

Annual Report 2023

Intelligence-Driven Scalability and Progress Sustainability



UAE Financial Intelligence Unit (UAEFIU)

2023 Annual Report

TABLE OF CONTENTS

YEAR IN REVIEW 03

FOREWORD 06

H.E. Khaled Mohamed Balama	06
Ali Faisal Ba'Alawi	07

A RESILIENT AML/CFT INSTITUTIONAL FRAMEWORK IN THE UAE 08

ORGANIZATIONAL OVERVIEW 12

UAEFIU Mission and Mandate	13
UAEFIU Organizational Structure	15
A Strong Workforce Against Financial Crimes	16
UAEFIU's Strategic Functions	17

PROGRESS DELIVERED ON 2020-2023 AML/CFT NATIONAL STRATEGY 19

OPERATIONS AND COLLABORATIONS 22

Operational Analysis	23
Research and Strategic Analysis	27

2023 Strategic Analysis Products Highlights	29
Abuse of Legal Persons and Arrangements in Illicit Activities	29
Patterns of Abusing Financial Institutions in Drug Trafficking and Laundering its Proceeds	30
Real Estate Money Laundering Typologies and Patterns	31
Designated Non-Financial Businesses and Professions (DNFBPs)	32
Strengthening Domestic Cooperation	33
Fostering International Cooperation	36

OUTREACH AND COMMUNICATION 44

Expansive Outreach Activities	45
-------------------------------	----

APPENDICES 47

UAEFIU Report Types	48
List of Risk Indicators Based on Outcomes of Research and Strategic Analysis Section's Products	49

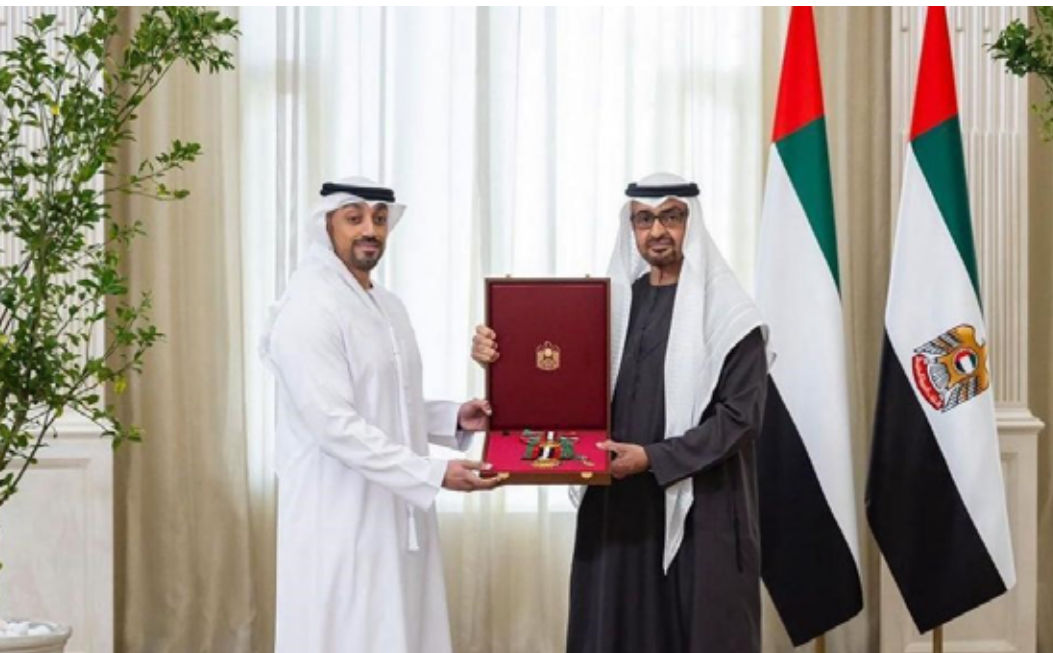
LIST OF ACRONYMS 59

YEAR IN REVIEW



UAE President with Higher Committee Overseeing the National Strategy on Anti-Money Laundering and Countering the Financing of Terrorism

His Highness Sheikh Mohamed Bin Zayed Al Nahyan, UAE President, met with the Higher Committee Group to recognize their significant efforts in achieving the UAE's removal from FATF's "Jurisdictions Under Increased Monitoring" list, marking a key milestone in enhancing the country's global commitment to financial transparency.



UAE President congratulates CoFIU

His Highness Sheikh Mohamed Bin Zayed Al Nahyan, UAE President, awarded the Financial Intelligence Unit on the recognition of its pivotal role in the UAE's removal from FATF's list of "Jurisdictions Under Increased Monitoring".



29th Annual Egmont Group Plenary in Abu Dhabi

The UAEFIU hosted the 29th annual Egmont Group Plenary in Abu Dhabi, reiterating its commitment to contribute towards the UAE's efforts to combat money laundering, and financing of terrorism. Held under the theme 'Use of advanced IT technologies by FIUs to enhance their operations,' the event saw participation from over 500 representatives from several global entities within the anti-money laundering field.

Enhanced cooperation to fight money laundering

The UAEFIU entered into agreements and pact with different entities including Abu Dhabi Global Market (ADGM), Dubai Financial Services Authority (DFSA), and the Executive Office for Control and Non-proliferation (EOCN), to join hands in fighting money laundering and fighting terrorism financing and proliferation financing through information exchange and bilateral cooperation.





Advanced strategic analysis program

The UAEFIU hosted an Advanced Strategic Analysis Program, organized by the ECOFEL, alongside the Middle East and North Africa Financial Action Task Force (MENAFATF), the International Monetary Fund (IMF), and the United Nations Office on Drugs and Crime (UNODC). The Strategic Analysis function within the UAEFIU focuses on identifying money laundering (ML) and terrorist financing (TF)-related trends and patterns in order to determine ML and TF threats and vulnerabilities.

UAEFIU Week with Law Enforcement Authorities

The UAEFIU dedicated a fruitful week with law enforcement authorities under the title "Together against Financial Crime". The UAEFIU discussed its strategy and operational plan for AML/CFT and devoted two sessions related to the abuse of financial institutions in drug trafficking and laundering its proceeds and the abuse of legal persons and arrangements in illicit activities. These activities were followed by a designed training program on advancing financial analysis backed with interactive practice sessions.



Podcast with the UK

The UK Financial Intelligence Unit (UKFIU) released a podcast focusing on the risks of money laundering associated with money service bureaus in the UK and the exchange house sector in the UAE. This podcast was hosted by the UKFIU and the National Crime Agency (NCA), with the UAEFIU joining the discussion.



DNFBPS workshop

The UAEFIU organized a workshop for Designated Non-Financial Businesses and Professions (DNFBPs) in cooperation with the Ministry of Economy, Abu Dhabi Global Market, and Dubai Financial Services Authority. The workshop discussed Designated Non-Financial Businesses and Professions (DNFBPs) requirements and their obligations to the anti-money laundering and combatting the financing of terrorism (AML/CFT) regime. During this workshop, the UAEFIU provided DNFBP reporting entities with the UAEFIU observations and guidance in submitting suspicious reports (STRs/SARs) through the UAEFIU reporting system.



FOREWORD

2023 has been a year of further progress for the UAE Financial Intelligence Unit (UAEFIU) in its vital role within the UAE's approach to combatting money laundering, terrorist financing, proliferation financing (ML/TF/PF), and cooperating closely with local and international authorities to achieve objectives at the local and international levels.

Firstly, I would like to commend the tireless efforts of the UAEFIU to strengthen its systems and its contribution to detect and reduce national risks related to ML/TF/PF in the country. Specifically, the upgrade in June 2023 of the UAE's compliance rating on the Financial Action Task Force's Recommendation 29 is an evident of the great contribution made by the UAEFIU in 2023 in the UAE's compliance with the FATF standards, resulting in the removal from FATF's list 'jurisdiction under increased monitoring' in February 2024.

From a domestic perspective, stakeholder outreach in 2023 remained a key priority for UAEFIU, both to raise awareness of ML/TF/PF risks in society, and to ensure regulated entities and supervisory authorities



H.E. Khaled Mohamed Balama

Chairman, NAMLCFTC

fulfil their reporting obligations with respect to Suspicious Activity Reports and Suspicious Transaction Reports. This is evidenced by the record number of entities registered with the UAEFIU's reporting system (2023: 18,899), in addition to the volume of SARs and STRs submitted (2023: 53,470).

These inputs have supported the increased distribution of financial intelligence by UAEFIU, with 246 cases (2022: 212) disseminated to law enforcement agencies, state security and public prosecution for further action during the year. Ultimately, these disseminated cases play an important role in the issuance of freeze orders, a key legal power within the UAE's toolkit to address suspected ML/TF/PF. In 2023 alone, such orders covered AED400m of funds domiciled in the UAE, and is a testament to how the UAEFIU's proactive approach helps uphold the integrity of the financial system.

Refinements to the way in which the UAEFIU undertakes engagement with key UAE stakeholders has allowed its key messages to reach a much wider audience in recent years, totalling 882 entities in 2023 alone. At an operational level, the UAEFIU further expanded its network with counterpart FIUs in other jurisdictions, signing an additional 5 Memoranda of Understandings (MoUs) in 2023 to bring the total to 68.

These MoUs provide a basis for the information exchange that is so critical to proactive financial crime detection, and have enabled Outward Requests for Information¹ and Outward Spontaneous Disseminations to rise to 687 in 2023 (2022: 477). In particular, I would like to highlight the notable reduction in the UAEFIU's average turnaround time for completion of Inward Requests For Information² to 41 days (2022: 58 days). This serves as a clear example of the continuing enhancements to the efficiency of the UAEFIU's business-as-usual activity.

To support this commitment, the UAEFIU continued to actively engage in international co-operation during the year. At a strategic level, this was exemplified by the UAEFIU's hosting of the 29th Annual Egmont Group Plenary in July 2023, which was co-chaired by the Chief of the UAEFIU, Ali Faisal Ba'Alawi.

The UAEFIU's membership and participation in the Egmont Group is a strategic priority, given its role in connecting 177 national Financial Intelligence Units across the world. Therefore, it was an honour for the UAE to welcome over 500 delegates to Abu Dhabi to discuss developments in cross-border collaboration and information exchange.

Finally, the UAEFIU's role should never be overlooked to combating the harm of the financial crimes to the prosperity of the economy, and the safety of society and individuals, at both the UAE and global level. We would like to thank our wise leadership in continuing to protect against these threats with the support of the systems, and to strengthening the country's position as a leading finance and trade hub, as well as the UAEFIU to adapt to an evolving financial crime landscape.

1- Sent by the UAEFIU to counterpart FIU's in other jurisdictions

2- Received by the UAEFIU from counterpart FIU's in other jurisdictions

MESSAGE FROM THE CHIEF OF THE UAEFIU

“ The UAEFIU has strengthened its role as a critical player in the global financial security landscape, enhancing our analytical capabilities and expanding collaboration with domestic and international partners. ”



Ali Faisal Ba'Alawi

Chief of the UAEFIU

| A Year Marked by Significant Advancements

The past year has underscored the critical role we play in ensuring the integrity of our financial system. In 2023, we faced challenges yet also celebrated significant milestones. As we reflect on the UAE Financial Intelligence Unit's (UAEFIU) accomplishments in 2023, we recognize a year marked by significant advancements in our commitment to combatting money laundering and the financing of terrorism.

The UAEFIU has strengthened its role as a critical player in the global financial security landscape, enhancing our analytical capabilities and expanding collaboration with domestic and international partners.

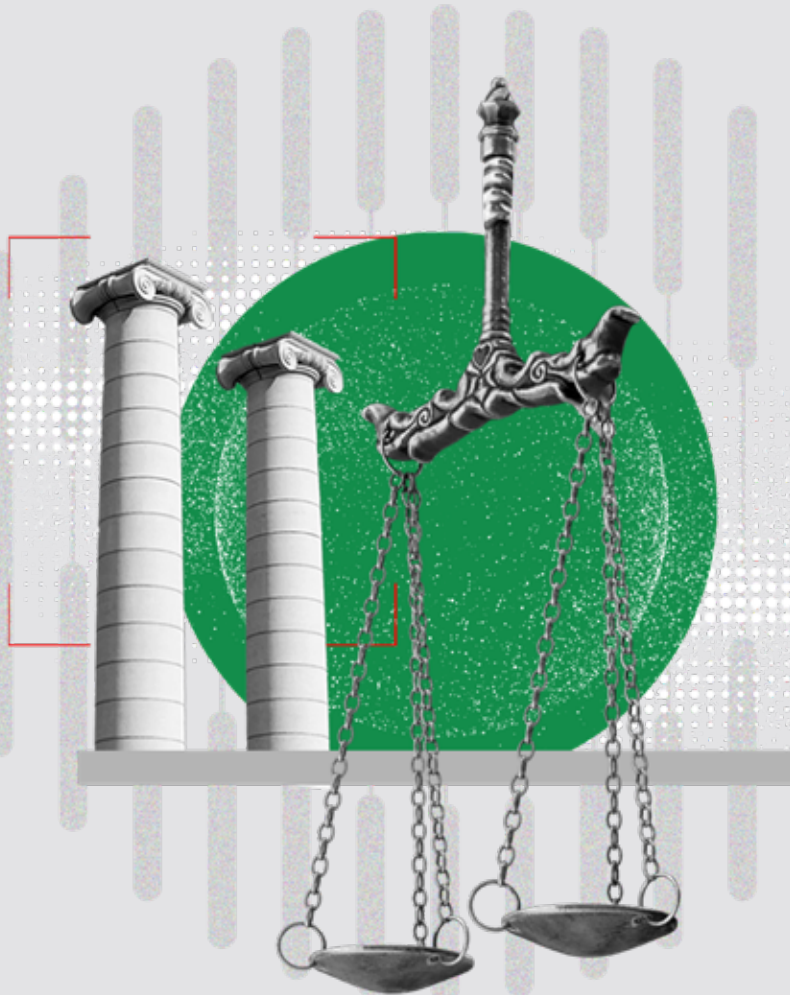
In 2023, we continued refining our data analysis techniques, resulting in improved detection and reporting mechanisms for suspicious criminal activities. We also continued building on our strong collaboration with our domestic partners, which resulted in a better alignment of priorities and feedback. Our outreach initiatives have fostered greater awareness among financial institutions, enabling them to recognize better and mitigate risks associated with illicit financial flows and further strengthen public-private partnerships.

