterns and typologies create significant vulnerabilities within the UAE’s financial ecosystem, enabling potential large-scale money laundering, sanctions evasion, proliferation financing (PF), terrorist financing and high-volume fraud cash-outs. Consequently, there is a growing risk that such illicit activities may intersect with UAE-supervised financial institutions, such as banks, exchange houses, payment service providers, and licensed VASPs, particularly at on-ramp and off-ramp points.

To address these threats, the UAE has taken proactive steps to strengthen its regulatory and supervisory response to virtual asset risks. These measures include the issuing of the new Federal Decree-Law No. 10 of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing and Cabinet Decision No. 134/2025 On the Implementing Regulation of Federal Decree-Law No. 10/2025; establishing dedicated inter-agency coordination mechanisms, such as joint supervisory taskforces focused on illicit virtual asset activities; issuing national guidance that reinforces the prohibition on unlicensed VASP operations and that outlines the risks for financial institutions engaging with VASPs; and increasing supervisory scrutiny by the authorities responsible for overseeing VASPs, including strong enforcement actions carried out by UAE supervisory authorities.

This policy paper outlines emerging risks, threats, and vulnerabilities in the UAE’s VASP sector, with a particular focus on developments involving stablecoins. It summarises the current regulatory framework and highlights key risk typologies and common control deficiencies, including weak customer due diligence, insufficient monitoring of cross-chain activity, limited visibility of beneficial ownership, and inadequate controls when dealing with unlicensed offshore VASPs. In addition, the paper sets out enhanced control expectations for UAE VASPs and licensed financial institutions (‘UAE-licensed firms’) to improve detection, prevention, and reporting of high-risk virtual asset flows. Finally, the paper outlines supervisory priorities for UAE Supervisory Authorities, including targeted thematic reviews, advanced data-driven analytics, and coordinated enforcement actions. Together, these measures aim to safeguard financial system integrity while supporting secure and transparent innovation in the virtual asset sector.

2. UAE Regulatory Framework

The UAE has developed a comprehensive regulatory framework for virtual assets and VASPs, built on coordinated oversight by the concerned authorities. The framework is intended to support innovation while ensuring strong safeguards against money laundering, terrorist financing, and related risks, as well as protecting consumers and investors. The main regulatory bodies and their roles are outlined below:

2.1. Central Bank of the UAE (CBUAE)

The CBUAE licenses and supervises payment token service providers in accordance with the Payment Token Services Regulation.[1] Broadly, Payment Tokens are defined as virtual assets pegged to a fiat currency, classified as either Dirham Payment Tokens or Foreign Payment Tokens. They do not have legal tender status and function as a means of payment only by user agreement. The CBUAE is also responsible for the supervision of other Licensed Financial Institutions (LFIs) in the UAE, including banks, exchange houses and payment service providers.

In the context of virtual assets, the CBUAE has issued guidance for LFIs on the risks associated with virtual assets and VASPs. This guidance emphasizes the need for LFIs to conduct thorough risk assessments, implement robust customer due diligence (CDD) measures, and monitor transactions involving virtual assets for any signs of suspicious activity. The CBUAE has also co-issued Joint Guidance with other UAE supervisory authorities to combat the activities of unlicensed VASPs, demonstrating a unified national stance against illicit activities connected to virtual assets[2].

2.2. Securities and Commodities Authority (SCA)

The SCA is the federal authority responsible for regulating investment-type virtual assets and licensing VASPs operating in the UAE, except for payment tokens and VASPs located within the UAE's financial free zones. Overall, SCA's regulatory regime is designed to ensure market integrity, protect investors, and prevent financial crime. The authority has established a comprehensive framework for the licensing and supervision of VASPs, which includes requirements for AML/CFT/CPF compliance, capital adequacy and technology governance. A full description of SCA's regulated activities in relation to virtual assets and virtual asset service providers is provided in Cabinet Resolution No. (111) of 2022 on the Regulation of Virtual Asset Service Providers.

2.3. Dubai Virtual Assets Regulatory Authority (VARA)

VARA was established under Law No. (4) of 2022 on the Regulation of Virtual Assets in the Emirate of Dubai. Under this law and a cooperation agreement with the SCA, VARA serves as the competent Authority responsible for all virtual asset activities conducted in or from the Dubai mainland and commercial free zones (excluding the Dubai International Financial Centre (DIFC)). VARA's regulatory framework is activity-based and technology agnostic, focusing on licensing and supervising the specific activities undertaken by a VASP, rather than the type of virtual assets they offer as part of their services. VARA has been particularly active in its enforcement efforts, imposing financial penalties and issuing public warnings against unlicensed VASP activity or marketing within its jurisdiction. This has been a strong deterrent to illicit actors and reinforces the UAE's commitment to regulatory compliance.

2.4. Dubai Financial Services Authority (DFSA)

The DFSA is the independent regulator of financial services conducted in or from the DIFC. The DFSA introduced a comprehensive 'Crypto Token' regime in 2023, which was further enhanced in 2024. More recently, the DFSA also issued Consultation Paper 168 (CP-168) in October 2025, which proposes further amendments to its regime, including a significant overhaul of the crypto token-suitability assessment process. These proposals aim to support a regulatory framework that remains adaptable to innovation while addressing emerging risks.

2.5. Financial Services Regulatory Authority (FSRA)

The FSRA is the regulator of the Abu Dhabi Global Market (ADGM), a UAE financial free zone. In 2018, it introduced a regulatory framework for spot virtual asset activities, covering multilateral trading facilities (MTFs), brokers, custodians, and intermediaries, as well as provisions for staking and other emerging

[1] https://rulebook.centralbank.ae/en/rulebook/payment-token-services-regulation

[2] https://www.centralbank.ae/media/g5bgxlz5/joint-guidance-on-combating-the-use-of-unlicensed-virtual-asset-providers-in-the-uae-en.pdf

activities. Since then, ADGM has issued Financial Services Permissions (FSPs) to firms engaged in virtual asset activities. FSRA works to maintain the integrity of the ADGM ecosystem and collaborates with other UAE regulators to contribute to the national virtual asset regulatory framework.

3. Emerging ML/TF/PF risk typologies

The rapid development of virtual assets contributes to an evolving risk environment in which new methods of misuse continue to emerge. These methods may be used for financial crime, including money laundering, terrorist financing, or proliferation financing. There is a particular focus on stablecoin-related activity, as it is considered a significant area of global AML/CFT/CPF concern and is similarly relevant in the UAE. This section outlines the key emerging typologies currently identified as relevant to the UAE's financial system.

3.1. Stablecoin-Related Illicit Flows

Stablecoins are a type of virtual asset that is designed to maintain a stable value relative to a reference asset, typically a fiat currency such as the UAE Dirham (AED) and the US dollar (USD). The most common type is the fiat-backed stablecoin, which is backed by reserves of fiat currency held by the issuer. Other types of stablecoins include crypto-backed stablecoins, which are collateralised by other virtual assets.

