Supervisory subcommittee

Emerging ML/TF/PF Risks and Trends in the Financial Sector

Table of Contents

1. INTRODUCTION

The global financial landscape is undergoing rapid transformation, driven by technological innovation, geopolitical shifts, and evolving criminal methodologies. These changes have introduced new and complex risks related to money laundering (ML), terrorism financing (TF), and proliferation financing (PF), which pose significant threats to the integrity and stability of financial systems worldwide.
Licensed financial institutions, Insurance Companies and Related Professions, and Registered Hawala providers (LFI/ICRP/RHPs) in the United Arab Emirates (UAE) operate within this dynamic environment and must remain vigilant to emerging trends that challenge traditional AML/CFT/CPF compliance frameworks. Criminal actors are increasingly exploiting advancements such as digital assets, decentralized finance (DeFi), and cross-border payment systems, while leveraging opaque corporate structures and trade-based mechanisms to obscure illicit financial flows. At the same time, global crises - such as armed conflicts, sanctions regimes, and supply chain disruptions - have amplified vulnerabilities, creating fertile ground for proliferation financing and terrorism-related activities. Moreover, the Financial Action Task Force's (FATF) guidance - "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers[1]" - identifies generative AI and crypto assets as top threats in 2025. These developments demand a proactive and risk-based approach from the LFIs/ICRPs/RHPs to safeguard the country's financial system against misuse by illicit actors.

This report provides LFI/ICRPs/RHPs with a comprehensive overview of some of the key emerging ML/TF/PF risks and trends, highlighting typologies, red flags, and sector-specific vulnerabilities. By understanding these evolving threats, institutions can strengthen their ML/TF/PF risk management strategies, enhance detection capabilities, and contribute to the resilience of the financial ecosystem. The CBUAE is committed to upholding the highest standards of AML/CFT/CPF compliance in alignment with Financial Action Task Force (FATF) recommendations and national AML/CFT/CPF regulatory requirements. This report should be read in conjunction with other risks and typology papers issued by the CBUAE and the UAE Financial Intelligence Unit. One report to note, that was issued by the UAE FIU, is the Financial Crime Typologies in the Financial Sector Summary Report January 2024[2], which addresses the financial crime typologies categorized by frequently observed predicate offences that are contributing to money laundering, alternative banking services and underground banking, and trade system and trade-based money laundering techniques.

This report is issued in line with Article 16 Federal Decree-Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing - which provides the legal foundation for the CBUAE's AML/CFT Supervision Department to periodically communicate ML/TF/PF risks, trends, and compliance expectations to the LFI/ICRPs/RHPs.

SCOPE

This report examines emerging risks and trends related to money laundering, terrorist financing, and proliferation financing (ML/TF/PF) within the UAE financial sector. It encompasses all categories of financial institutions operating under the regulatory framework of the Central Bank of the UAE (CBUAE), excluding Virtual Asset Service Providers (VASPs), which are addressed in a separate report titled "Virtual Asset Service Providers (VASPs) – Emerging ML/TF/PF Risks, Threats & Vulnerabilities in the UAE" - issued December, 2025.

The analysis highlights both domestic vulnerabilities and global developments that may impact the UAE, with particular focus on technological innovations, geopolitical dynamics, and evolving criminal typologies. These insights

[1] https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html
[2] https://www.uaefiu.gov.ae/media/zqun0wsh/financial-crime-typologies-in-the-financial-sector-jan-2024.pdf

aim to support financial institutions in strengthening their risk management frameworks and aligning with regulatory expectations in an increasingly complex threat environment

METHODOLOGY

The following reviews were undertaken by AMLD to come up with the key ML/TF/PF risks and trends presented in this report.

a) Review of the country's National and Sectoral Risk Assessments.
b) Analysis of supervisory data collected from LFI/ICRPs/RHPs through off-site monitoring and on-site examinations.
c) Examination of international typologies and guidance issued by FATF, FATF Style Regional Bodies, and other global bodies.
d) Trend analysis using recent enforcement cases, and cross-border intelligence.
e) Consultation with internal and external stakeholders, including policy experts and compliance officers, to validate emerging risk indicators.

This structured approach ensured the report reflects current realities, anticipates future threats, and provides practical insights for LFI/ICRPs/RHPs to enhance their AML/CFT/CPF frameworks.

KEY EMERGING RISKS & TRENDS

Artificial Intelligence (AI) and Machine Learning (ML) Exploitation.