Furthermore, our commitment to aligning with international standards has been unwavering. We actively participated in global forums, sharing insights and best practices to bolster collective efforts against financial crime. We also witnessed the impact of our increased engagement with international stakeholders in building trust, better understanding, and improved proactiveness in taking action against illicit actors.

As we move forward, we remain dedicated to our mission, ensuring sustainability and striving to enhance the integrity of the UAE's financial system.

Together with our stakeholders, we look forward to building a more resilient and effective AML/CFT system in the years to come.

I will take this opportunity to thank all members of the UAEFIU for their dedication and unwavering commitment during the year and our stakeholders for all their support in achieving our common goals.



01

A RESILIENT AML/ CFT INSTITUTIONAL FRAMEWORK

A RESILIENT AML/CFT INSTITUTIONAL FRAMEWORK BOLSTERING ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING EFFORTS

Since the national legislation of 2002, the National Anti-Money Laundering and Combating Financing of Terrorism and Financing of Illegal Organizations Committee (NAMLCFTC) was established as the primary body in the UAE for policymaking, adopting required national policies and regulations, and all other aspects relevant to anti-money laundering (AML) and combating the financing of terrorism (CFT).

Article (11) of the Federal Decree-Law No. (20) of 2018



1.

A committee chaired by the Governor, called "National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations", shall be established by virtue of the provisions of this Decree-Law.

Article (12) of the Federal Decree-Law No. (20) of 2018 : Competencies over



1.

Preparing and developing a national strategy to combat crime and proposing related regulations, policies and procedures in coordination with the competent authorities, and monitoring their implementation.



2.

Determining and assessing the risks of the crime on the national level.



3.

Coordinating with the relevant authorities and referring to related international sources of information in order to identify high-risk countries in relation to money laundering and financing of terrorism and instructing the supervisory authorities to ensure the adherence to the required due diligence procedures by financial institutions, designated nonfinancial businesses and professions, virtual asset service providers, and non-profit organisations which are under their supervision.



4.

Facilitating the exchange of information and coordination among the various bodies represented therein.



5.

Collecting and analysing statistics and other information provided by the Competent Authorities to assess the effectiveness of their Regulations on combating Money laundering, Terrorism financing and financing of illegal organizations.



6.

Representing the State in international forums related to Money laundering.



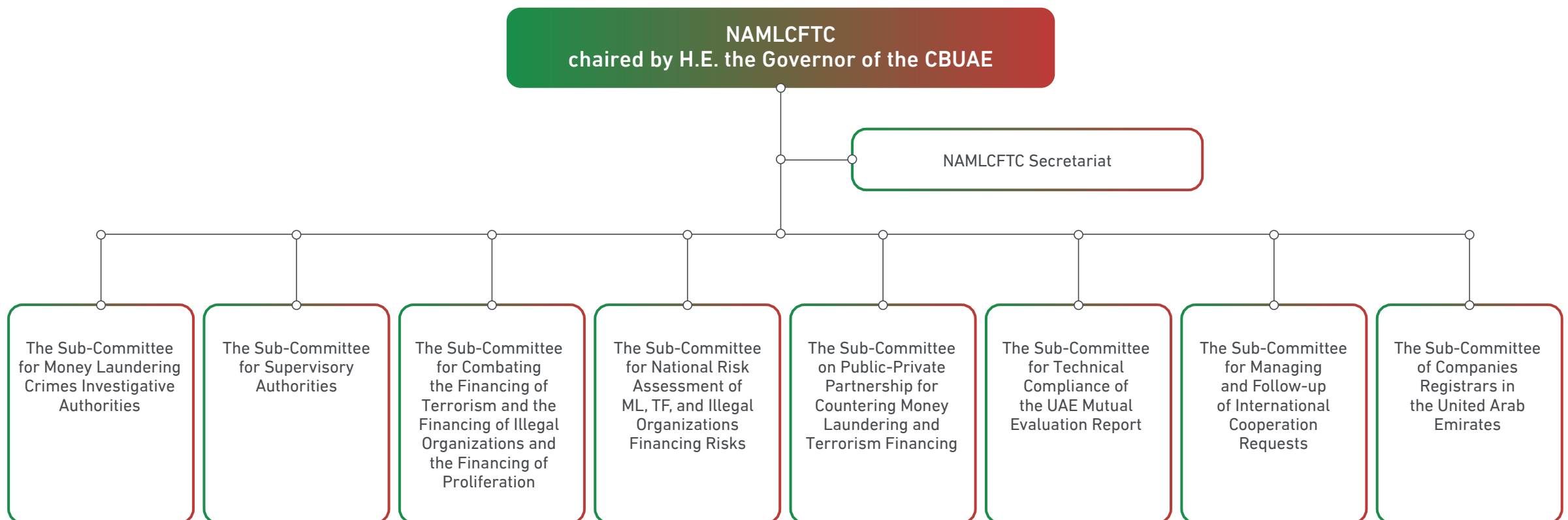
7.

Proposing the regulation covering the work of the Committee, and submitting it to the Minister for approval.

A RESILIENT AML/CFT INSTITUTIONAL FRAMEWORK

BOLSTERING ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING EFFORTS

The NAMLCFTC is chaired by H.E. the Governor of the Central Bank of the UAE (CBUAE) and has 44 permanent members from 32 federal and local competent government authorities, including the UAEFIU. Furthermore, the NAMLCFTC established eight subcommittees comprising members from all the national concerned competent authorities of the AML/CFT regime. The UAEFIU is an active member of the NAMLCFTC and its eight subcommittees.



A RESILIENT AML/CFT INSTITUTIONAL FRAMEWORK

BOLSTERING ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING EFFORTS

In 2020, the UAE Cabinet established the Higher Committee Overseeing the National Strategy on AML/CFT (the Higher Committee), chaired by H.H. Sheikh Abdullah Bin Zayed Al Nahyan, Minister of Foreign Affairs of the UAE, and membership of different ministerial level members from the concerned competent authorities.



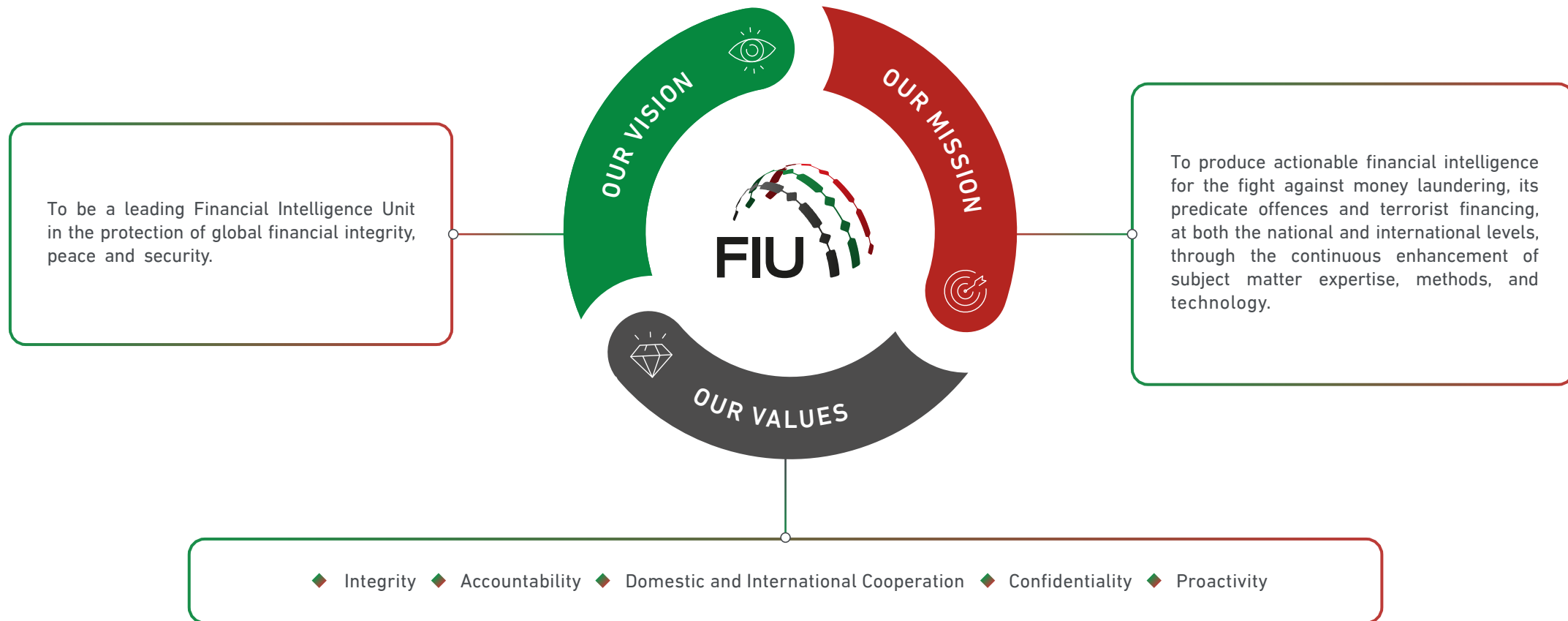


02

ORGANIZATIONAL OVERVIEW

ORGANIZATIONAL OVERVIEW

UAEFIU MISSION AND MANDATE



Our Legal Mandate

The UAEFIU has witnessed different institutional changes over time to keep pace with criminal schemes and international standards updated against financial crime. In early 1998, the Central Bank of the UAE (CBUAE) established a special unit to investigate fraud and suspicious transactions, which was developed into the Anti-Money Laundering and Suspicious Cases Unit (AMLSCU) in 2002. At the end of 2018, further significant changes were shaped by the Federal Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations, and its associated Cabinet Decision No. (10) of 2019,³ in addition to Federal Decree Law No. (26) of 2021 to amend certain provisions of Federal Decree Law No. (20) of 2018. With said legal framework, the unit was renamed the Financial Intelligence Unit (FIU).

3- Amended by Cabinet Resolution No. (24) of 2022

ORGANIZATIONAL OVERVIEW

UAEFIU MISSION AND MANDATE

For pursuing its mandate, the UAEFIU has the legal competence over the following:

“ The UAEFIU independently operates as a national center that exclusively receives suspicious transaction and activity reports from regulated entities for analysis and referral to the competent authorities ”

Article (9) of Federal Decree-Law No. (20) of 2018



Reporting and receiving suspicious transactions and activities

Requesting financial institutions and designated nonfinancial businesses and professions, virtual asset service providers and the competent authorities to submit any information or further documentation related to received reports and information and other information deemed necessary for FIU to perform its duties on schedule and in the form determined by the Unit.



International information exchange

Exchanging information with its counterparts in other countries, with respect to Suspicious Transactions Reports (STR) or any other information to which the FIU has exclusive access or is the exclusive recipient, whether directly or indirectly, according to international agreements to which the State is a party or bilateral agreements signed by the FIU with its counterparts governing bilateral cooperation or conditional upon reciprocity.