Stablecoins offer several advantages to illicit actors that make them particularly attractive for money laundering, sanctions evasion, and other financial crimes. These advantages include:

- ***Stability***: Unlike other virtual assets, which can be highly volatile, stablecoins are designed to maintain a stable value. This makes them a more reliable store of value and a more practical medium of exchange for illicit transactions.

- ***Liquidity***: Stablecoins are highly liquid, meaning that they can be easily bought and sold on a wide range of exchanges and platforms. This makes it easy for illicit actors to convert their proceeds of crime into stablecoins and to move those stablecoins across borders.

- ***Low Transaction Fees***: Stablecoins, particularly those on the networks that are fast and have low transaction fees. This makes them an attractive option for illicit actors who need to move large volumes of funds quickly and cheaply.

- ***Cross-Border Settlement***: Stablecoins can be used to settle cross-border transactions quickly and efficiently, without the need for traditional banking intermediaries. This makes them an attractive option for illicit actors who are seeking to evade detection by law enforcement.

- ***Pseudonymity***: Although blockchain transactions are recorded on a public ledger, the identities of the parties involved are not always evident. This pseudonymity makes it challenging for law enforcement to trace illicit funds to specific individuals or entities, as wallet addresses are difficult to attribute.

Tether (USDT) is the most widely used stablecoin, with a market capitalization larger than most other stablecoins combined. USDT is a fiat-backed stablecoin that is designed to maintain its value in line with the US dollar. It is issued on multiple blockchain networks, including Ethereum, TRON, BNB Smart Chain and Solana, with the TRON network being particularly popular for illicit transactions due to its low transaction fees and fast settlement times.

Patterns observed: The pattern observed in relation to stablecoin activity is that illicit actors, including organised fraud networks and sanctions-exposed groups or nation-states, are increasingly using stablecoins for cross-border transfers because of their stability, liquidity, and low transaction costs. Globally, public reports and blockchain analytics show a significant increase in stablecoin transactions linked to money laundering, terrorist financing, and proliferation financing in 2024, alongside a growing market share for these assets. The UAE is primarily exposed to these risks at the entry and exit points of the virtual asset system, as well as through transactions conducted by licensed VASPs when the counterparty is an offshore or unlicensed entity.

Proliferation financing/ targeted financial sanctions angle: stablecoins are increasingly observed as a vehicle in sanctions-evasion and proliferation financing schemes. Their ability to move funds quickly across borders, combined with high liquidity and a degree of pseudonymity, makes them a tool of interest for sanctioned individuals and entities. Gaps in the implementation of the FATF Travel Rule, inconsistent counterparty due diligence, and limited transaction monitoring can increase this risk by obscuring the origin and destination of funds. This typology highlights the need for heightened vigilance, robust counterparty verification, and strengthened compliance measures to mitigate potential misuse.

Operational Red Flags:

Certain behavioural and operational patterns have been identified as potential indicators of heightened risk in stablecoin activity within the UAE. These red flags are particularly relevant for identifying transactions that may be linked to money laundering, terrorist financing, or proliferation financing. Key indicators include:

- **High-velocity stablecoin transactions:** Sudden bursts of transfers across wallets, accounts or jurisdictions may indicate attempts to quickly move funds.
- **Rapid off-ramping to AED:** Quick conversion of stablecoins into the UAE Dirham, which may indicate an effort to integrate illicit funds into the local financial system.
- **Counterparty VASPs not registered in the UAE:** Transactions involving virtual asset service providers that are absent from the public registers of UAE regulatory authorities, potentially signalling engagement with unlicensed or offshore entities.
- **Flows linked to sanctioned or high-risk clusters:** Transactions that can be traced to blockchain clusters previously associated with sanctioned individuals, entities, or other high-risk networks both directly or indirectly, suggesting possible sanctions evasion or exposure to proliferation financing.

Mitigation Strategies for Stablecoin-Illicit Flow Risks

To effectively mitigate the risks associated with stablecoins, UAE-licensed firms should implement the following strategies:

- **Chain-Specific Analytics:** Firms should implement blockchain analytics tools that are capable of analyzing stablecoin transactions on multiple blockchain networks, including TRON, Ethereum, and BNB Smart Chain. These tools should be able to identify high-risk wallet clusters, including those associated with sanctioned entities, fraud, and other illicit activities.

- **Issuer Blacklists and Freezes:** Firms should monitor for stablecoins that have been blacklisted or frozen by their issuers. Many stablecoin issuers have the ability to freeze tokens that are associated with illicit activity, and firms should be aware of these freezes and should take appropriate action.

- **Velocity and Hop Thresholds:** Firms should establish velocity and chain-hop thresholds for stablecoin transactions. Transactions that exceed these thresholds should be subject to enhanced scrutiny and may be held or declined pending further investigation.

- **Scenario Rules:** Given the high prevalence of illicit activity on the different networks e.g. including the TRON network, firms should develop specific scenario rules for stablecoins including USDT transactions on the TRON network. These rules should be designed to identify high-risk patterns, such as high-velocity bursts, rapid off-ramping, and exposure to sanctioned clusters.

- **Tuned Sanctions/TF Models:** Firms should ensure that their sanctions and terrorist financing screening models are specifically tuned to the unique characteristics of stablecoins. This includes ensuring that the models are capable of screening against the full range of sanctions lists and that they are updated regularly to reflect new designations.

3.2. Cross-Chain Obfuscation (Bridges, Mixers, DEX Routers)

Cross-chain obfuscation techniques represent one of the most sophisticated methods used by illicit actors to launder virtual assets. This section provides a technical overview of these techniques and outlines approaches that UAE-licensed firms can use to identify and monitor such activity.

Understanding Bridges and Routers

Bridges and routers are technologies that allow virtual assets to be moved between different blockchain networks. For example, a bridge might allow a user to move Bitcoin from the Bitcoin blockchain to the Ethereum blockchain, where it can be used in decentralized finance (DeFi) applications. While these technologies have legitimate uses, they are also frequently used by illicit actors to obscure the origin of funds.

When assets are transferred from one blockchain to another using a bridge, the assets on the source blockchain are locked in a smart contract or in some cases burned (permanently removed from circulation). An equivalent amount is then minted or released on the destination blockchain. This preserves the integrity of each blockchains ledger. However, this process can make it difficult to trace the flow of funds, as the asset on the destination blockchain may have a different address and may be subject to different transaction patterns.

Understanding Mixers and Tumblers

Mixers, also known as tumblers, are services that are designed to obscure the origin of virtual assets by mixing them with other assets. When a user sends virtual assets to a mixer, the mixer will combine those assets with assets from other users and will then send the combined assets to a series of different addresses. This process makes it extremely difficult to trace the flow of funds, as the assets that are received by the user may have no apparent connection to the assets that were originally sent.