While AI is increasingly used for compliance, criminals are also using AI to generate false documents, create realistic deepfakes for identity verification circumvention, and develop more sophisticated fraud schemes.

How it Occurs: Criminals use AI to generate synthetic identities and highly realistic deepfakes (audio/video impersonations) to bypass traditional identity verification and biometric security systems during client onboarding or transaction authentication. This allows for the creation of numerous fraudulent accounts or the compromise of existing high-value accounts at scale. Institutions that are primarily affected include Banks, Exchange Houses, Stored Value Facilities (SVFs), and Payment Token Service Providers (PTSPs), that may be using digital onboarding and biometric verification for remote customers. Call centres are also vulnerable to voice deepfakes.

Detection/Mitigation: LFI/ICRPs/RHPs vulnerable to this risk should, in addition to other Customer Due Diligence / Know Your Customer measures, employ "liveness detection" technologies to confirm a genuine human is present during verification, not a static image or a video. Further, LFI/ICRPs/RHPs should combine AI-driven identity document (ID) capture with comprehensive data consistency and validation checks across extracted information to spot anomalies in identity documents, and should implement behavioural biometrics to monitor user interactions for deviations from normal human behaviour.

Greenwashing & Environmental, Social, and Governance (ESG) Related Fraud.

As Environmental, Social, and Governance (ESG) investing grows, opportunities for "greenwashing" (disguising illicit funds as legitimate green investments) are emerging.

Legitimate green investments are financial products designed to fund environmentally sustainable projects, such as renewable energy, clean transportation, and climate adaptation, often structured through green bonds, ESG funds, or sustainability-linked loans under recognized standards like International Capital Market Association (ICMA)[3] or the EU Green Bond framework. Under the UAE Sustainable Finance Framework 2021–2031, some Licensed Financial Institutions like Banks are actively issuing green bonds and sukūk to support sustainability goals.

However, these instruments can be exploited for money laundering as they often involve complex cross-border structures, perceived low-risk profiles, and limited transparency, allowing criminals to layer illicit funds through green-labelled securities; use shell entities to obscure beneficial ownership; or engage in "greenwashing" by misrepresenting projects as sustainable to legitimize dirty money. One incident to note, which shows that ESG greenwashing and AML/CFT/CPF failures tend to co-exist, relates to the U.S. Security Exchange Commission (SEC), which in October 2023, charged DWS Investment Management (Deutsche Bank's asset-management arm) for misstatements about its ESG investment process and failure to develop an adequate AML programme, and imposing a USD 25 million penalty[4]. Further, in April 2025, Frankfurt prosecutors imposed a €25 million greenwashing fine on DWS for misleading ESG-related marketing and documentation[5].

How it Occurs: Greenwashing involves deceptively marketing financial products, assets, or entire entities as environmentally friendly or ethically sound when they are not. Criminals may exploit the rapidly growing demand for ESG investments to launder illicit funds by:

- **Investing in shell companies that own "green" assets**: Purchasing assets like a small solar farm or a land with conservation potential using illicit funds, then marketing the returns as legitimate ESG returns.
- **Misrepresenting fund origins**: Blending dirty money with legitimate capital in large, complex green investment funds to obscure its origin.
- **Exploiting lack of standardized reporting**: The absence of universally mandated ESG disclosure standards allows entities to make vague or unverifiable "green" claims, making it difficult to differentiate genuine sustainable finance from fraud.

Banks (through green bonds, loans, and investment funds), Asset Managers, Insurance Companies (through sustainable insurance products), and any Investment Fund operating in the ESG space are exposed ML risks associated with greenwashing and ESG.

These developments are particularly relevant to UAE's LFI/ICRP/RHPs as United Arab Emirates positions itself as a regional hub for sustainable finance, carbon markets and energy-transition investment.

Detection/Mitigation: The following are some of the key detection and mitigation measures LFI/ICRP/RHPs should develop and effectively implement:

a) **Implement robust due diligence on ESG claims**: LFI/ICRP/RHPs should scrutinize the actual underlying assets, certifications, and third-party verifications of an investment's "green" credentials. This requires specific training for compliance teams.
b) **Enhance source of wealth/funds checks**: by applying rigorous enhanced due diligence on clients investing large sums in ESG funds, especially if the source of wealth is from high-risk sectors (e.g., extractive industries known for environmental breaches).
c) **Monitor for inconsistencies**: LFI/ICRP/RHPs should look for discrepancies between a company's known business activities and its sudden declaration of significant ESG-focused initiatives or funds.