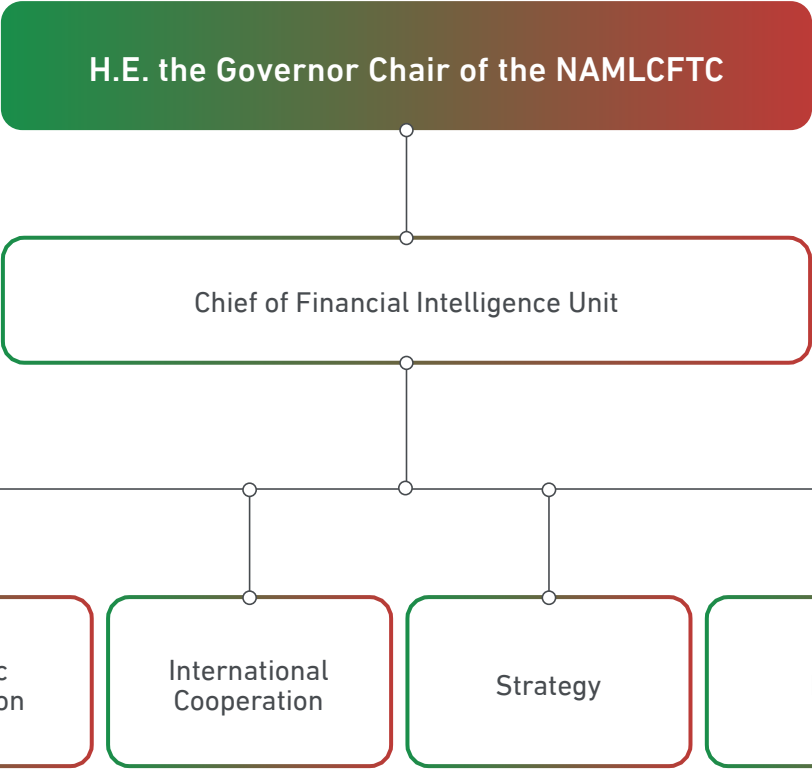


Data protection and security

Establishing a database or a special register to record all available information and to implement data privacy and data security procedures to protect this information including procedures for handling, archiving transferring and accessing the data, and make sure that access to its premises, its database and its technology systems is restricted.

ORGANIZATIONAL OVERVIEW

UAEFIU ORGANIZATIONAL STRUCTURE





ORGANIZATIONAL OVERVIEW

A STRONG WORKFORCE AGAINST FINANCIAL CRIMES

| Strengthening human capital to address complex threats

The UAEFIU human capital comprises dedicated specialists who excel in a wide range of skills and expertise necessary to combat financial crime domestically and internationally. Our experience ranges from leaders who previously served in different sectors, including banking and corporate business, supervisory and regulatory authorities, and law enforcement, to auditors, accountants, legal professionals, data scientists, academic researchers, and fresh graduate elites.



29

UAEFIU Human Capital capacity in 2020



76

UAEFIU Human Capital capacity in 2023

“ During 2022 and 2023 the UAEFIU staff members attended 160 training programs and sessions relevant to financial crime ”



This represents a

162% increase in 4 years

From 2020, the UAEFIU's human resource capacity witnessed considerable development that enabled us to achieve national and international strategic and operational goals efficiently. Additional sections were added to the UAEFIU structure in 2021 and the headcount grew from 29 members in 2020 to 76 in 2023 representing a 162% increase over the four years.

In terms of capability and capacity building, the UAEFIU human resources are competent and certified in financial crime prevention. The analysts are regularly updated with new developments in money laundering (ML) and terrorist financing (TF), as well as new trends and methods, and trained in applying best practices and required operational approaches against financial crime.

Over the past two years of 2022 and 2023, the UAEFIU staff members attended 160 training programs and sessions in different high-risk topics relevant to financial crime. In 2023, the UAEFIU members were trained through 67 well-crafted training programs designed to meet the staff's operational needs.

ORGANIZATIONAL OVERVIEW

UAEFIU'S FUNCTIONS

Core areas that define our impact

The UAEFIU organizational chart comprises eight functions in addition to the Chief of Financial Intelligence Unit (CoFIU) Office, as follows:



Strategy

Crafting and developing a coherent strategy in line with national action plan and international best practices is crucial to the success of the UAEFIU. The UAEFIU operational plan ensures the flow of its daily functions according to the UAEFIU mission and vision, as well as the national AML/CFT/CPF strategy. Within this context, the UAEFIU KPIs are designed to guide the UAEFIU operations and ensure overall efficiency and sustainability of outcome.



Policy

The policy function formulates, implements, and continuously evaluates policies that ensure the UAEFIU operates according to national and international legal frameworks, standards, and best practices. This function also encompasses the development of guidelines and procedures for financial crime detection, reporting, and analysis, ensuring that all activities align with the broader objectives of combating money laundering, terrorist financing, and other financial crimes. Furthermore, it is pivotal in fostering collaboration with domestic and international stakeholders, enhancing the capacity to respond to emerging risks and evolving regulatory requirements.

OPERATIONAL ANALYSIS



Reporting and Data Collection

UAEFIU is the designated receiver of reports; the FIU receive Suspicious Transaction Reports (STRs), Suspicious Activity Reports (SARs), and other report types as mandated by the UAE's laws and regulations from reporting entities, including financial institutions (FIs), designated non-financial businesses and professions (DNFBPs) and virtual asset service providers (VASPs). Simultaneously, UAEFIU collects additional information from the broadest range of national and international sources.



Analyzing Reports

UAEFIU analyzes the reports and other information and data gathered to identify possible illicit activity in the financial, DNFBP, and VASP sectors, and the economy in general, used by potentially nefarious actors in their attempt to launder illicit proceeds, finance terrorism, and overall, fund their unlawful activities. This is done by developing actionable intelligence in the form of activity patterns, targets, criminal ties, relationships, networks, leads, criminal profiles, and the tracing of funds.



Intelligence Dissemination

The operational intelligence is disseminated, including recommendations to freeze accounts, when needed, to the concerned law enforcement, competent authorities, and international counterparts, for further action.

ORGANIZATIONAL OVERVIEW

UAEFIU'S FUNCTIONS

| Research and Strategic Analysis

The primary function of strategic analysis is to utilize all available information with the UAEFIU databases and obtainable data from competent authorities to identify ML and TF-related trends and patterns. This information is then developed into typology reports, statistical reviews, whitepapers, and periodic studies related to financial crime within the UAE and abroad when warranted.

The strategic analysis ultimately aims to develop the UAEFIU stakeholders' understanding from public and private sectors, domestically and internationally, of the primary risk drivers of financial crime within the UAE and underlines ML and TF-related threats and vulnerabilities. With said aim in mind, the research and strategic analysis function develops the necessary risk indicators relevant to high-risk typologies in order to guide reporting entities in identifying and monitoring suspicious transactions, activities, and drawing their risk-based approach.

| Domestic Cooperation

This function is mainly devoted to responding to competent authorities' requests and intakes further reactive dissemination of information and intelligence as well as provides the necessary technical reports for law enforcement investigations. It also serves as the focal point for engagement between the UAEFIU and all domestic stakeholders for combating ML/TF in the UAE, including Public Prosecution (PP), Law Enforcement Authorities (LEAs), State Security (SS), and supervisory authorities for the exchange of information and intelligence. As such, this function is often associated with the signatory of domestic memorandums of understanding (MOUs) between the UAEFIU and other competent authorities.

| International Cooperation

The primary function of international cooperation is to engage in and facilitate collaboration with the UAEFIU international partners, including the UAEFIU's membership with the Egmont Group and members and other international bodies and groups. International cooperation is a core function for receiving and analyzing incoming international requests for information from the UAEFIU international partners, as well as disseminating information and intelligence relevant to combating ML, TF, Proliferation Financing (PF), and associated predicate offences. Based on said intelligence, preventive measures are introduced through the UAEFIU recommendations and requests for freezing accounts.

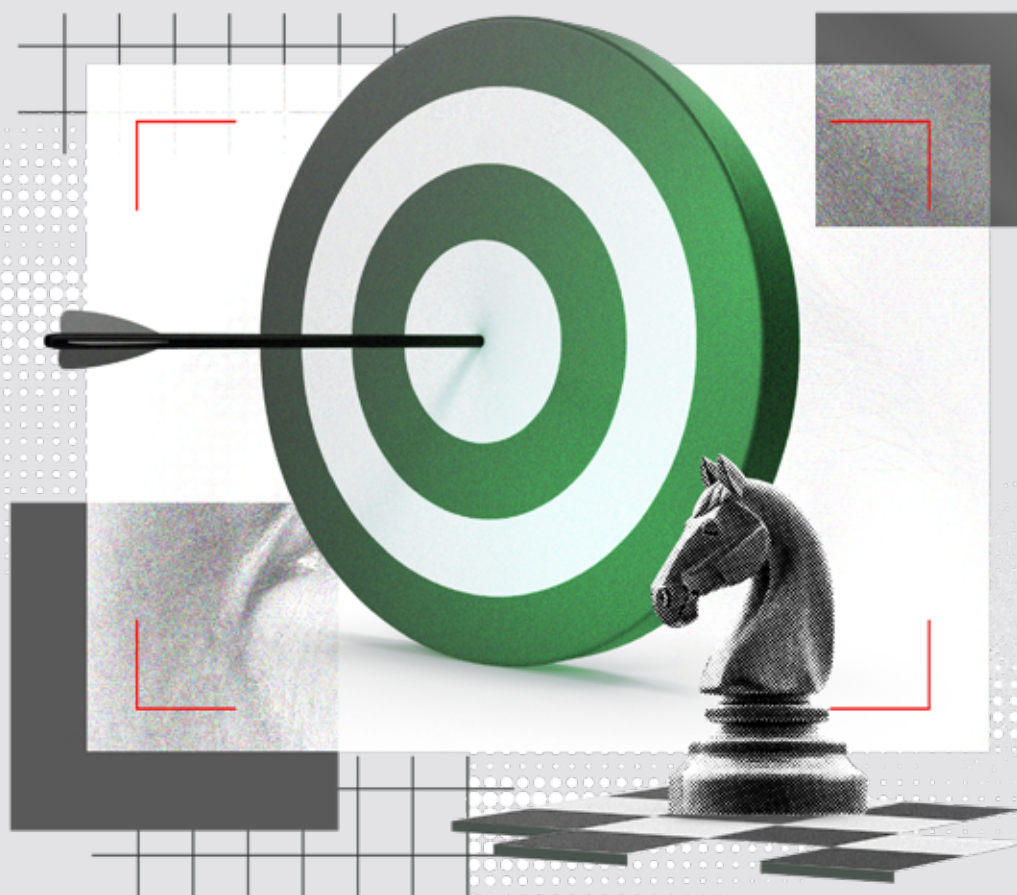
“ Domestic and international cooperation serve as the focal point for engagement between the UAEFIU and all stakeholders for combating ML/TF in the UAE ”

| Outreach

The outreach function handles engagements with reporting entities and supervisory authorities, offering recommendations on best practices to enhance compliance with AML/CFT laws and regulations. UAEFIU also provides feedback to reporting entities in order to promote an effective and interactive reporting process. The UAEFIU through this function essentially collaborates with local and international partners to organize and develop training programs related to AML/CFT and financial crimes and raise awareness of ML and TF risks.

| System Infrastructure

This function manages UAEFIU-owned systems and applications, database structures and system setup/configurations, and IT projects, among other day-to-day activities. The system infrastructure has a vital role in developing UAEFIU's digital transformation, adopting new technologies, analytical software, and solutions necessary for the UAEFIU's core functions.



03

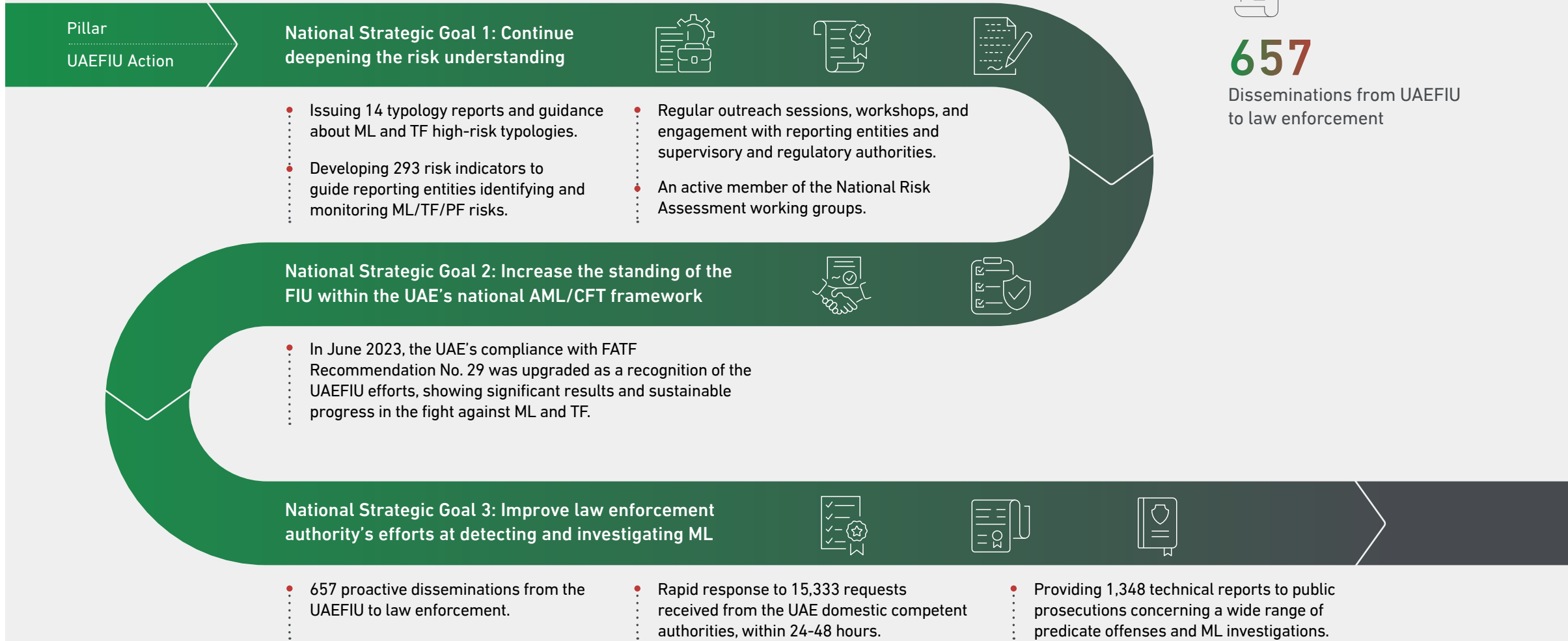
PROGRESS DELIVERED ON 2020-2023 AML/ CFT NATIONAL STRATEGY

PROGRESS DELIVERED ON 2020-2023 AML/CFT NATIONAL STRATEGY

MILESTONES ACHIEVED IN THE FIGHT AGAINST FINANCIAL CRIMES

The UAEFIU's strategy and operational plan over the past four years significantly contributed to different pillars of the 2020-2023 National Strategy for Combating Money Laundering and Terrorism Financing. This is in addition to promoting the UAE's compliance with international standards and best practices.