Mixers are frequently used by illicit actors to launder the proceeds of crime, including the proceeds of hacks, fraud, and ransomware attacks. Some mixers, such as Tornado Cash, have been previously sanctioned by the US Office of Foreign Assets Control (OFAC) due to their use in facilitating illicit financial flows; however, those sanctions have since been lifted.

Understanding DEX Routers

Decentralized exchange (DEX) routers are smart contracts that are designed to find the best price for a trade across multiple decentralized exchanges. While DEX routers have legitimate uses, they can also be used by illicit actors to obscure the origin of funds. By routing a trade through multiple DEXs, an illicit actor can make it more difficult for law enforcement to trace the flow of funds.

Typical cross-chain obfuscation sequence

A typical cross-chain obfuscation sequence may look like this:

1. **Initial Illicit Activity -** The illicit actor obtains virtual assets through a hack, fraud, or other illicit activity.
2. **Bridge Hop -** The illicit actor uses a bridge to move the assets from the original blockchain to a different blockchain.
3. **Mixer -** The illicit actor sends the assets through a mixer to obscure the transaction trail.
4. **DEX Router -** The illicit actor uses a DEX router to swap the assets for a different type of virtual asset, often a stablecoin.
5. **Consolidation -** The illicit actor consolidates the stablecoins into a smaller number of wallets.
6. **Off-Ramp -** The illicit actor attempts to cash out the stablecoins through an OTC desk, a P2P platform, or a licensed VASP.

The above sequence is further complicated by mismatches in cross-border messaging and data standards which can significantly impede the effectiveness of sanctions and terrorist financing screening processes.

Proliferation Financing Angle: State-sponsored actors, such as those linked to the Democratic People's Republic of Korea (DPRK), and other sanctioned networks have been observed to systematically use a sequence of bridge, mixer, and stablecoin consolidation before attempting to off-ramp the funds.[3] This highlights the critical need for enhanced monitoring and detection capabilities for these types of transactions.

Red Flags:

Based on the above, UAE licensed firms should consider the following red flags in identifying these types of illicit activities.

- Immediate use of bridges to hop chains after receiving inbound funds.
- Multiple chain hops before an off-ramp attempt.
- Transaction history linked to known hack-associated blockchain clusters.
- Repeated instances of missing Travel Rule data from the same foreign VASP.

Detection methods for cross-chain obfuscation

To effectively detect cross-chain obfuscation, UAE-licensed firms should consider implementing the following detection methods:

- **Embed bridge/mixer routing scores – UAE licensed f**irms should use blockchain analytics tools that are capable of identifying transactions that have passed through bridges or mixers. These tools

[3] https://www.mofa.go.jp/files/100922718.pdf

should assign a routing score to each transaction, which reflects the likelihood that the transaction has been used for obfuscation purposes. Transactions with high routing scores should be subject to enhanced scrutiny.

- **Auto-hold transaction flows - UAE licensed f**irms should implement automated controls that will hold transactions that match known obfuscation patterns. This includes transactions that have passed through bridges or mixers within a short period of time, transactions that have hopped across multiple blockchains, and transactions that are linked to known hack-associated clusters.

- **Converge travel rule validation with targeted finacncial sanctions screening:** UAE licensed firms should ensure that their Travel Rule validation processes are converged with their sanctions and terrorist financing screening processes. The intended end-state of this should be that transactions are not be released until both the Travel Rule data has been validated and the transaction has been screened against sanctions and terrorist financing lists.

- **Monitor for known hack-linked clusters - UAE licensed f**irms should monitor for transactions that are linked to known hack-associated clusters. Blockchain analytics firms maintain databases of wallet addresses that have been associated with hacks and other illicit activities, and institutions should use these databases to screen their transactions.

- **Track chain hopping– UAE licensed f**irms should track the number of chain hops that a transaction has undergone. A high number of chain hops can be an indicator of obfuscation activity, and transactions with a high number of hops should be subject to enhanced scrutiny.

3.3. Peer-to-Peer (P2P) and over-the-counter (OTC) "Merchants" and Unlicensed VASP Exposure

Unlicensed VASPs and P2P/OTC "merchants," often operating through social media platforms like Telegram, actively solicit users in the UAE. These entities typically lack any form of customer due diligence and fail to collect originator and beneficiary information, creating a high-risk channel for illicit financial flows. Marketing breaches are also common, with these entities often making misleading claims to attract customers.

Observed Patterns:

UAE Supervisory Authorities have observed the following patterns:

- P2P/OTC merchants and unlicensed VASPs frequently promote their services online, sometimes using misleading claims or aggressive marketing to attract customers.
- Transactions are often cash-funded, with purchased stablecoins subsequently deposited directly into exchange accounts, bypassing regulated intermediaries.
- These entities commonly fail to maintain records or provide verifiable transaction receipts from licensed institutions.

Operational red Flags:

- A customer providing a social media handle instead of the name of a licensed counterparty for a transaction.
- Cash-funded purchases of stablecoins followed by direct deposits into exchange accounts.
- Receipts or transaction details from brands or entities that are not on the public registers of the CBUAE, SCA, VARA, DFSA, or FSRA.

- Transactions through clusters identified as 'No KYC Exchanges'.
- Account use shows regular deposit activity during business working hours, indicative of a service being provided.
- Online reviews show users discussing virtual asset exchange activity
- Regular cash deposits to traditional financial services transferred in equal or similar amounts to virtual asset exchanges

3.4. Travel Rule implementation gaps (cross-border)

The FATF's Travel Rule, which is set out in FATF Recommendation 16, requires VASPs to obtain, hold, transmit and, where relevant to their role, verify the accuracy of the required originator and beneficiary information for virtual asset transfers, including but not limited to the name of the originator and beneficiary, the originator's account number (or virtual asset address), the originator's address, date of birth (for natural persons) and the connected business identifier code (BIC) or legal entity identifier (LEI) for legal persons.

Verification obligations vary depending on whether the VASP is acting as the ordering or beneficiary institution.

Broadly, the Travel Rule is designed to ensure that VASPs have the same level of transparency as traditional financial institutions when it comes to cross-border wire transfers. By requiring VASPs to collect and transmit originator and beneficiary information, the Travel Rule makes it more difficult for illicit actors to use virtual assets to launder money or to finance terrorism.

However, the implementation of the Travel Rule has been a major challenge for the VASP industry, for several reasons:

- **Lack of global standardisation -** There is no single global standard for the implementation of the Travel Rule. Different jurisdictions have implemented the rule in different ways, and this has created challenges for VASPs that operate across multiple jurisdictions.

- **Technical complexity -** The implementation of the Travel Rule requires VASPs to integrate new technology into their existing systems. This can be technically complex and expensive, particularly for smaller VASPs.