[3] **International Capital Market Association (ICMA)** is a global trade association that sets standards and guidelines for capital markets, including the widely used **Green Bond Principles** that define best practices for issuing environmentally focused bonds.
[4] https://www.sec.gov/newsroom/press-releases/2023-194

[5] https://www.reuters.com/sustainability/german-asset-manager-dws-fined-25-mln-eur-greenwashing-case-2025-04-02/

Abuse of Trade Finance for Proliferation Finance (PF):

Amid escalating global concerns driven by armed conflicts, the risks of proliferation financing have intensified. While this threat has been addressed in previous UAE's National Risk Assessment and the UAE FIU reports, it remains critical to highlight the misuse of trade finance for proliferation financing, given its continued relevance and evolving nature. The UAE's strategic position as a global trade and transport hub, combined with its proximity to high-risk jurisdictions, makes the country particularly vulnerable to this risk. Proliferation Financing (PF) often exploits vulnerabilities in international trade, such as misrepresentation of goods, values, or destinations, especially for dual-use items related to weapons of mass destruction.

How it Occurs: PF often relies on disguising the end-use or end-user of dual-use goods (items with both civilian and military applications). Non-state actors - entities and persons - designated under the United Nations Security Council (UNSC) sanctions for proliferation financing, purchase individual components rather than complete systems to avoid scrutiny, and use front companies to create a facade of legitimate trade. They falsify invoices, under/over-invoice, and misrepresent goods to exploit vulnerabilities in international trade.
Banks, Trade Finance divisions, and Insurance Companies are primarily the most affected institutions, given their financial role as the "lifeblood" of cross-border commerce.

Detection/Mitigation: LFI/ICRP/RHPs should establish robust transaction monitoring systems that will have the capacity to "red flag" trade-based alerts. Further, comprehensive internal processes should be put in place, which ensures that adequate and relevant trade documentation is always obtained and scrutinized as part of verifying the underlying transactions. LFI/ICRP/RHPs should look for inconsistencies in shipping routes, generic goods descriptions, and transaction values that do not match market rates. Continuous enhanced training of Trade Finance teams and front-line staff on dual-use goods lists and PF indicators is very critical.

Growth in Illicit Transactions Associated with VAs and VASPs activities in the Banking Sector.

Over the past years, the country has witnessed a significant growth in its virtual asset (VA) sector. This rapid expansion, however, has increased the exposure of conventional banking sector to ML/TF/PF risks, primarily driven by the convergence of traditional and digital finance channels.

In November 2023, the Supervisory Authority Sub-Committee of NAMLCFTC[6] issued the "Joint Guidance on Combating the Use of Unlicensed Virtual Asset Service Providers in the United Arab Emirates[7]". Further, in 2023, the CBUAE issued, the "Guidance for Licensed Financial Institutions on Risks Related to Virtual Assets and Virtual Asset Service Providers[8]".

Whilst these documents outline the vulnerabilities of the LFI/ICRP/RHPs; the ML/TF/PF trends and methods associated with VAs/VASPs; and the controls that need to be placed and effectively implemented - this Report further outlines the growing exposure to ML/TF/PF risks that Banks and other Financial Institutions are increasingly getting exposed to in light of the growth being witnessed in virtual assets space, and the ever-changing risk trends and methods.

---

[6] NAMLCFTC is the National Anti-Money Laundering and Combatting Financing of Terrorism and Financing of Illegal Organizations Committee

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

[8] https://www.centralbank.ae/media/avwlktgy/cbuae-guidance-for-lfis-on-risks-related-to-virtual-assets-and-virtual-assets-providers_final-clean-version1.pdf#:~:text=customer)%20VASPs:%20Additionally%2C%20LFIs%20may%20be%20indirectly,include%20the%20provision%20of%20accounts%20or%20custodial

How it Occurs:

1) Criminals, unlicensed or non-compliant VASPs can open bank accounts using potentially legitimate or slightly obfuscated business descriptions. They then use these accounts to process significant volumes of fiat currency transactions that are the result of virtual asset activities (e.g., selling crypto for cash). By routing funds through a traditional bank account, they introduce illicit or high-risk funds into the regulated financial system, often obscuring the true origin and nature of the transactions from the bank's AML/CFT/CPF systems.
2) Funds are moved from an unregulated or peer-to-peer (P2P) crypto exchange, where robust Know Your Customer (KYC) checks might be absent, into a traditional bank account. Alternatively, illicit fiat funds in a bank account can be used to purchase crypto (provide liquidity), which is then moved to unhosted wallets or mixed with other crypto, making tracing difficult. The bank often lacks visibility into the specifics of the crypto endpoint (wallet details, ownership).
3) Criminals use sophisticated synthetic media (deep-fakes) or stolen/forged digital identities to open bank accounts remotely. Once opened, these mule accounts receive proceeds from illicit virtual asset trades (e.g., ransomware payments, fraud proceeds) and then layer them into the broader financial system, often by transferring them to other accounts or purchasing high-value goods.