A glimpse into relevant National Strategy pillars and the UAEFIU action from 2020-2023



14

Typology ML/TF reports and guidance issued



657

Disseminations from UAEFIU to law enforcement

PROGRESS DELIVERED ON 2020-2023 AML/CFT NATIONAL STRATEGY

MILESTONES ACHIEVED IN THE FIGHT AGAINST FINANCIAL CRIMES



Estimated amount frozen based on UAEFIU analysis in 2022

AED 452,529,528



Associated with 200% additional freeze orders in 2023

AED 399,286,370

Pillar
UAEFIU Action

National Strategic Goal 4: Use provisional and confiscation measures more frequently and effectively



- The UAEFIU actively utilized its function in issuing freeze orders by H.E. the Governor of Central Bank of United Arab Emirates based on received suspicious reports from Reporting Entities.

- AED 452,529,528 was the estimated amount frozen based on UAEFIU analysis in 2022 and **AED 399,286,370 in 2023⁴** associated with 200% increase in number of freeze orders.

National Strategic Goal 10: Strengthen the level of assistance UAE provides to its International Partners



- Exchanged 5,622 intelligence with the UAE's strategic international partners reactively and spontaneously in 2023.
- 68 MOUs signed with counterpart FIUs as of December 2023.

- Joint operational team with strategic partners on identified subjects.
- Hosting the Egmont Group Plenary in 2023.

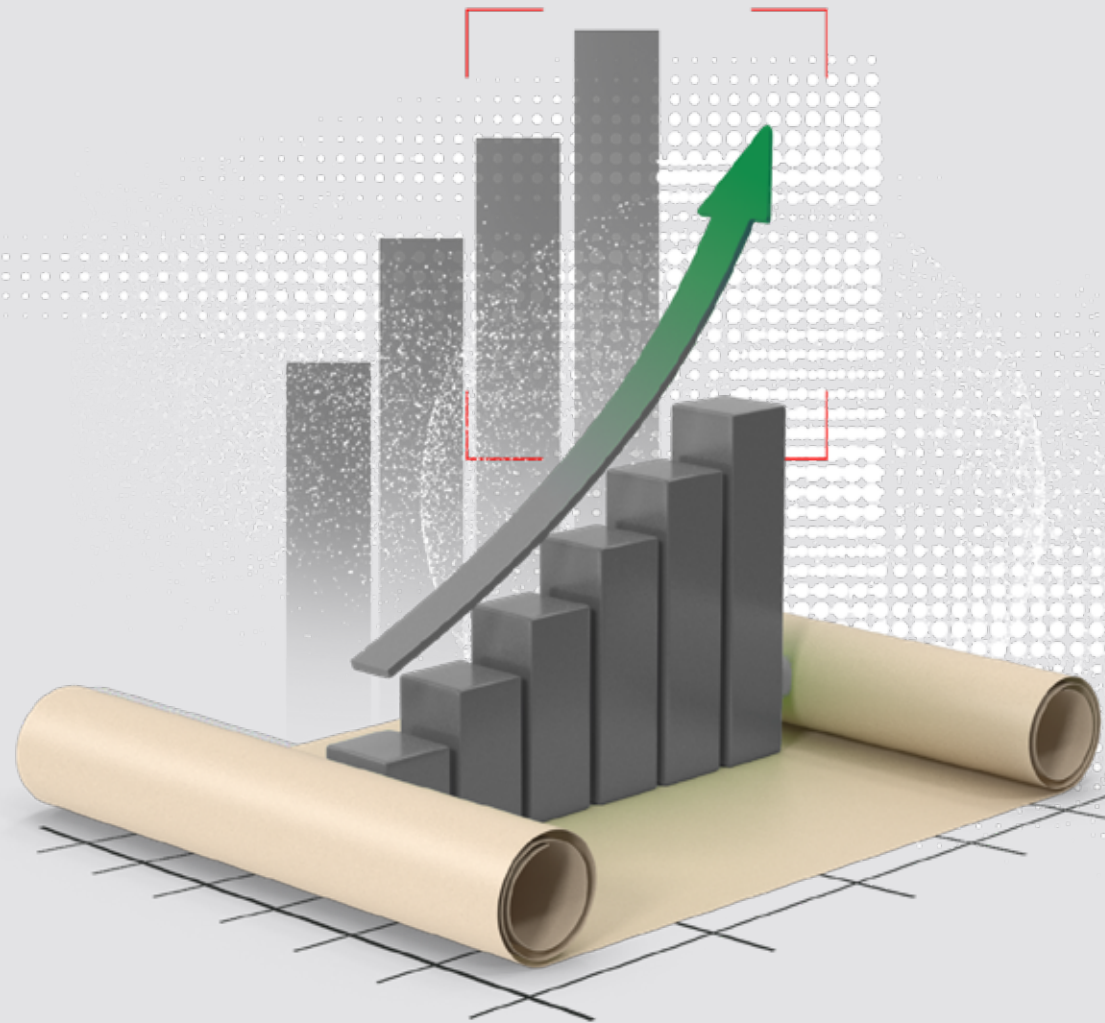
- Contributor to the Egmont Center of Excellence and Leadership (ECOFEL) established to assist Financial Intelligence Units in different technical and operational topics relevant to AML/CFT.

National Strategic Goal 11: Continue to effectively investigate, prosecute, and convict TF offences



- 79 cases were disseminated to law enforcement from the UAEFIU, and 125 intelligence insights were exchanged with international partners relevant to TF.

4- Said amounts may upsurge or decrease for different reasons.



04

OPERATIONS AND COLLABORATIONS

OPERATIONS AND COLLABORATIONS

OPERATIONAL ANALYSIS

Significant growth in registered entities and STRS/SARS filings to goAML

Regulated entities are obligated to file different types of reports, including STRs/SARs, to the UAEFIU, via the UAEFIU reporting system (goAML).

The number of reporting entities significantly escalated over the past few years to meet the regulatory obligation required from financial institutions and DNFBP and VASP sectors. As of December 2023, the number of reporting entities registered with the goAML reached 18,899, expanding from 1,524 in 2020.

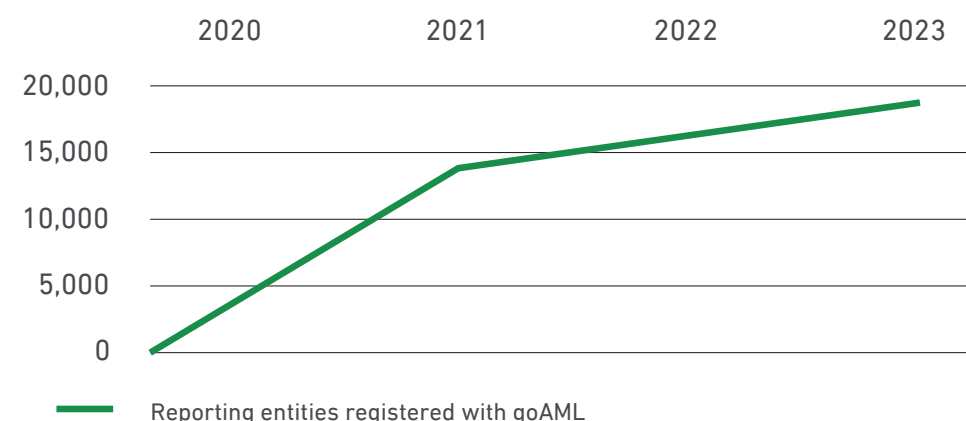
With such growth in the number of reporting entities, STRs and SARs also considerably increased from 16,621 in 2020 to 53,470 in 2023, suggesting dynamic engagement and compliance with the AML/CFT requirements.



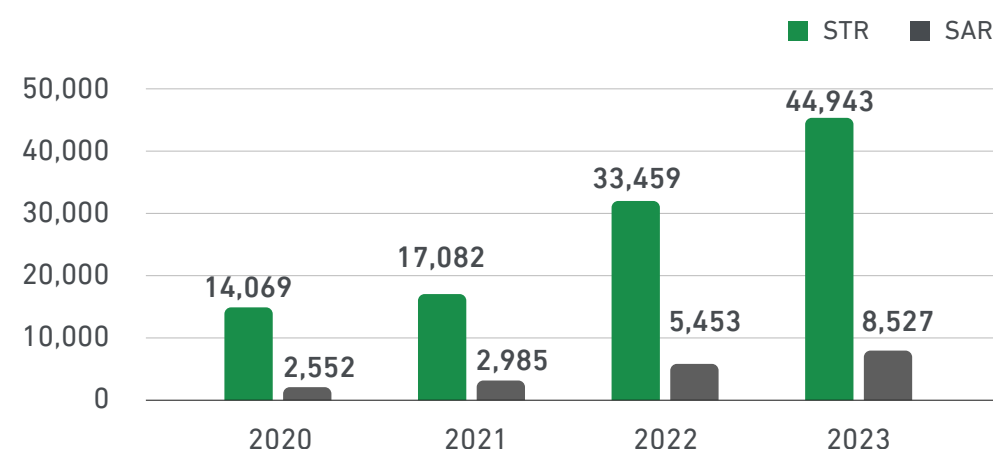
18,899

goAML-registered reporting entities in 2023

Reporting entities registered with goAML



Number of STRs and SARs 2020 - 2023



The engagement of reporting entities with the UAEFIU reporting system started to witness a significant increase from the year 2021 due to the new types of reports added by the UAEFIU and including new reporting entities, such as VASPs.⁵

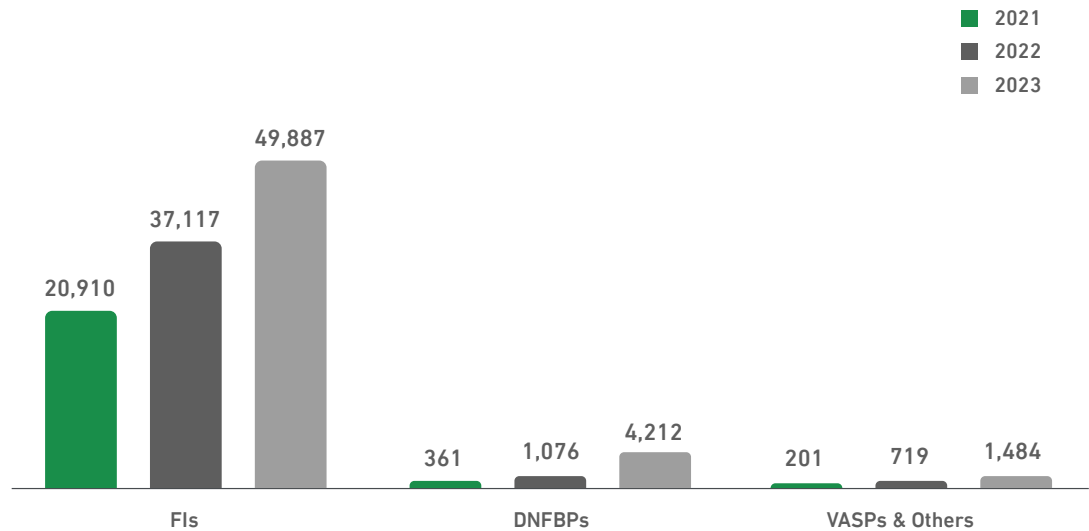
5- Based on Federal Decree-Law No. (26) of 2021.

OPERATIONS AND COLLABORATIONS

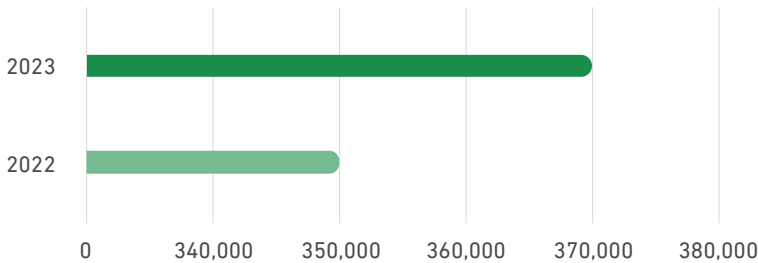
OPERATIONAL ANALYSIS

In coordination with the supervisory authorities of DNFBP sectors, in 2021, the UAEFIU created two types of threshold transaction reports: DPMSR for dealers in precious metals and stones (cash and international wire transfer) transactions and REAR for real estate (cash and crypto) transactions. Please revert to **Annex 1** for additional information on report types.