- **Interoperability issues -** For the Travel Rule to be effective, VASPs need to be able to exchange originator and beneficiary information with each other. However, there are a number of different Travel Rule solutions on the market, and these solutions are not always interoperable with each other.

- **Jurisdictional gaps -** Not all jurisdictions have implemented the Travel Rule, and this creates gaps in the global Travel Rule network. When a UAE-licensed VASP transacts with a VASP in a jurisdiction that has not implemented the Travel Rule, the UAE-licensed VASP may not receive the required originator and beneficiary information.

- **Accuracy and timeliness:** Challenges relating to the accuracy and timeliness of originator and beneficiary information have also slowed down the effectiveness of travel rule solutions implemented.

Best practices for Travel Rule compliance

To ensure effective Travel Rule compliance, UAE-licensed firms should consider introducing the following controls:

- **Use interoperable providers:** UAE licensed firms should seek to use Travel Rule solution providers that support broad interoperability with other VASP solutions, enabling reliable exchange of originator and beneficiary information across different networks and counterparties.

- **Ensure reject/return logic:** UAE licensed firms should implement strict controls to ensure that transactions lacking required originator or beneficiary information are not processed. For outbound transfers, firms should reject the transaction until the required information is provided. For inbound transfers received without the necessary data, firms should apply appropriate risk-based measures (such as contacting the counterparty VASP, delaying crediting, or returning the equivalent value to the sender) before making the virtual assets available to the customer.

- **Monitor counterparties' compliance rates:** UAE licensed firms should monitor the Travel Rule compliance rates of their counterparties. Counterparties that repeatedly fail to provide the required originator and beneficiary information should be subject to enhanced scrutiny, and the firm should consider terminating the relationship if the counterparty's compliance does not improve.

- **Run periodic effectiveness testing:** UAE licensed firms should conduct periodic effectiveness testing of their Travel Rule compliance programs. This should include testing the completeness of transaction messages, the logic for rejecting or holding transactions, and the alignment of Travel Rule screening with other AML/CFT/CPF compliance processes.

- **Maintain a counterparty whitelist:** UAE licensed firms should maintain a whitelist of approved counterparties that have demonstrated a strong commitment to Travel Rule compliance. Transactions with counterparties that are not on the whitelist should be subject to enhanced scrutiny.

3.5. Tokenisation & New Issuance Risks (Real world assets, fiat-backed coins, platform tokens, staking)

The tokenization of real-world assets (RWAs) and the issuance of new types of virtual assets is one of the newest developments in the virtual asset space. However, these developments also introduce new risks that must be carefully managed.

What is Tokenization?

Broadly, tokenization is the process of representing real-world assets, such as real estate, commodities, or securities, as tokens on a blockchain. Generally, unless there are specific restrictions in place, these tokens can then be bought, sold, and traded. Tokenization has the potential to unlock significant value by making it easier to fractionalize ownership of assets, to improve liquidity, and to reduce transaction costs.

Types of Tokenized Assets

Generally, there are several different types of tokenized assets, including, but not limited to:

- **Real estate tokens -** These tokens represent ownership of real estate assets, such as residential or commercial properties. Real estate tokens can allow investors to gain exposure to real estate markets without the need to purchase an entire property.

- **Commodity tokens:** These tokens represent ownership of commodities, such as gold, silver, or oil. Commodity tokens can allow investors to gain exposure to commodity markets without the need to take physical delivery of the commodity.

- **Security tokens:** These tokens represent ownership of securities, such as stocks, bonds, or investment funds. In the UAE, security tokens are subject to securities regulations and must be issued in compliance with the applicable securities regulations.

- **Fiat-Backed stablecoins:** As discussed above, fiat-backed stablecoins are tokens that are backed by reserves of fiat currency. These tokens are designed to maintain a stable value relative to the fiat currency.

Observed Patterns:

The tokenization of real-world assets, issuance of fiat-backed stablecoins, and growth of platform tokens and yield-bearing create material ML/TF/ PF risks when controls are insufficient.

Off-chain dependencies, such as opaque or infrequent verification of reserves, can allow illicit actors to misrepresent the backing of tokens. This can enable the movement or layering of illicit funds under the guise of legitimate assets, increasing the risk of money laundering and TF/PF exposure.

Issuer concentration, where a single entity controls a large portion of a token's supply, further amplifies these risks. Large-volume, rapid transfers can obscure the origin and destination of funds, providing opportunities for money laundering and potential circumvention of sanctions or proliferation financing controls.

Operational Red Flags:

- Rapid minting and burning cycles of a token, potentially indicating laundering or market manipulation.
- Lack of transparent reserve attestations for fiat-backed stablecoins, enabling misrepresentation of backing.
- Use of yield-bearing or staking products without proper compliance checks, particularly where offered across borders, which may facilitate ML, TF, or PF.

The DFSA and the FSRA have both issued consultation papers on the regulation of tokenized assets, and these consultations are expected to lead to new rules and guidance in the near future.

The DFSA's CP-168[4] proposes significant changes to the token-suitability assessment process, which is designed to ensure that only appropriate tokens are offered to investors. The FSRA has also issued proposals establishing a regulatory framework for staking, designed to ensure these activities are conducted transparently, under robust governance, and with strong investor safeguards[5].

UAE-licensed firms should closely monitor these regulatory developments and should be prepared to adapt their controls and processes to comply with the new requirements.

4. Vulnerabilities in/around UAE VASPs

The evolving threat landscape exposes a number of vulnerabilities within and around the UAE's VASP ecosystem. These vulnerabilities can be categorized into four key areas: counterparty and perimeter risks, institutional controls, product and technology weaknesses, and market conduct issues. A clear understanding of these vulnerabilities is essential for developing effective risk mitigation strategies.

4.1. Counterparty & Perimeter

- **Unlicensed VASP Exposure:** A significant vulnerability arises from the continued operation of foreign platforms and local platforms marketing their services to UAE residents without the appropriate licenses. While enforcement actions are actively being taken, user behaviour and the ease of accessing these platforms online mean that this remains a persistent channel for illicit activity.
- **Cross-border Travel Rule Gaps:** Even when UAE-licensed firms have taken substantial steps to meet UAE Travel Rule requirements and have established robust processes consistent with the UAE regulatory framework, there are still challenges when dealing with counterparties in jurisdictions that have not yet implemented the FATF's Travel Rule. This lack of reciprocal compliance means that UAE licensed firms can lose visibility into the origin and destination of funds, creating a significant vulnerability that can be exploited by illicit actors.