Detection/Mitigation: As provided in the AML/CFT/CPF laws, regulations and guidance, Banks should focus on strengthening their due diligence and monitoring capabilities to counter virtual asset-related financial crime risks. Banks must invest in identity verification and transaction monitoring technology; and implement robust digital identity verification processes and biometric authentication measures as part of customer onboarding and throughout the ongoing business relationship, to ensure the integrity of customer due diligence, prevent impersonation and identity fraud and strengthen the overall AML/CFT control environment Regular employee training is essential to ensure staff can recognize red flags and escalate suspicious virtual asset-related transactions and activities appropriately.

Sanctions Evasion Risks – Related to Commonwealth of Independent States (CIS) [9]

In accordance with Section 3.5 of the Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening, LFI/ICRP/RHPs are required to establish and maintain sanctions screening lists that are commensurate with their risk profile. At a minimum, such lists must include all names contained in the United Nations Consolidated List and the UAE Local Terrorist List. Institutions may, based on their risk assessment, supplement these with additional jurisdictional lists (e.g., OFAC, EU, UK), internal lists of persons with a known sanctions' nexus, geographic identifiers (cities, regions, ports), banking-related terms (such as BICs), and lists of prohibited goods or securities, where applicable.

It is imperative that lists issued by the United Nations Security Council and the UAE Cabinet are applied universally across all customers and transactions. The inclusion of other lists like OFAC should be determined on a risk-based approach, consistent with the institution's documented sanctions risk appetite.

This emerging risk is particularly relevant for LFI/ICRP/RHPs whose sanctions risk appetite explicitly recognizes the applicability of international regimes such as the Office of Foreign Assets Control (OFAC).

How it Occurs: In light of historical geopolitical and diplomatic ties between the Russian Federation and Commonwealth of Independent States (CIS), an emerging typology has been observed involving individuals and entities in Russia leveraging CIS-based entities to circumvent international sanctions and export control measures. These jurisdictions are frequently utilized to facilitate the transshipment of goods subject to import or export restrictions to and from the Russian Federation. The following trends have been identified:

[9] The following are the Commonwealth of Independent States: Azerbaijan; Kazakhstan; Armenia; Belarus; Russia; Turkmenistan; Uzbekistan; Kyrgyzstan; Belarus; Moldova; Russia; Tajikistan

1) **Changes in Business Activity post Russia Sanction Regime**: The are some entities which had sudden or significant changes in business activity post the start of the Ukraine-Russia war. An example to note relates to a customer which traded in items listed on the Common High Priority List. Prior to the war, the customer shipped directly to Russia, but started using a different business model, including change in shipment routes and a spike in counterparties located in CIS countries.
2) **Trading Through Intermediaries**: some entities change their business operations and supply chains by introducing third parties located in CIS countries.
3) **Use of CIS-Based Shell or Front Companies**: Entities in CIS jurisdictions are established or leveraged as intermediaries to obscure the Russian Federation's involvement. These entities often have minimal operational substance and serve primarily as conduits for trade.
4) **Transshipment of Restricted Goods**: Goods subject to export controls (e.g., dual-use items, high-tech components) are shipped to CIS countries first. From there, they are re-exported to Russia, circumventing direct sanctions restrictions.
5) **Layering Through Complex Trade Routes**: Multi-jurisdictional routing of goods and payments creates opacity. Further, usage of free trade zones and bonded warehouses in CIS countries is also used to mask ultimate destination.
6) **Financial Flows**: Payments are routed through CIS-based banks or payment service providers to avoid direct links to sanctioned Russian entities. When making the payments, third-party intermediaries and nested correspondent banking relationships are used.

Detection/Mitigation: LFI/ICRP/RHPs should implement robust detection measures to identify potential sanctions evasion through CIS jurisdictions. Key controls include - enhanced due diligence on customers and counterparties with trade links to CIS countries; verification of beneficial ownership to uncover Russian connections; and transaction monitoring for red flags such as unusual trade routes, high-risk commodities, and sudden spikes in CIS-related activity. Trade finance documentation, including letters of credit and end-user certificates, must be scrutinized for inconsistencies or signs of transshipment. Additionally, LFI/ICRP/RHPs should maintain strong governance and oversight over the application of the sanctions risk appetite provisions.