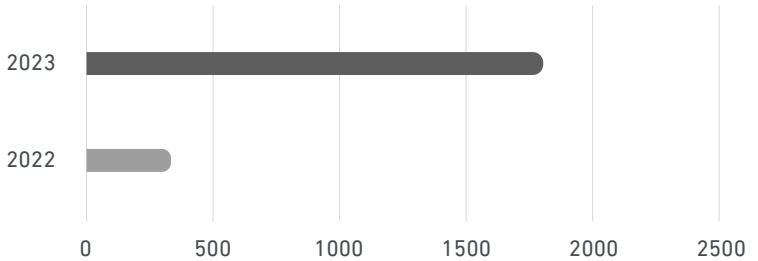
Number of suspicious reports filed by reporting entities⁶



Dealers in Precious Metals and Stones Reports (DPMSRs)



Real Estate Activity Reports (REARs)



6- Suspicious reports may include STRs, SARs, RFI, RFIT, PNMR, FFR, HRC, and HRCA, noting that new types of reports were added over the years.

OPERATIONS AND COLLABORATIONS

OPERATIONAL ANALYSIS

Based on the UAEFIU's risk-based approach and applying a systematic triage process for prioritization, analysis of received suspicious reports would be developed into a case referral to law enforcement, noting that a case often includes intelligence from multiple suspicious reports.

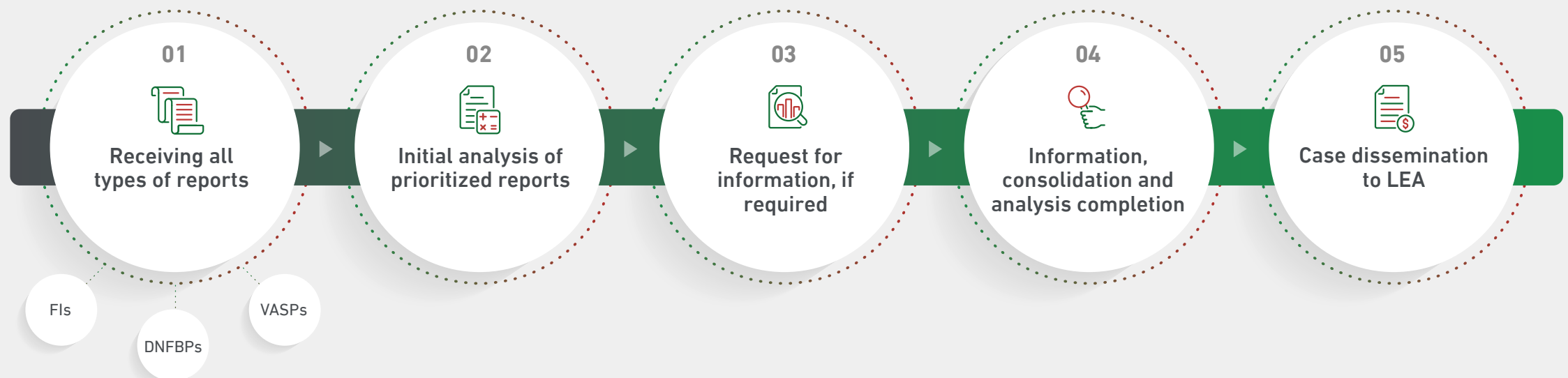
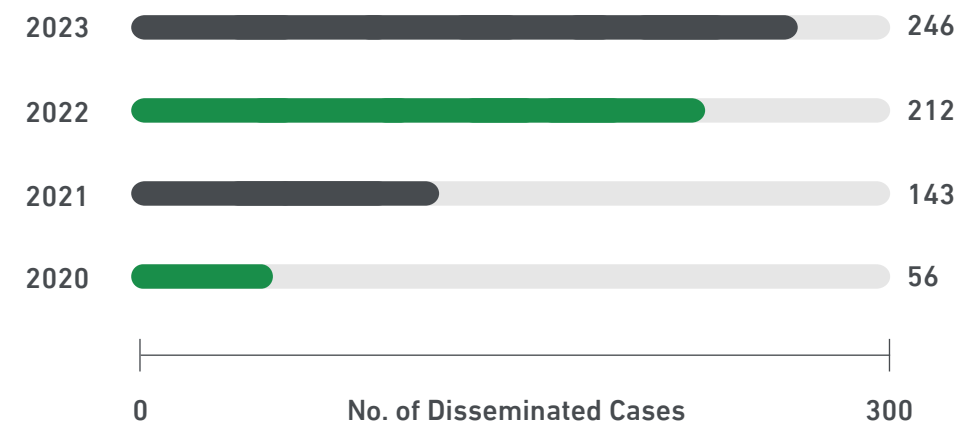
The number of disseminated cases to competent authorities (i.e. LEA, SS, PP) significantly increased from 56 cases in 2020 to 246 in 2023, representing a 339% increase.

Over the four-year period, 657 proactive disseminations associated with 7,145 suspicious reports were disseminated.



246








Cases disseminated in 2023



OPERATIONS AND COLLABORATIONS

OPERATIONAL ANALYSIS

Top disseminated cases by typologies or possible predicate offence

Associated Typology/ Possible Predicate Offence	2020	2021	2022	2023	Total
 Fraudulent transfer (domestic & international fraud recall)	37	37	30	38	142
 Professional money laundering or networks of third-party laundering	2	18	56	50	126
 Possible terrorist financing	1	12	12	48	73
 The laundering of proceeds in UAE from foreign predicate offences (including direct and indirect tax crimes)	7	26	13	24	70
 Trade-based money laundering	5	17	27	16	65
 Complex ML cases and/or businesses in higher risk sectors	1	10	26	16	53
 Laundering the proceeds of drug/human trafficking	1	3	27	20	51

OPERATIONS AND COLLABORATIONS RESEARCH AND STRATEGIC ANALYSIS

The strategic analysis function has a crucial role in understanding and mitigating financial crime risks at the institutional and national levels by identifying potential vulnerabilities and threats to enable the UAEFIU and its stakeholders to proactively address financial crime risks and prevent criminal schemes. Through this function, the UAEFIU suggests to policymakers, reporting entities, and supervisory and law enforcement authorities, different policy developments and recommendations underlying the required controlling measures to address and mitigate the identified risks.

Over the past three years, 2021-2023, the UAEFIU issued 14 strategic analysis reports to develop the understanding of the UAEFIU stakeholders of a wide range of criminal patterns and schemes.

Strategic analysis products developed 293 risk indicators to guide reporting entities in detecting and identifying suspicious transactions and activities relevant to financial crime.



293

Risk indicators developed

2021

The Abuse of Legal Entities in Money Laundering and Terrorist Financing

The Abuse of Non-Profit Organizations: Guidance for Reporting Entities

Strategic Analysis on Trade-Based Money Laundering

Strategic Analysis on Money Value Transfer Services (MVTs) and Registered Hawala Providers (RHP)

Strategic Analysis on Professional Money Laundering (PML) and Foreign Proceeds of Crimes

Strategic Analysis on Virtual Assets

2022

Fraud Crimes, Trends and Typologies

Strategic Analysis Report on Dealers in Precious Metals and Stones

Far East Typology Patterns and Schemes - White Paper

Statistical Review of UAE Remittance Reporting System (UAE RRS) and Federal Customs Authority Data

2023

The Abuse of Legal Persons and Arrangements in Illicit Activities

Designated Non-Financial Businesses and Professions - A Strategic Analysis Review

Patterns of Abusing Financial Institutions in Drug Trafficking and Laundering its Proceeds

Real Estate Money Laundering Typologies and Patterns

“ Over the past three years, 2021-2023, the UAEFIU issued 14 strategic analysis reports to develop the understanding of the UAEFIU stakeholders of a wide range of criminal patterns and schemes ”

OPERATIONS AND COLLABORATIONS RESEARCH AND STRATEGIC ANALYSIS

Strategic analysis draws its methodology within the context of the UAE National Risk Assessment (NRA) and Sectoral Risk Assessments (SRAs) and relies on analyzing large datasets to detect patterns, trends, and anomalies in transactions and activities that may indicate financial crime. This often involves a wide range of sources, available within the UAEFIU databases and obtainable from stakeholders, in addition to open source intelligence (OSINT).

All the UAEFIU's strategic analysis reports involved the examination of a sample of suspicious reports covering one previous year (as a minimum) or three previous years (as a maximum), depending on the topic methodology. The total examined samples from 2020-2023 included 6,729 suspicious reports received from different reporting entities and over 500 international intelligence reports. These are in addition to customs and remittances data, as well as cases referred from/to LEAs.



6,729

Suspicious reports from reporting entities



500+

International Intelligence reports examined

2021



102

Risk indicators

- 1,182 STRs/SARs
- 60 incoming RFIs and SDs
- 5 outgoing RFIs and SDs
- 5 cases referred to competent authorities
- 23,608 ingoing and outgoing cash declarations
- Inward/outward remittance data

2022



59

Risk indicators

- 1,580 STRs
- 139 SARs
- 327,424 DPMSRs
- 81 incoming RFIs and SDs
- 44 outgoing RFIs and SDs
- 105 cases referred to competent authorities
- 85,172 ingoing and outgoing cash declarations
- Inward/outward remittance data

2023



132

Risk indicators

- 3,246 STRs
- 582 SARs
- 80 HRCAs
- 976 REARs
- 280 incoming RFIs and SDs
- 80 outgoing RFIs and SDs
- 265 cases referred to competent authorities
- 129 cases referred by competent authorities involving 292 subjects
- 16,637 ingoing cash declarations
- 2,905 outgoing cash declarations

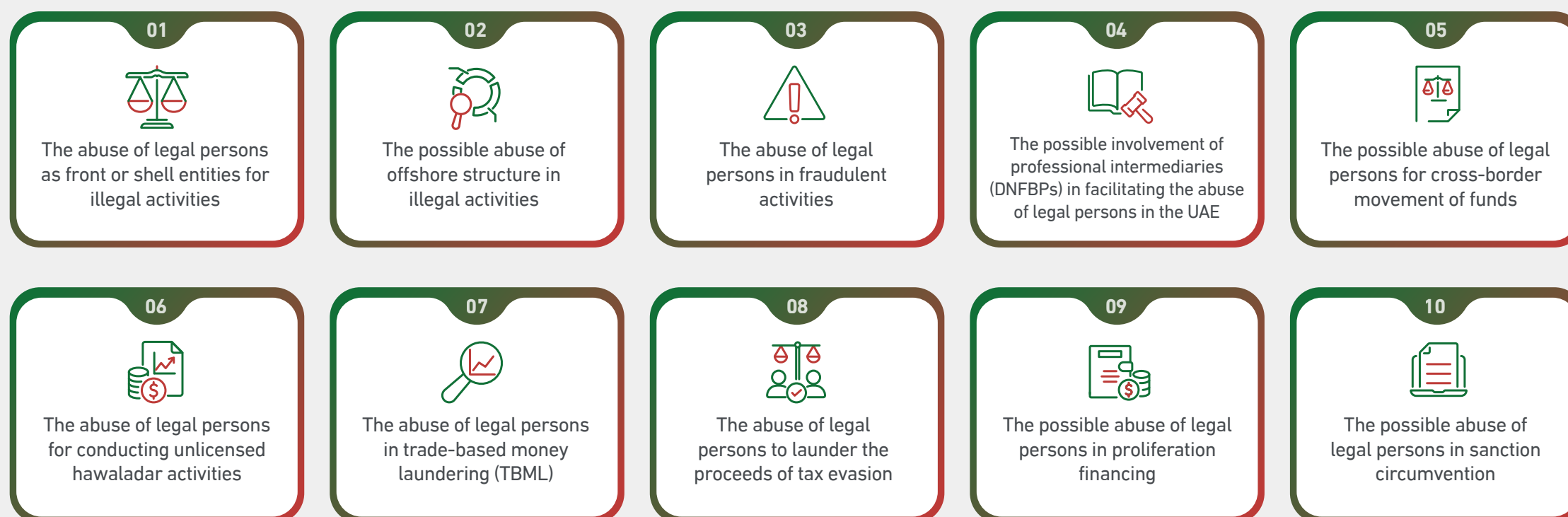
OPERATIONS AND COLLABORATIONS

2023 STRATEGIC ANALYSIS PRODUCTS HIGHLIGHTS

| Abuse of Legal Persons and Arrangements in Illicit Activities⁷

The UAEFIU draws different scenarios of typologies potentially associated with the abuse of legal persons and arrangements in the UAE for illicit purposes. Testing said scenarios using the UAEFIU's available and obtainable data affirmed the possibility of misusing local legal persons as a pass-through to route or layer unknown sources of funds.

| 10 specific techniques and methods were identified



7- Source: UAEFIU website at <https://www.uaefiu.gov.ae/en/more/knowledge-centre/publications/trends-typology-reports/the-abuse-of-legal-persons-and-arrangements-in-illicit-activities/>

OPERATIONS AND COLLABORATIONS

2023 STRATEGIC ANALYSIS PRODUCTS HIGHLIGHTS

Patterns of Abusing Financial Institutions in Drug Trafficking and Laundering its Proceeds⁸

According to the FATF's 4th round of Mutual Evaluations, two-thirds of countries have identified drug trafficking as a major predicate offence involving ML, followed by corruption, fraud, and tax crimes.⁹

The strategic analysis aimed to determine attributes and factors associated with the abuse of narcotics and psychotropic substances involving financial institutions. Essentially, the strategic analysis report outlined the most popular patterns and trends wherein financial institutions are being misused in moving illicitly traded narcotics. In addition, it attempted to identify ways of laundering drug trafficking proceeds in the UAE, including the possibility of integrating drug money with virtual assets and the real estate sector. The report also explored how financial institutions are being abused in the exponentially rising trend of utilizing social media platforms to traffic drugs in a larger market.