4.2. Institutional Controls

- **Inconsistent CDD/Beneficial Ownership transparency:** The complex corporate structures of some customers, including Decentralized Autonomous Organizations (DAOs), can make it difficult to identify the ultimate beneficial owners. Omnibus wallets and the commingling of funds can further complicate the process of determining the origin and ownership history of assets, creating a vulnerability that can be exploited for money laundering and other financial crimes.
- **Analytics maturity gaps:** The effectiveness of a VASP's AML/CFT/CPF controls is heavily dependent on the maturity of its transaction monitoring and blockchain analytics capabilities. Notwithstanding the deployment of leading blockchain analytics solutions, gaps in data coverage and in the identification and tracking of transactions and wallets, particularly in relation to unhosted wallets and peer-to-peer activities remain prevalent. Where such limitations persist, including an inability to detect bridge and mixer activity, analyse chain-hopping heuristics, or identify stablecoin clustering and exposure risks, a UAE-licensed firm may remain exposed to heightened money laundering, terrorist financing, and proliferation financing risks.
- **Inefficiencies in risk management integration:** The operational processes for complying with the Travel Rule are not always fully converged with sanctions and terrorist financing screening processes. This can lead to high rates of false negatives or positives, potential manual

[4] https://dfsaen.thomsonreuters.com/rulebook/consultation-paper-no168-enhancements-regulation-crypto-tokens
[5] https://www.adgm.com/media/announcements/proposed-regulatory-framework-for-the-staking-of-virtual-assets

workarounds, and a fragmented approach to risk management, creating inefficiencies and potential compliance gaps.

4.3. Product/Technology

- **Bridge/Router risk:** The risks associated with bridges and routers are not always fully integrated into VASPs' transaction monitoring frameworks. This gap can create vulnerabilities that facilitate **money laundering, terrorist financing, or proliferation financing**, particularly when combined with the inconsistent adoption of security measures such as withdrawal allow-listing and robust hot-wallet key management. Malicious actors may exploit these weaknesses to move illicit funds across chains with limited detection.
- **Issuer/Token due diligence:** The level of due diligence on token issuers and the underlying technology of new tokens is uneven across the market. Insufficient verification of reserves, irregular attestation of fiat-backed stablecoins, and unclear redemption mechanics can expose VASPs to **fraud, market manipulation, and financial crimes**, including **the potential use of tokens for laundering illicit funds or financing terrorist or proliferation activities.**
- **Omnibus and pooled wallets:** Omnibus or pooled wallets commingle funds from multiple users, making it difficult to attribute individual transactions. While omnibus and pooled wallets are not automatically subject to increased AML/CFT/CPF risks, this opacity can prevent effective **beneficial ownership identification in circumstances where a VASP is not fully compliant with AML/CFT requirements enabling** misuse of funds for **money laundering or terrorist financing purposes.**
- **Cross-Border payment features:** Automated or instant cross-border transfers with limited oversight increase the potential for **sanctions evasion, terrorist financing, and proliferation financing,** as illicit actors can rapidly move funds across multiple jurisdictions without detection.

4.4. Market Conduct / Consumer

The promotion of offshore yield products into the UAE, including claims of rapid or "instant" cash-out through OTC providers, can create channels for ML/TF/PF. These products are often distributed via P2P or OTC "merchants" and other unlicensed VASPs, which typically operate outside the regulated framework. Such entities are likely to lack adequate customer due diligence, transaction monitoring, and reporting, increasing the risk that illicit funds could enter or move through the financial system undetected through them.

5. Risk Assessment Matrix (illustrative)

To provide a clearer understanding of the relative significance of the various risks discussed above, the following illustrative risk assessment matrix has been developed. This matrix considers the likelihood of each risk occurring and the potential impact on the UAE's financial system. It is important to note that this is an illustrative assessment and the actual risk levels may vary depending on a variety of factors.

Risk Category	Risk Description	Likelihood	Impact	Overall Risk
Stablecoin-led Illicit fllows	Use of stablecoins (e.g., USDT) for money laundering, sanctions evasion, and other illicit activities.	High	High	**Significantly High**

Risk Category	Risk Description	Likelihood	Impact	Overall Risk
Cross-Chain obfuscation	Use of bridges, mixers, and DEX routers to obscure the origin of illicit funds.	High	High	**Significantly High**
Unlicensed VASP exposure	UAE residents using unlicensed VASPs, which may have weak or non-existent AML/CFT/CPF controls.	High	High	**Significantly High**
Travel rule implementation gaps	Inconsistent implementation of the Travel rule across jurisdictions, leading to loss of visibility over cross-border transactions	High	Medium	**High**
Institutional control weaknesses	Gaps in CDD, beneficial ownership transparency, and transaction monitoring capabilities.	Medium	High	**High**
New issuance & tokenization risks	Risks associated with new tokens, including those backed by real-world assets and staking models.	Medium	Medium	**Medium**
Product & technology vulnerabilities	Security risks related to bridges, routers, and hot wallets, Omnibus or pooled wallets as well as inadequate due diligence on new tokens.	Medium	Medium	**Medium**
Market conduct & consumer risks	Misleading marketing of high-risk products and services to UAE residents.	Medium	Medium	**Medium**

6. Control Expectations for UAE-Licensed Firms (What “Good” looks like)

To effectively mitigate the risks outlined in this paper, UAE-licensed VASPs are expected to implement a comprehensive and robust set of controls. These controls should be proportionate to the UAE licensed firm’s risk appetite and the nature, scale, and complexity of its operations. The following outlines the key control expectations for UAE-licensed firms, representing what “good” looks like in practice. This is not an exhaustive list of controls but a high-level overview of what is generally expected. It does not replace any existing regulations, laws or guidance. It is intended to clarify and/or supplement them.

6.1. Governance and Oversight

Strong governance and oversight are essential for ensuring that a VASP's AML/CFT/CPF program is effective. The board of directors and senior management must take ultimate responsibility for the UAE licensed firm's AML/CFT compliance and must ensure that adequate resources are allocated to the compliance function.

UAE licensed firms must ensure that its board receives regular reports on the firm's AML/CFT/CPF performance, including information on the number and nature of suspicious transaction reports filed, the results of transaction monitoring, and any significant compliance issues or breaches. The board/senior

management must also approve the firm's AML/CFT/CPF
policies and procedures and should review and approve any significant changes to these policies and procedures.

6.2. The Three lines of defense model

VASPs are required to adopt a three lines of defense model for their AML/CFT/CPF compliance. The nature, complexity, and scale of VASP activities should be considered when applying the mode. The first line of defense is the business units, which are responsible for identifying and managing risks in their day-to-day activities. The second line of defense is the compliance function, which is responsible for developing policies and procedures, providing guidance and training, and monitoring compliance. The third line of defense is the internal audit function, which provides independent assurance on the effectiveness of the firm's AML/CFT/CPF controls.