CASE STUDIES

UAE Banking Sector.

The following case studies were observed across the UAE banking sector in 2025. The case studies are based on supervisory observations, FIU intelligence, and industry feedback from examinations and remediation programmes.

Case Study 1: Money Mule Networks and Digitally Enabled Fraud

In Q1 2024, a newly incorporated trading entity opened an account at a UAE bank. Within weeks, the account exhibited multiple small-value cash deposits via ATMs across different Emirates, followed by rapid withdrawals and outward transfers. Investigation revealed the account was part of a network of 'money mules' laundering proceeds from investment and task fraud schemes. Key red flags included inconsistent business activity, structured deposits below reporting thresholds, and repetitive commentary across multiple alert closures.

In its 2024 annual report, the FIU reported a 57% year-on-year increase in fraud-related STRs, with a significant portion linked to digital scams[10]. Banks should develop and outsource behavioural and network analytics to detect such mule networks.

Case Study 2: Trade-Based Money Laundering (TBML)

A UAE-based bank extended a USD 10 million Trade Finance facility to a trading company dealing in electronics and building materials. Over an 18-month period, repetitive over-invoicing, duplicated documentation, and payments routed through offshore intermediaries indicated a TBML scheme. The FIU's strategic Analysis Report (2024)[11] highlights similar patterns, where fictious documentation and over/under-invoicing remain dominant TBML typologies.

Banks and other relevant LFI/ICRPs/RHPs exposed to this risk should make use of advanced technology like AI and machine learning, to analyse trade documents for inconsistencies and monitor transactions for suspicious patterns. Further, they should establish and implement data-driven trade monitoring systems that integrate customs, shipping, and market-price data.

Case Study 3: Virtual Asset to Fiat Conversion via Banked VASPs

A licensed Virtual Asset Service Provider (VASP) maintained settlement accounts with a UAE bank. The VASP received high-volume fiat inflows from foreign exchanges, followed by small-denomination outward payments to personal accounts. The activity masked illicit virtual asset proceeds.

Banks must map VA-fiat flows, monitor settlement accounts for conversion cycles, and assess VASPs' exposure to foreign high-risk exchanges.

Case Study 4: Sanctions Evasion via Free-Zone corporate Structures

A free-zone trading entity processed US dollar payments for 'industrial equipment' to a sanctioned destination, masking ownership through offshore intermediaries. Beneficial Ownership information was incomplete, and payments were routed through multiple UAE banks to fragment the audit trail. The FATF report on Complex Proliferation Financing and Sanctions Evasion Schemes (2025)[12] and the UAE FIUs Strategic Analysis report on TBML (2024)[13] highlight such kind of sanctions evasion using free-zone corporate structures and front companies.

Banks must verify Beneficial Ownership during the Customer Due Diligence processes. Furthermore, Banks should escalate complex corporate structures to the Compliance Officer or Senior Management for verification and approval; and should link sanctions screening tools with the core trade finance payment systems to ensure data accuracy and completeness during screening.

---

[10] https://www.uaefiu.gov.ae/media/lfdhf4sa/fiu-annual-report-2025-e_-revised-sep-9-hyperlinked.pdf

[11] https://www.uaefiu.gov.ae/media/vduba40z/updated-strategic-analysis-report-on-trade-based-money-laundering-rsas-2024.pdf

[12] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf

[13] https://www.uaefiu.gov.ae/media/vduba40z/updated-strategic-analysis-report-on-trade-based-money-laundering-rsas-2024.pdf

Case Study 5: Real-Estate Linked Integration via Mortgage Repayments

A Private banking client repaid a mortgage worth AED 8 million within six months, funded by multiple third-party transfers. Analysis revealed the funds originated from offshore shell companies under investigation abroad. The property was quickly resold to a related-party entity. Such patterns typify Real-Estate integration, where illicit funds are laundered through early loan settlements.

Banks should perform Due Diligence not only at loan origination but also at repayment and discharge stages. Integration of mortgage, property registry, and AML data is essential.

Case Study 6: Fraudulent "green" investment schemes

November 2023[14]: Fraudsters in United Kingdom were sentenced to imprisonment after they lured wealthy individuals to invest in fake "green" projects and stole £20 million of the investors' money and laundered it via bank accounts and secret trusts, spending it on luxury properties in London, Australia, and Dubai, as well as hiding some in offshore investments.