Six typologies identified along with their associated risk indicators, wherein risk mitigation measures are required

01



Abusing the banking sector in drug trafficking and money laundering

02



Abusing the money services businesses (MSBs) in drug trafficking and money laundering

03



Misusing legal persons in drug trafficking and money laundering

04



Employing trade-based money laundering (TBML) techniques in drug trafficking and laundering the proceeds of illicit drugs

05



Abusing the real estate sector in laundering the proceeds of drug trafficking

06



Potential misuse of virtual assets in drug trafficking and money laundering

8- Source: UAEFIU website at <https://www.uaefiu.gov.ae/en/more/knowledge-centre/publications/trends-typology-reports/patterns-of-abusing-financial-institutions-in-drug-trafficking-and-laundering-its-proceeds/>

9- FATF (2022) 'Report on the State of Effectiveness and Compliance with the FATF Standards'.

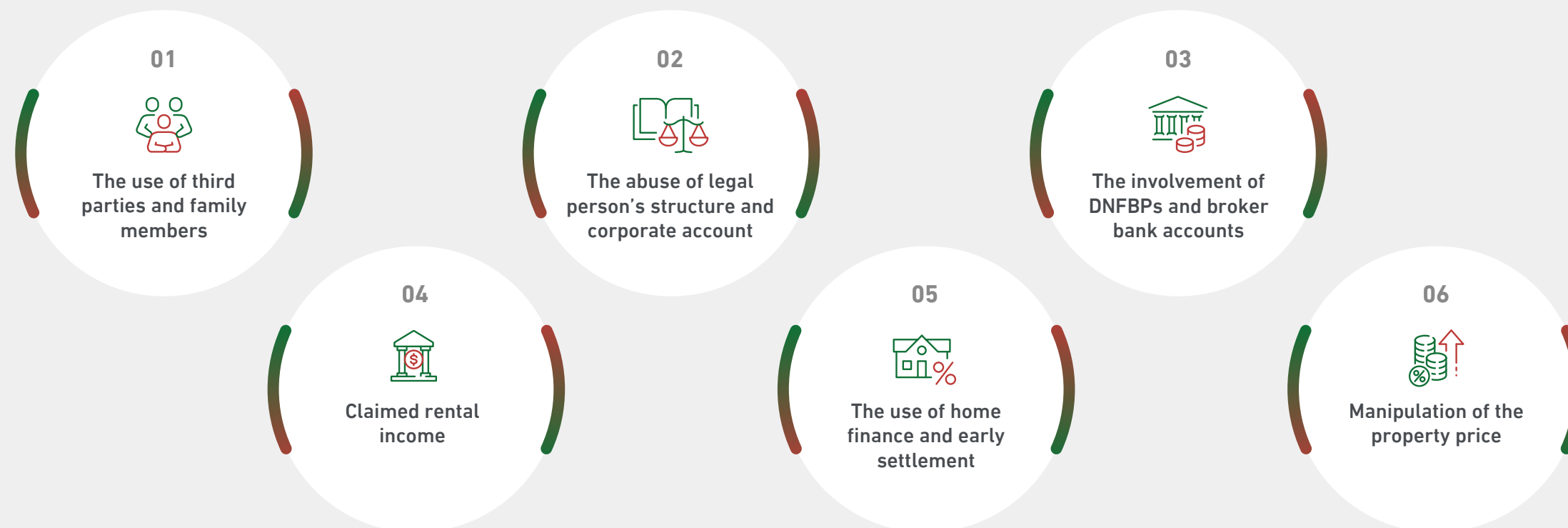
OPERATIONS AND COLLABORATIONS

2023 STRATEGIC ANALYSIS PRODUCTS HIGHLIGHTS

Real Estate Money Laundering Typologies and Patterns¹⁰

Due to the real estate nature as a source of high-value assets, it is observed to be an attractive method for criminal networks to launder their illicit proceeds. The UAEFIU examined the potential ML/TF risks associated with the real estate sector to develop the UAEFIU stakeholders' understanding of typologies potentially associated with misusing the real estate sector in laundering the proceeds of crime. This is in addition to providing more guidance to reporting entities involved in real estate transactions to enable them to detect and report suspicious transactions and activities related to the sector.

The UAEFIU identified six frequent patterns of how illicit funds are possibly integrated into the real estate sector in the UAE



10- Source: UAEFIU website at <https://www.uaefiu.gov.ae/en/more/knowledge-centre/publications/trends-typology-reports/real-estate-money-laundering/>

OPERATIONS AND COLLABORATIONS

2023 STRATEGIC ANALYSIS PRODUCTS HIGHLIGHTS

Designated Non-Financial Businesses and Professions (DNFBPs)¹¹

As mandated by the Federal Decree Law No. (20) of 2018, DNFBPs, similar to other reporting entities, are obliged to report any suspicious transactions and activities to the UAEFIU in a timely manner when there are suspicions, or reasonable grounds to suspect, that the proceeds are related to a crime, or to the attempt or intention to use funds or proceeds to commit, conceal, or benefit from a crime. Moreover, DNFBPs are required to identify, assess, and take preventative actions to mitigate any risks of being involved in facilitating the transfer of illicit proceeds for ML or TF purposes.

The UAEFIU conducted a strategic analysis of suspicious reports received from DNFBP sectors since their registration with the UAEFIU reporting system (goAML). The analysis aimed to assess DNFBPs' understanding and awareness of ML/TF risks and their reporting requirements. This is in addition to identifying potential patterns of how DNFBPs could be misused by their customers. For example, the analysis highlighted the possible misuse of DNFBPs in concealing the ultimate beneficial owner(s)' fund, facilitating the establishment of legal persons to be used as a conduit for the proceeds of crime or intermediaries to transactions in order to conceal the identities of their clients and their involvement in specific transactions.

“ The UAEFIU conducted a strategic analysis of suspicious reports received from DNFBP sectors since their registration with the UAEFIU reporting system (goAML) ”

Regulated DNFBPs



11- Available to Supervisory and Regulatory Authorities.

OPERATIONS AND COLLABORATIONS STRENGTHENING DOMESTIC COOPERATION

Unified efforts to identify and eradicate criminal networks throughout the country

Financial crime does not only transcend borders but also involves multiple sectors and jurisdictions within one country to add further layers and complexity in tracing the origin of illicit proceeds. Therefore, domestic cooperation among competent authorities has a vital role in ensuring comprehensive monitoring of financial crime risks and constructing a united front against criminal networks through the country's harmonized enforcement approaches and procedures. The exchange of accurate information and sharing of intelligence domestically in a timely manner plays a crucial role in achieving such an aim.

To foster the sharing of information and intelligence at the national level, the UAEFIU signed different MOUs with domestic partners from competent authorities over the past years, including: Three MOUs in 2023 with Abu Dhabi Global Market (ADGM), Dubai Financial Services Authority (DFSA), and The Executive Office for Control and Non-Proliferation (EOCN).



▲ Meeting between the FIU team and authorities

“ Three MOUs in 2023 with Abu Dhabi Global Market (ADGM), Dubai Financial Services Authority (DFSA), and The Executive Office for Control and Non-Proliferation (EOCN) ”

OPERATIONS AND COLLABORATIONS

STRENGTHENING DOMESTIC COOPERATION

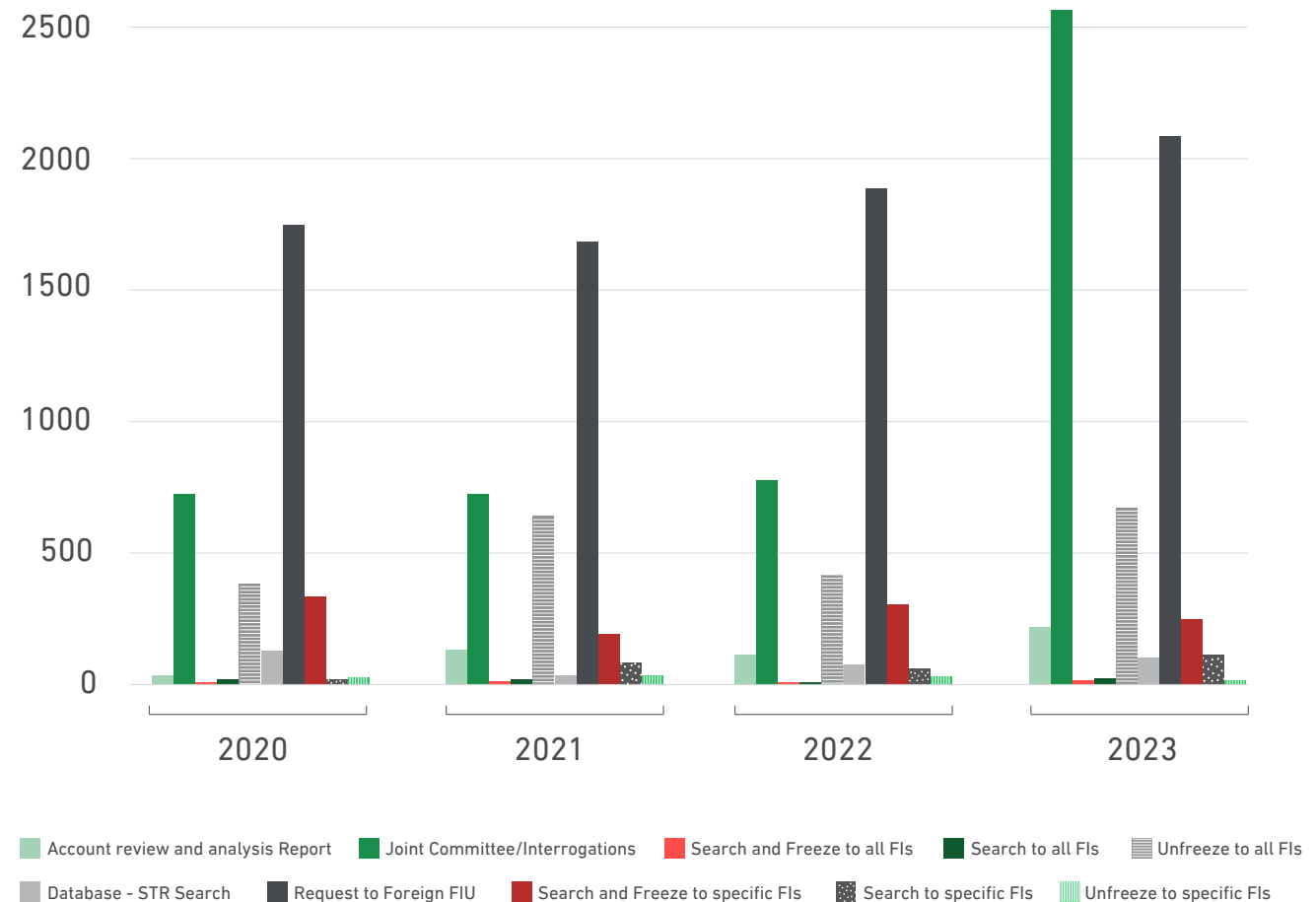
Integrated Enquiry Management System

Furthermore, the UAEFIU established a robust approach at the national level through its Integrated Enquiry Management System (IEMS) to facilitate communication among competent authorities and processing of requests for information and intelligence sharing between supervisory authorities, law enforcement, and judiciary authorities, regulated entities, and the UAEFIU.

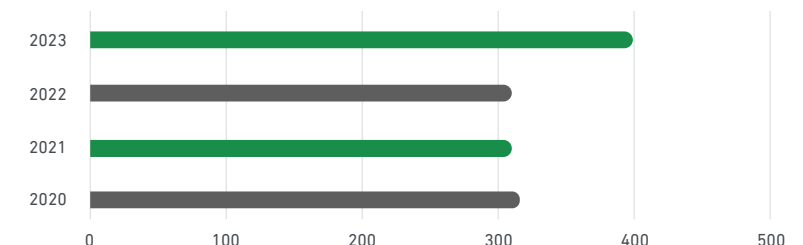
Over the past four years, the UAEFIU processed a total of 15,333 requests received from domestic competent authorities, including PP, LEAs, and supervisory authorities. In 2023 alone, the number of processed requests escalated to 4,608 from 3,742 in the previous year. The majority of these requests required information from all financial institutions in the UAE about the subjects of investigation. Due to the importance of the required information to ongoing investigations, the UAEFIU processes received requests within 24-48 hours.