6.3. Business Risk Assessment

A business risk assessment is a core component of an effective AML/CFT framework. VASPs must maintain a comprehensive and documented assessment of the ML/TF/PF risks arising from their business model, products and services, customer base, delivery channels, and geographic exposure. The business risk assessment must be proportionate to the nature, scale, and complexity of the VASP's activities and must inform the design, implementation, and calibration of AML/CFT controls. VASPs must assess risks associated with specific activities, including custody, exchange, brokerage, transfer, staking, yield-bearing products, DeFi integrations, and interactions with unhosted wallets, as well as the use of anonymity-enhancing features, cross-chain bridges, and automated transaction mechanisms. Where higher-risk activities are identified, VASPs must implement appropriate mitigating measures, which may include enhanced controls, restrictions, or limitations on products or services.

6.4. Customer Due Diligence

Customer due diligence is the foundation of any effective AML/CFT program. Therefore, VASPs must implement robust CDD processes that are designed to identify and verify the identity of their customers, to understand the nature and purpose of the customer relationship, and to assess the ML/TF/PF risks associated with the customer.

For corporate customers, this is required to include identifying and verifying the identity of the beneficial owners and understanding the corporate structure and control arrangements. For complex corporate structures, including DAOs, VASPs should conduct enhanced due diligence to understand the governance arrangements and to identify any potential red flags.

6.5. Transaction monitoring and blockchain analytics investment

The maturity of a VASP's transaction monitoring capabilities is a key indicator of the effectiveness of its AML/CFT/CPF program. VASPs are expected to implement robust transaction monitoring systems capable of detecting a wide range of suspicious activity patterns, including those related to stablecoins, cross-chain obfuscation, and transactions involving sanctioned entities.

These systems should be regularly updated to reflect emerging typologies and subject to periodic effectiveness testing. VASPs should also maintain processes for investigating alerts generated by the monitoring system and for escalating suspicious activity to the appropriate level of management.

UAE licensed firms should apply chain-specific analytics for virtual assets, including stablecoin transactions. This may include the use of issuer blacklists, freezes, and stablecoin cluster lists, as well as establishing chain-hop thresholds. Scenario rules should be developed for high-risk stablecoins, such as USDT on the TRON network, and sanctions and terrorist financing screening models should be tailored to the characteristics of these assets.

To enhance detection and prevention of ML/TF/PF,
VASPs should consider investing in advanced blockchain analytics and other technologies. Tools that analyze on-chain transaction data, identify high-risk wallet clusters, and screen for exposure to sanctioned entities can strengthen monitoring. Artificial intelligence and machine learning technologies may further improve the identification of complex suspicious activity patterns that traditional rule-based systems might not identify.

6.6. Cross-Chain Obfuscation

To combat the use of cross-chain obfuscation techniques, UAE licensed firms should embed bridge and mixer routing scores into their transaction monitoring systems. Automated holds should be placed on financial flows that match known obfuscation patterns. Furthermore, the validation of Travel Rule data should be converged with sanctions and terrorist financing screening processes before funds are released.

6.7. Counterparty governance

UAE licensed firms should adopt a strict approach to counterparty governance, transacting only with VASPs that are appropriately licensed or registered in their relevant jurisdictions.

6.8. Travel Rule Effectiveness

To ensure the effectiveness of their Travel Rule compliance, firms should seek to use Travel Rule solution providers that support broad interoperability with other VASP solutions, enabling reliable exchange of originator and beneficiary information across different networks and counterparties. The compliance rates of counterparties should be monitored, and periodic effectiveness testing should be conducted to identify and remediate any weaknesses in the firm's Travel Rule processes.

6.9 Training and Awareness

All staff who are involved in AML/CFT/CPF compliance should receive regular training on the UAE licensed firm's policies and procedures, as well as on emerging typologies and red flags. This training should be tailored to the specific roles and responsibilities of the staff and should be updated regularly to reflect changes in the regulatory environment and the threat landscape.

VASPs should also conduct regular awareness campaigns to ensure that all staff understand the importance of AML/CFT/CPF compliance and their role in preventing ML/TF/PF.

6.10 Reporting suspicious activities and transactions to the UAEFIU

Reporting suspicious activities is essential for combating financial crime and safeguarding the integrity of the national financial system by detecting transactions involving criminal actors and preventing the movement of illicit assets. A virtual asset service provider is obligated to file a suspicious transaction report (STR), suspicious activity report (SAR), or other relevant report directly to the UAE Financial Intelligence Unit ("UAE FIU") without delay, when there are reasonable grounds to suspect that a transaction, whether completed or attempted, regardless of the amount is intended for use in criminal activity.

7. Supervisory Priorities (SCA / VARA / DFSA / FSRA / CBUAE)

To support the effective implementation of the regulatory framework and manage the risks outlined in this paper, the UAE's supervisory authorities will adopt a coordinated and proactive approach. The list below sets out the key supervisory priorities for the SCA, VARA, DFSA, FSRA, and the CBUAE, noting that the

risk profile of virtual asset activities varies depending on
the nature of the activity and the characteristics of the entity involved, which in turn determines which supervisory strategies are applied and how each authority implements them.

1. **Deter unlicensed activity:** Supervisory authorities will continue to take strong action to deter unlicensed activity in the UAE. This will include issuing public warnings, imposing financial penalties, and taking down the websites and social media accounts of unlicensed operators. UAE licensed firms will be required to display their license information clearly in all marketing materials, and supervisors will require UAE licensed firms to maintain and provide evidence of their counterparty whitelists.

2. **Travel Rule effectiveness reviews:** During onsite inspections and thematic reviews, supervisors will test the effectiveness of the firms' Travel Rule compliance programs. This will include testing the completeness of transaction messages, the logic for rejecting or holding transactions, and the alignment of Travel Rule screening with other AML/CFT/CPF compliance processes. Anonymized findings from these reviews will be published to share best practices and highlight common failure modes.

3. **CDD/EDD, Business Risk Assessment and Customer Risk Assessment effectiveness reviews**: During onsite inspections and thematic reviews, supervisory authorities will assess the effectiveness of firms' customer risk assessment and customer due diligence frameworks. This will include testing the accuracy of customer risk classification, the adequacy of CDD and EDD measures applied, the timeliness of risk reviews, and the alignment of business and customer risk outcomes with transaction monitoring, sanctions screening, and escalation processes. Where appropriate, anonymised findings will be published to promote good practices and highlight common control weaknesses.

4. **Virtual assets analytics guidance:** Supervisory authorities will issue guidance on their expectations for virtual assets and stablecoin analytics. This may include guidance on the use of cluster-risk analysis, the setting of chain-hop thresholds, and the identification of typologies associated with OTC and P2P transactions at on-ramps and off-ramps, including at banks and exchange houses.

5. **Cross-regime alignment:** The UAE's supervisory authorities will continue to work closely together through the Supervisory Sub-Committee of the National AML/CFT Committee (NAMLCFTC) to further strengthen coordination and enhance alignment across the different regulatory regimes..