The fraudsters told investors that their money would be spent on research and development into carbon credits, attracting more than £65 million in investment in the 'green' scheme. However, only £16 million of this was spent on planting trees.

Emerging Typologies in the Stored Value Facilities (SVF) and Retail Payment Service and Card Schemes (RPSCS) Sector

Merchants established solely for laundering illicit funds

This typology involves the creation of shell or front merchants that appear legitimate but exist primarily to launder illicit funds rather than conduct genuine business operations. Such entities often obtain new trade licenses and rapidly engage in high transaction volumes with minimal or no genuine customer interaction. Common indicators include the absence of an online presence, incomplete or unverifiable merchant websites, and shared IP addresses or devices across multiple entities, suggesting centralized control or coordination.

These merchants typically process funds through card transactions, online gateways, or payment service providers to create the illusion of legitimate sales. The lack of verifiable commercial activity and overlapping digital footprints highlight the high risk of money laundering and potential collusion. Financial institutions should apply enhanced due diligence, monitor transaction anomalies, and cross-reference digital identifiers to detect and disrupt such synthetic merchant structures.

Mule or Rented Accounts

This typology highlights the misuse of legitimate merchant or personal accounts—often referred to as mule or rented accounts—by third parties to facilitate the movement of illicit funds under the guise of genuine business transactions. Fraudsters or money launderers use these accounts to simulate commercial activity, typically through multiple low-value transactions structured just below monitoring or alert thresholds, to evade detection. A common indicator is the

[14] https://www.cps.gov.uk/cps/news/oxbridge-fraudster-gets-another-eight-years-jail-failing-pay-back-ps27m-court-order

use of the same payment card across multiple merchants or accounts, along with repetitive transactions of nearly identical amounts.

Additionally, a geographical mismatch between the merchant's registered location and the customers' origin often signals suspicious activity. Such behaviour patterns indicate potential layering of illicit proceeds and concealment of beneficial ownership. Institutions should monitor these trends closely, implement typology-based transaction monitoring rules, and enhance customer due diligence to identify and mitigate risks associated with mule or rented accounts.

High-Risk Countries (Iraq / Libya) Typology

This typology highlights the misuse of UAE-based merchant and financial channels by entities linked to high-risk jurisdictions such as Iraq and Libya. Iraq's financial system faces stringent controls on the flow of US Dollars, the main currency for international trade, prompting illicit actors to exploit alternative corridors.

Given the UAE Dirham's peg to the USD and the UAE's role as a global trading hub, certain merchants have been used to facilitate indirect USD-linked transfers and trade settlements. As part of the typology, significant proportion of transactions were identified as originating from cards issued in high-risk markets. The typology was identified after multiple merchants were noted to have the majority of their customer transactions originating from these high-risk countries, indicating potential cross-border money laundering and sanctions evasion risks.

Laundering via Exchange Houses -Saudi Riyal Typology

Criminal networks exploit Exchange Houses in UAE by conducting large or structured Saudi Riyal (SAR) cash conversions to Dirhams (AED). Their objective is to layer proceeds of crime generated in Saudi Arabia (KSA) or Gulf Cooperation Council (GCC) border areas, disguise illicit funds through routine currency exchanges, and reintegrate them into the UAE financial system as AED. UAE Authorities identified repeated structured SAR cash conversions into AED using bulk SAR notes, with transactions consistently kept below the reporting threshold of AED 55,000 (structuring).

Criminals recruited Money Mules (blue-collar labourers and low-income individuals) who were used to perform the exchange of currencies. This typology - which aligns with the FATF-identified third-party money laundering typologies - was observed during the period Y2022-2025 and was most prelevant in high risk Exchange Houses, and walk-in cash customers.

CONCLUSION

This report underscores the dynamic nature of ML/TF/PF risks within the UAE financial sector, emphasizing the need for continuous vigilance and adaptive risk management. While domestic vulnerabilities remain a priority, global developments—particularly technological innovations, geopolitical shifts, and evolving criminal typologies—pose significant challenges that require proactive measures.

LFI/ICRP/RHPs must integrate these insights into their compliance strategies, ensuring robust controls, timely detection, and effective mitigation to safeguard the integrity of the UAE's financial system against emerging threats.

Further guidance and typologies reports are available through the CBUAE Rulebook and the UAE FIU's website. Continuous engagement with these resources and proactive risk mitigation are vital to safeguarding the integrity of the UAE's financial system.