Moreover, the UAEFIU provides public prosecutions across the UAE with comprehensive technical reports that further support ongoing cases, underlying when freezing of assets is recommended. Over the years 2020-2023, the UAEFIU provided 1,348 technical reports concerning a wide range of predicate offences and ML investigations. In 2023 alone, the number of technical reports grew to 398 from 312 in the previous year, representing 28% additional comprehensive reports.

Received Requests from LEAs by type



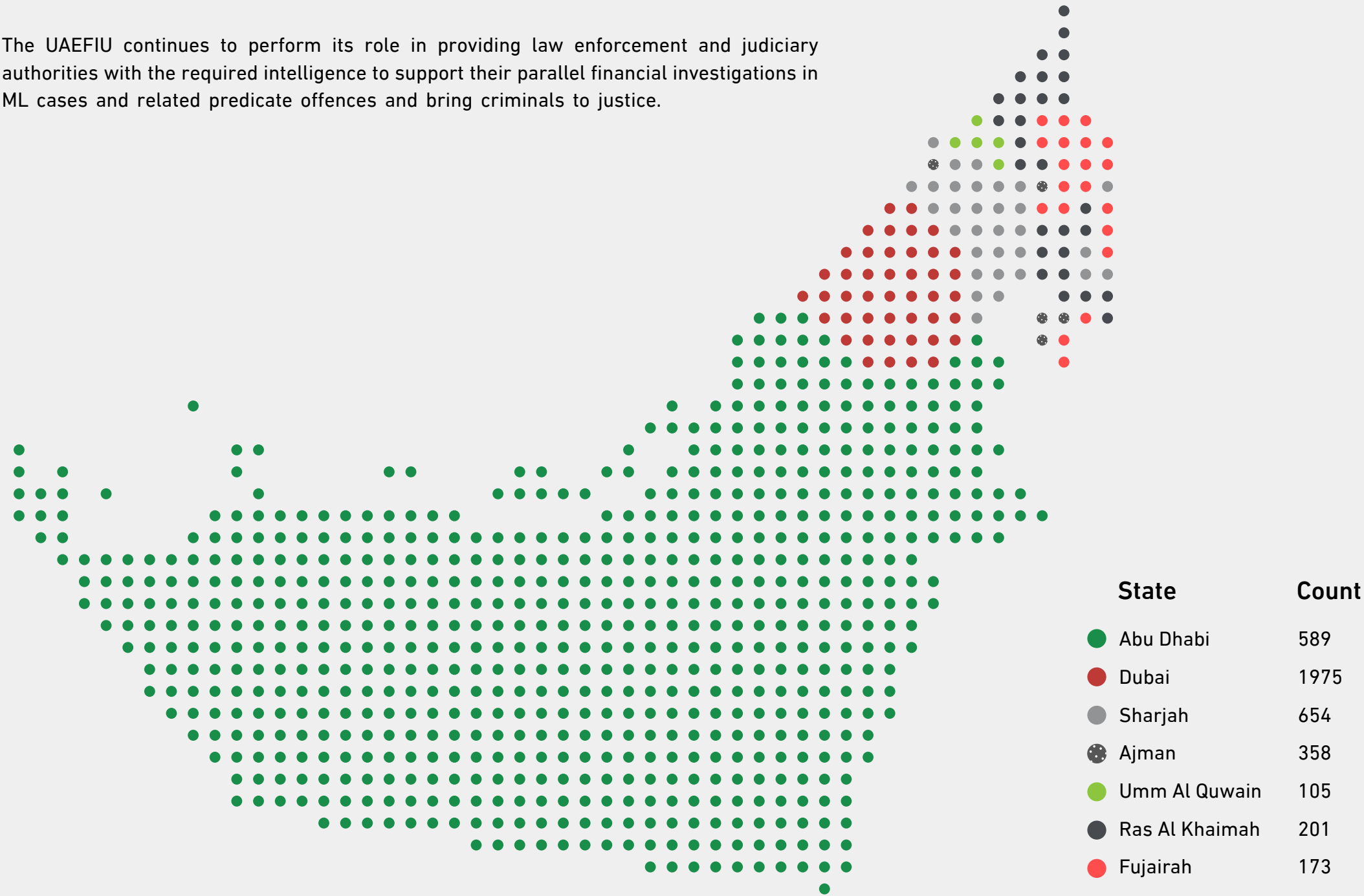
Technical Reports Provided to Domestic Authorities



OPERATIONS AND COLLABORATIONS

STRENGTHENING DOMESTIC COOPERATION

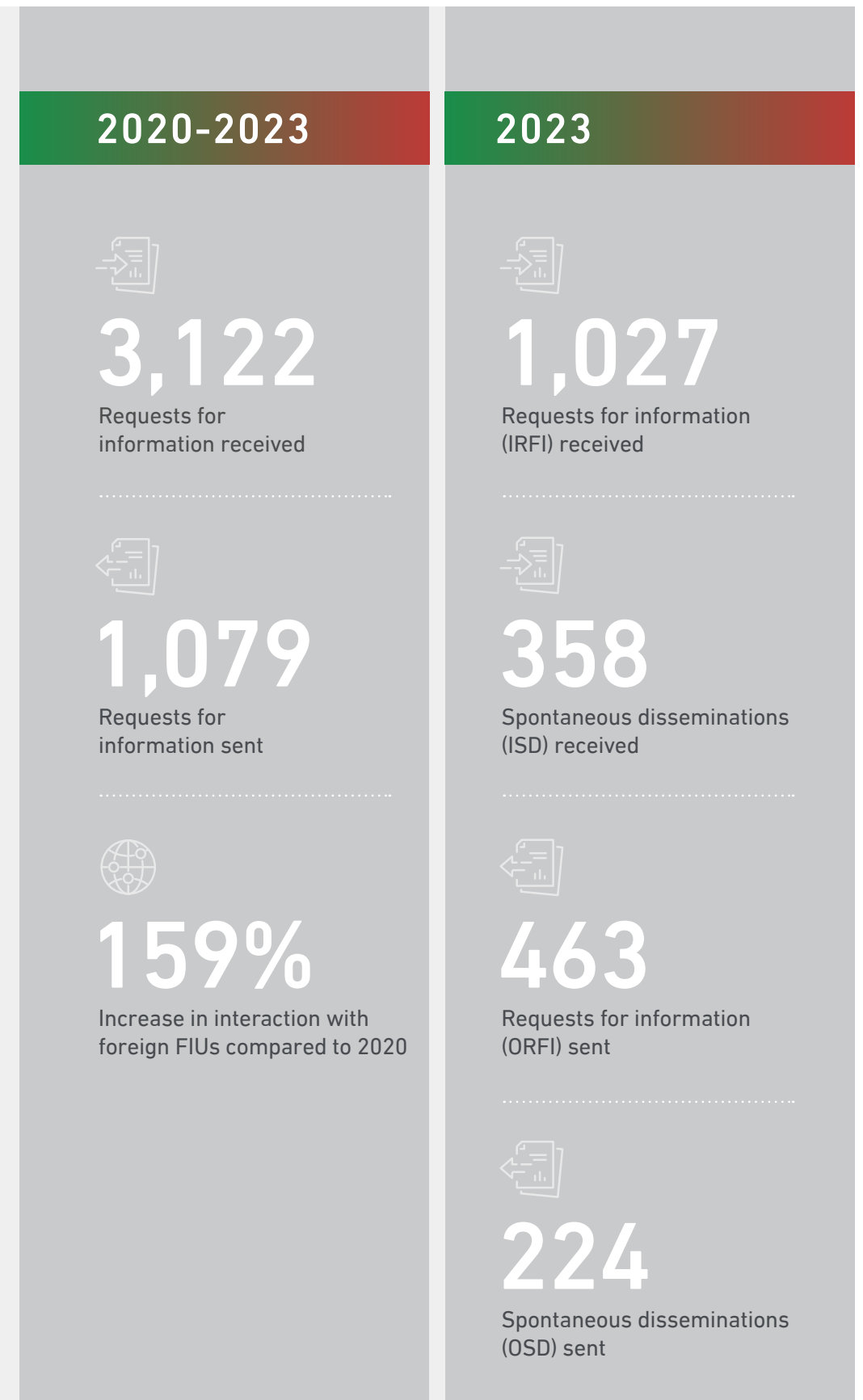
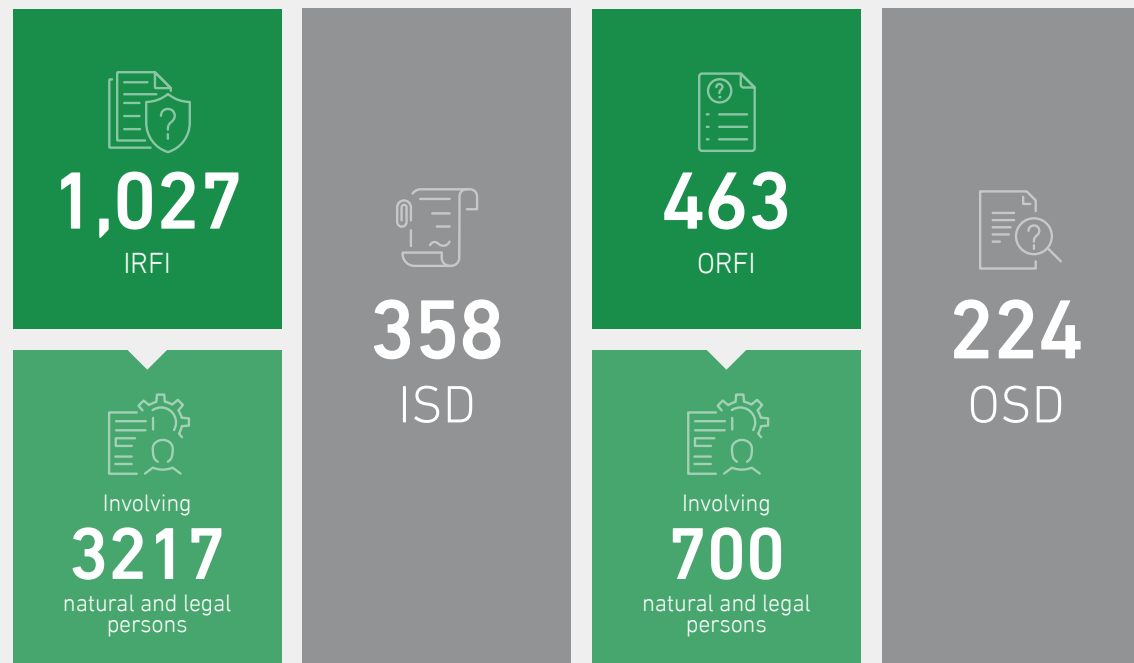
The UAEFIU continues to perform its role in providing law enforcement and judiciary authorities with the required intelligence to support their parallel financial investigations in ML cases and related predicate offences and bring criminals to justice.



OPERATIONS AND COLLABORATIONS FOSTERING INTERNATIONAL COOPERATION

Building strong alliances for transnational coordination and intelligence exchange

Financial crimes such as ML, financing of terrorism, and proliferation, often involve cross-border transactions, which require transnational coordination and information sharing to enable the tracing of criminal proceeds. The UAEFIU continues its collaboration and coordination with counterpart FIUs and other international stakeholders in identifying and tracing suspicious transactions and activities to support investigations and enforcement effectively with the required intelligence.