6. **Sector outreach:** The Joint Guidance on virtual assets will be refreshed with updated red flags and case vignettes to reflect the latest trends and typologies. Supervisory authorities will also coordinate their communications with the private sector through the national AML/CFT framework/mechanisms to ensure that UAE licensed firms are kept informed of emerging risks and regulatory expectations.

8. Red-Flag checklist (for day-to-day monitoring)

To assist UAE licensed firms in their day-to-day monitoring activities, the following checklist of red flags has been developed. This checklist is not exhaustive, but it provides a useful starting point for identifying potentially suspicious activity. UAE licensed firms should incorporate these red flags into their transaction monitoring systems and ensure that their compliance staff are trained to recognize and respond to them.

8.1. Customer behaviour

- The customer refers to a "merchant" or "broker" on a social media platform such as Telegram or WhatsApp as the counterparty to a transaction, and is resistant to naming a licensed VASP.
- The customer insists on splitting transfers to avoid transaction monitoring thresholds, or there are repeated failures to provide originator and beneficiary data from the same foreign VASP.

8.2. Transaction Patterns

- High-frequency transfers of stablecoins, eg. USDT on the TRON network, with evidence of bridge and mixer activity within hours of the transaction, followed by rapid attempts to cash-out into AED.
- Inbound funds that are linked, through blockchain analytics, to sanctioned ecosystems or to clusters that have been associated with hacks or other illicit activities.

8.3. Counterparty/VASP

- The counterparty VASP is not present on the public registers of UAE Supervisory Authorities or if it's a foreign VASP, within the jurisdiction's relevant licensing register.
- The counterparty VASP has a history of public enforcement notices or other adverse media coverage.

9. Data & metrics firms should track (for reporting to boards and supervisory authorities)

To ensure effective oversight and risk management, it is essential that UAE licensed firms track and report on a range of data and metrics. This data will provide valuable insights into the UAE licensed firm's risk exposure and the effectiveness of its controls. The following are some of the key data and metrics that should be tracked for reporting to the firm's boards and to the firm's respective supervisory authorities.

- **Share of incoming/outgoing volume by asset type & chain:** UAE licensed firms should track the share of their incoming and outgoing transaction volume by asset type (e.g., stablecoins, BTC, ETH) and by blockchain (e.g., TRON, ETH, BSC). This will provide a clear picture of the firm's business mix and its exposure to different types of assets and blockchains.
- **Bridge/mixer exposure:** UAE licensed firms should track this to assess their exposure to cross-chain obfuscation techniques. Firms should track the percentage of their transaction volume that occurs within a certain number of hours of a known bridge or mixer interaction. They should also track the median hop count for transactions, as a high number of hops can be an indicator of suspicious activity.
- **Travel rule key performance indicators:** UAE licensed firms should track a range of key performance indicators to monitor the effectiveness of their Travel Rule compliance. This should include the percentage of compliant messages, the reject and return rates for non-compliant messages, and the top non-compliant counterparties.
- **Counterparty risk:** To manage their counterparty risk, UAE licensed firms should track their whitelist coverage (i.e., the percentage of their counterparties that are on their approved whitelist) versus their total number of counterparties. They should also monitor for any enforcement actions or adverse media coverage related to their counterparties, and for any exposure to sanction-exposed clusters.
- **STR/SAR triggers & outcomes:** UAE licensed firms should track the triggers for their suspicious transaction reports / suspicious activity reports (STRs/SARs). This should include the time taken to file an STR/SAR and any feedback received from the UAE Financial Intelligence Unit (UAE FIU).

This data will help firms to refine their transaction monitoring rules and to improve the quality of their reporting.

10. Case Studies

To further illustrate the practical application of the concepts discussed in this paper, the following case studies have been developed. These case studies are designed to be used for training purposes, to help AML/CFT/CPF compliance staff and other relevant staff to identify and respond to potential instances of illicit financial activity relating to VASPs.

10.1. Case Study A: Sanctions evasion via Stablecoins

Scenario: A UAE-based customer receives a large inbound transfer of USDT from a blockchain cluster that has been associated with a sanctioned country. The funds are then immediately moved through a series of bridges and mixers before an attempt is made to cash them out into AED through a third-party payment provider.

Red flags:

- Funds originate from a blockchain cluster linked to a sanctioned country.
- Rapid movement through multiple bridges and mixers to obscure provenance.
- Attempt to convert into AED via a third-party provider, indicating potential sanctions evasion.

Actions:

- The VASP should immediately hold and decline the transaction, consistent with its obligation to prevent dealing directly or indirectly with sanctioned persons, jurisdictions, or tainted assets.
- The VASP should conduct enhanced due diligence on the client, including an assessment of the customer's expected activity, the economic purpose of the inbound transfer, and any direct or indirect exposure to the sanctioned region.
- Given the combination of high-risk indicators, including a sanctioned linked cluster, rapid obfuscation, and an attempted conversion to fiat, the VASP should file a suspicious transaction report with the UAEFIU and maintain all relevant records.
- Where appropriate, the VASP should reassess the customer's risk rating, strengthen monitoring triggers for similar activity, and ensure that controls around stablecoin based cross-chain transactions are calibrated to detect sanctions evasion typologies.

10.2. Case Study B: "Pig-Butchering" Consolidation

Scenario: A number of small USDT deposits from multiple sources in Asia are consolidated into two wallets and sent to a UAE-based platform that converts digital assets into local currency. The pattern matches known "pig-butchering" scams, where victims are tricked into sending funds over time. The consolidation and proposed cash-out suggest the money may be illicit proceeds.

Red flags:

- Multiple small USDT deposits from various sources in Asia.
- Funds consolidated into a few wallets before transfer.
- Rapid conversion to local currency on a UAE platform, consistent with illicit proceeds.

Actions:

- **The VASP should f**reeze the funds (or make it unavailable to the customer) to prevent further movement and reduce the risk of ML/TF/PF.
- **The VASPs should c**onduct a thorough review of the customer, transaction origin, and counterparties to assess potential ML/TF/PF risks.
- **Then, the VASP should n**otify the UAEFIU and relevant supervisory authorities. File a suspicious transaction report to the UAEFIU including all relevant wallet addresses, transaction details, and links to high-risk clusters or typologies.
- **The VASP should a**pply enhanced monitoring to the client's account and related wallets. Track subsequent transactions for patterns indicative of layering, obfuscation, or other ML/TF/PF activity.

10.3. Case Study C: Unlicensed P2P Merchant Exposure

Scenario: A UAE-based customer approaches a licensed VASP to open an account. During the onboarding process, the customer indicates that they intend to use the account to facilitate peer-to-peer (P2P) trading of virtual assets. The customer provides a Telegram handle as their primary method of contact and is unable to provide details of the counterparties with whom they will be trading.

Red Flags:

- Reliance on a Telegram handle as the primary contact method, limiting traceability.
- Inability to identify P2P trading counterparties, preventing effective risk assessment.
- Unclear or open-ended purpose for P2P activity, indicating elevated ML/TF/PF risk.

Actions:

- The VASP should conduct enhanced due diligence on the customer to understand the nature of their business and to verify that they are not operating as an unlicensed VASP.
- If the customer is unable to provide satisfactory information about their counterparties or if the VASP determines that the customer is likely to be facilitating unlicensed VASP activity, the VASP should decline to open the account.
- The VASP should file a suspicious transaction report to the UAEFIU if there are grounds to suspect that the customer is engaged in money laundering or other financial crime.

10.4. Case Study D: Cross-Chain Bridge Activity

Scenario: A licensed VASP receives an incoming transfer of Ethereum from a customer. Blockchain analytics reveal that the Ethereum was received by the customer's wallet just hours earlier through a cross-chain bridge from the BNB Smart Chain. Further analysis reveals that the funds on the BNB Smart Chain were received from a wallet that has been associated with a known hack. The transaction pattern appears unusual for the customer.

Red Flags:

- Funds came from a wallet linked to a known hack.
- Ethereum moved quickly through a cross-chain bridge.
- Transaction pattern is unusual for the customer and may indicate laundering

Actions:

- The VASP should immediately hold the funds and conduct enhanced due diligence on the customer.
- The VASP should request that the customer provide an explanation for the source of the funds and the reason for the bridge activity.
- If the customer is unable to provide a satisfactory explanation, or if the VASP determines that the funds are likely to be proceeds of crime, the VASP should decline to process the transaction and should file a suspicious transaction report to the UAEFIU.
- The VASP should also consider reporting the incident to law enforcement.

10.5. Case Study E: High-Velocity USDT on TRON

Scenario: A licensed VASP observes that one of its customers is conducting a high volume of USDT transactions on the TRON network. The transactions involve rapid transfers between multiple wallets, with funds being received and then immediately sent out to different addresses. The customer then attempts to off-ramp a large amount of USDT into AED.

Red Flags:

- High-velocity USDT transactions on TRON.
- Rapid movement between multiple wallets.
- Immediate off-ramp attempt.

Actions:

- The VASP should hold the off-ramp transaction and conduct enhanced due diligence on the customer.
- The VASP should use blockchain analytics to trace the origin of the USDT and to identify any links to illicit activity.
- If the VASP determines that the transaction pattern is consistent with money laundering or other financial crime, the VASP should decline to process the off-ramp and should file a suspicious transaction report to the UAEFIU.

10.6. Case Study F: Missing Travel Rule Data from Repeat Counterparty

Scenario: A licensed VASP receives multiple incoming transfers from the same foreign VASP. In each case, the Travel Rule data is either missing or incomplete. The licensed VASP has reached out to the foreign VASP to request the missing data, but the foreign VASP has been unresponsive.

Red Flags:

- Repeated failures to provide Travel Rule data.
- Unresponsive counterparty.

Actions:

- The VASP should reject or return the transactions until complete Travel Rule data is provided.
- The VASP should escalate the issue to senior management and should consider terminating the relationship with the foreign VASP if the Travel Rule compliance does not improve.
- The VASP should report the issue to the relevant supervisory authority.

11. Conclusion

The integrity of the UAE's financial system, particularly in the virtual asset sector, relies on the diligence and proactive measures of Licensed VASPs. While UAE Supervisory Authorities provide a clear framework and supervision, the primary defense against Money Laundering, Terrorist Financing, and Proliferation Financing risks lies with the industry. Compliance should not be static but must evolve with emerging threats.

As set out in the paper, UAE financial institutions should implement advanced, chain-specific analytics to detect high-risk transactions, including rapid cross-chain movements and bridge or mixer activity. Automated controls should be in place to hold or reject suspicious flows. Firms must also transact only with verified counterparties and fully operationalize the Travel Rule, rejecting transactions with missing originator or beneficiary data and terminating relationships with non-compliant foreign VASPs.

Boards and senior management must also treat ML/TF/PF risk in relation to VASPs as a core priority. This includes thorough due diligence on new tokens, verification of reserves and redemption mechanics, and monitoring key metrics such as bridge and mixer exposures and Travel Rule compliance. Continuous, scenario-based staff training is essential to ensure emerging typologies and red flags are identified and addressed.

The UAE’s regulatory framework provides a solid foundation for licensed firms to operate. By maintaining strong operational AML/CFT/CPF practices, effective technology, and a strong/vigilant culture, firms help protect the integrity of the industry and support the UAE’s reputation as a trusted financial centre. Failure to meet these standards may lead to regulatory action.

Appendix A: Glossary of Terms

AED - United Arab Emirates Dirham

AML - Anti-Money Laundering

ADGM - Abu Dhabi Global Market

Blockchain - A distributed ledger technology that records transactions across multiple computers in a way that makes the records difficult to alter retroactively.

Bridge - A technology that allows virtual assets to be moved between different blockchain networks.

CBUAE - Central Bank of the United Arab Emirates

CDD - Customer Due Diligence

CFT - Countering the Financing of Terrorism

DAO - Decentralized Autonomous Organization, an organization that is governed by smart contracts and operates without centralized control.

DEX - Decentralized Exchange, a cryptocurrency exchange that operates without a central authority.

DFSA - Dubai Financial Services Authority

DIFC - Dubai International Financial Centre

DeFi - Decentralized Finance, a range of financial services that are provided through decentralized protocols and smart contracts.

EDD - Enhanced Due Diligence

FATF - Financial Action Task Force

FSRA - Financial Services Regulatory Authority

KYC - Know Your Customer

LFI - Licensed Financial Institution

Mixer - A service that is designed to obscure the origin of virtual assets by mixing them with other assets.

ML - Money Laundering

NFT - Non-Fungible Token, a unique digital asset that is often used as a collectible or as a representation of digital art.

OTC - Over-the-Counter, a market where transactions are conducted directly between two parties, without the supervision of an exchange.

P2P - Peer-to-Peer, a decentralized network where participants interact directly with each other, without intermediaries.

PF - Proliferation Financing

RWA - Real-World Asset, a physical or traditional financial asset that is represented as a token on a blockchain.

SAR/STR - Suspicious Activity Report/ Suspicious Transaction Report

SCA - Securities and Commodities Authority

Stablecoin - A type of virtual asset that is designed to maintain a stable value relative to a reference asset, typically a fiat currency.

TF - Terrorist Financing

TRON - A blockchain network that is popular for stablecoin transactions due to its low fees and fast settlement times.

UBO - Ultimate Beneficial Owner, the natural person who ultimately owns or controls a legal entity.

USDT - Tether, a fiat-backed stablecoin that is designed to maintain a value of one US dollar.

VA - Virtual Asset

VARA - Virtual Assets Regulatory Authority, the regulator of virtual assets in Dubai (excluding the DIFC).

VASP - Virtual Asset Service Provider