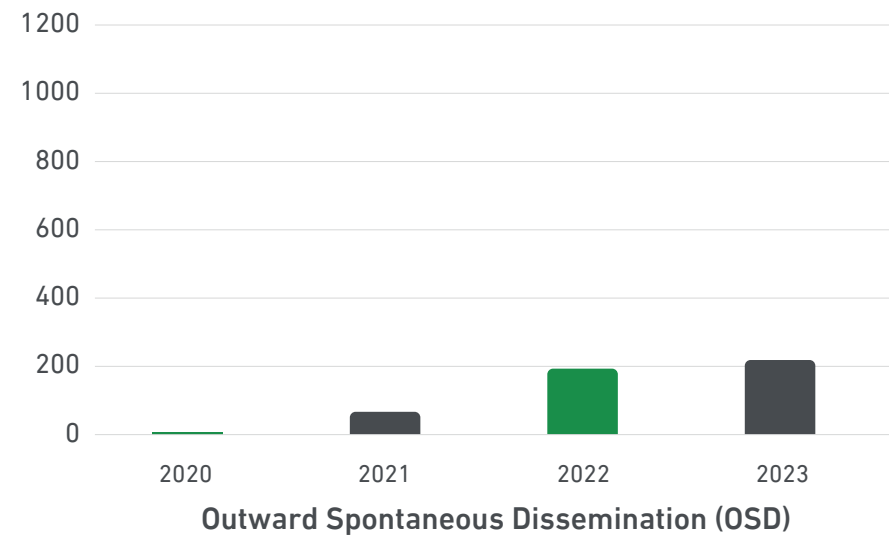
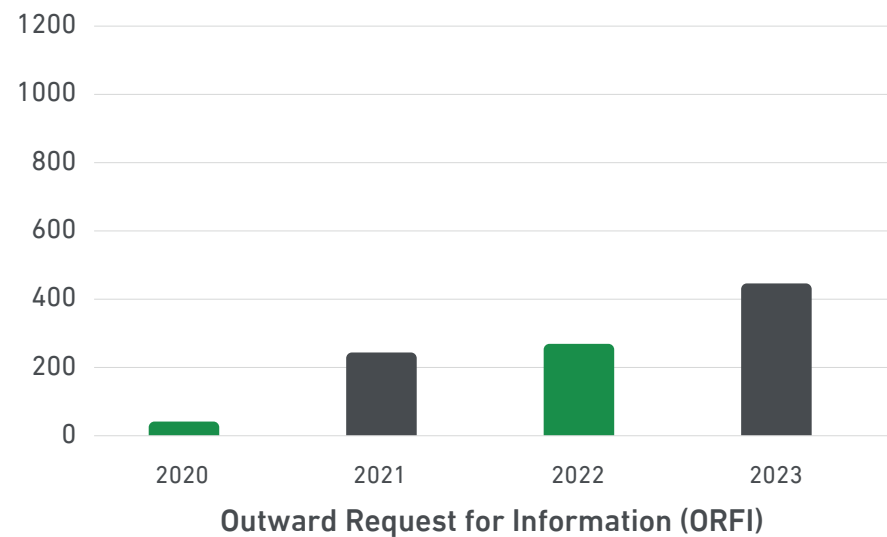
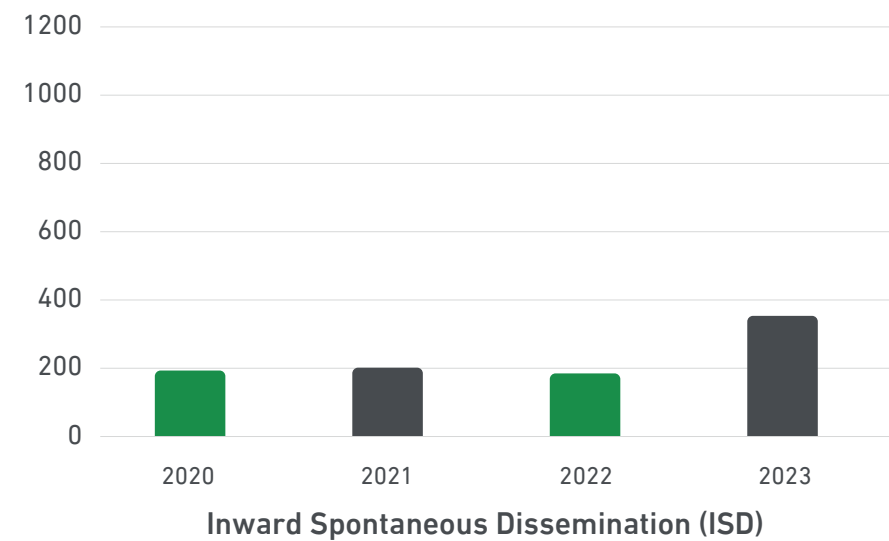
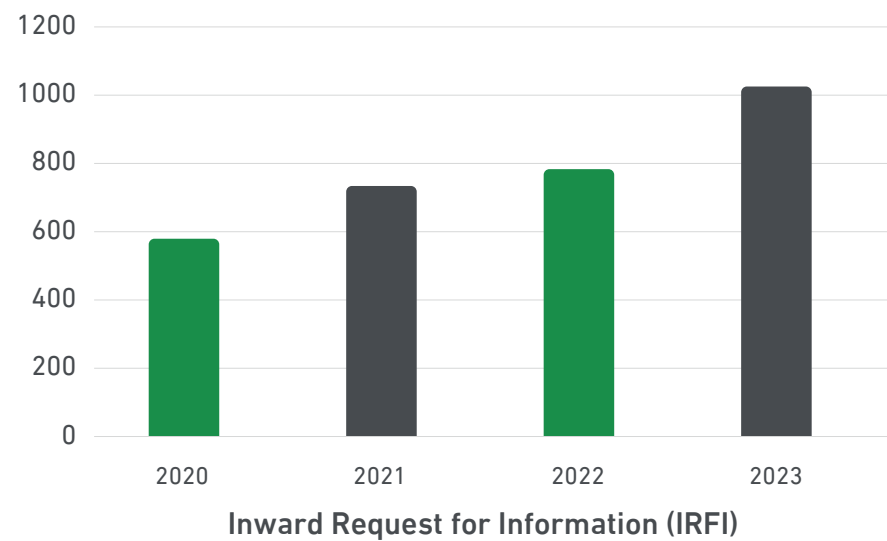


OPERATIONS AND COLLABORATIONS

FOSTERING INTERNATIONAL COOPERATION

Intelligence Reports exchanged with Foreign FIUs 01/01/2020 to 31/12/2023

A remarkable increase of 1127% was recorded concerning the number of outgoing reports (ORFIs and OSDs) in 2023 in comparison to 2020. At the same time, the turnaround time of IRFIs has declined substantially by 280%, from 156 days in 2020 to 41 days in 2023.

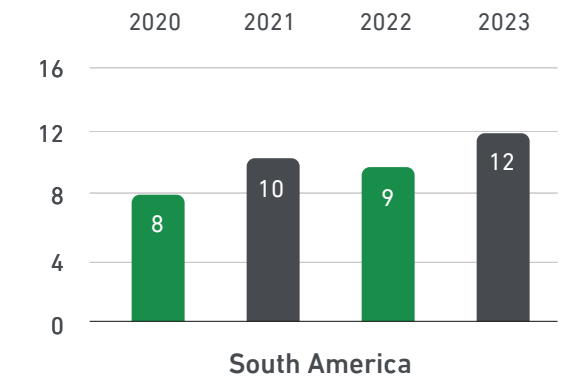
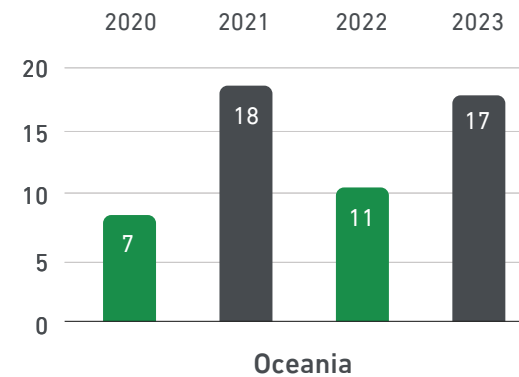
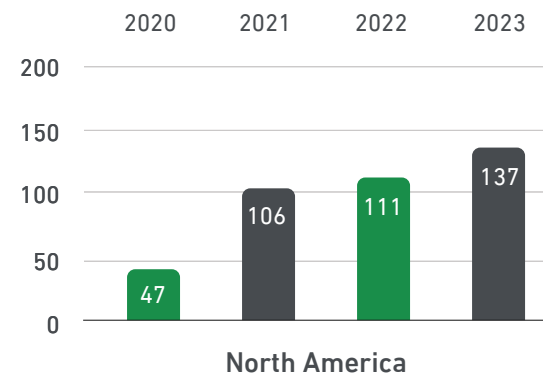
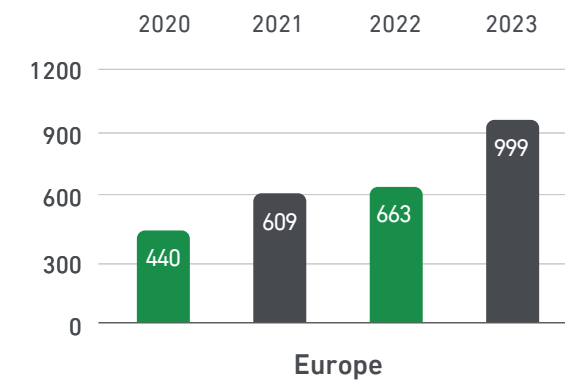
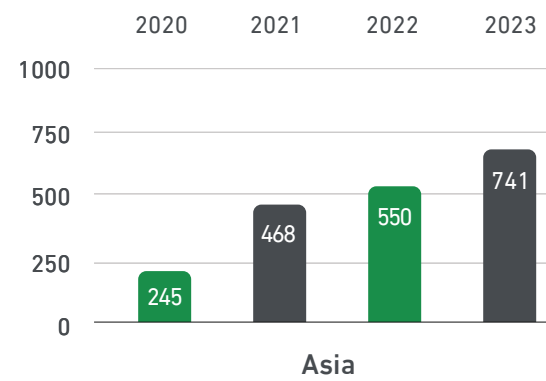
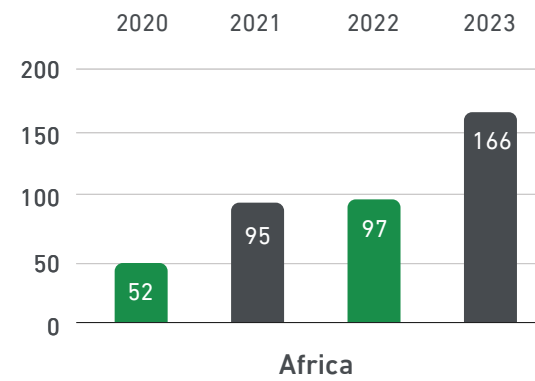


OPERATIONS AND COLLABORATIONS

FOSTERING INTERNATIONAL COOPERATION

Geographical Distribution of Information Exchanged with Counterpart FIUs 2020-2023

The UAE Financial Intelligence Unit (UAEFIU) engages internationally with 48% of jurisdictions in Europe and 38% in Asia. Additionally, it has established connections with 14% of jurisdictions from Africa, North America, Oceania, and South America.



OPERATIONS AND COLLABORATIONS

FOSTERING INTERNATIONAL COOPERATION

In terms of the involved potential predicate offence/typology in the exchanged information over the past four years, ML concerns through unexplained transfers remained at the top of the list, followed by fraud, trade-based ML, and other foreign predicate offences.

Frequent predicate offence/Typology	2020	2021	2022	2023	Total ¹²
Fraud	13%	16%	13%	10%	13%
Trade-based money laundering (TBML)	4%	6%	7%	13%	8%
Foreign predicate offences	2%	4%	5%	15%	8%
Unlicensed hawala providers	3%	4%	7%	9%	7%
Professional (third-party) Money Laundering	1%	3%	4%	11%	6%
Tax crimes	7%	4%	8%	6%	6%
Other ML offence (unexplained transfers)	39%	37%	35%	16%	29%

12- The percentage per predicate offence/typology of the total exchanged information.

OPERATIONS AND COLLABORATIONS

FOSTERING INTERNATIONAL COOPERATION

Frequent predicate offence/Typology	2020	2021	2022	2023	Total ¹³
Drug trafficking	8%	4%	7%	5%	5%
Corruption and bribery	13%	6%	7%	3%	5%
Subject of adverse media	1%	3%	1%	5%	3%
Potential misuse of virtual currency	1%	1%	1%	2%	2%
Smuggling (including in relation to customs, excise duties and taxes)	2%	3%	2%	1%	2%
Terrorism including terrorist financing	2%	3%	2%	2%	2%
Illicit trafficking in stolen and other goods	1%	2%	1%	0%	1%
Forgery	2%	1%	1%	0%	1%
Connected to sanctioned parties/countries	0%	1%	1%	2%	1%

13- The percentage per predicate offence/typology of the total exchanged information.

OPERATIONS AND COLLABORATIONS FOSTERING INTERNATIONAL COOPERATION

Ultimately, to ensure an agile engagement with the UAEFIU's strategic partners, the UAEFIU follows a systematic approach to plan its annual international engagement based on 11 different relevant criteria. Within the said plan, different activities are conducted with counterpart FIUs.

UAEFIU's 2023 activities with international partners



Establishing joint Operational teams with strategic partners focusing on common targets



Hosting the 29th Annual Egmont Group Plenary in Abu Dhabi



Signing additional five MOUs with counterpart FIUs to reach a total of 68 MOUs



REINFORCING THE UAE'S COMMITMENT TO COMBAT FINANCIAL CRIMES UAEFIU HOSTED 29TH ANNUAL EGMONT GROUP PLENARY IN ABU DHABI



The UAEFIU hosted the 29th annual Egmont Group Plenary in Abu Dhabi, under the theme 'Use of advanced IT technologies by FIUs to enhance their operations.'

Held under the patronage of HH Sheikh Mansour bin Zayed Al Nahyan, Vice President, Deputy Prime Minister, Minister of the Presidential Court, and Chairman of the Central Bank of the UAE (CBUAE), Khaled Mohamed Balama, Governor of CBUAE and Chairman of the UAE National Anti-Money Laundering and Combatting Financing of Terrorism and Financing of Illegal Organisations Committee, the event saw participation from over 500 representatives from several global entities within the anti-money laundering field.

The plenary hosted a series of discussions around various topics, including a panel around the 'Use of privacy enhancing technologies for FIUs', 'Use of artificial intelligence to enhance FIU operations, creative models of collaboration, and strategic effectiveness', and 'Use of block-chain technology to enhance FIU operations.'

By hosting the plenary, the UAEFIU reiterated its commitment to contribute towards the UAE's efforts to combat money laundering, and financing of terrorism and financial crimes, by bolstering international and promoting the exchange of information and expertise.

OPERATIONS AND COLLABORATIONS

FOSTERING INTERNATIONAL COOPERATION

68

Countries with MOUs Signed

160

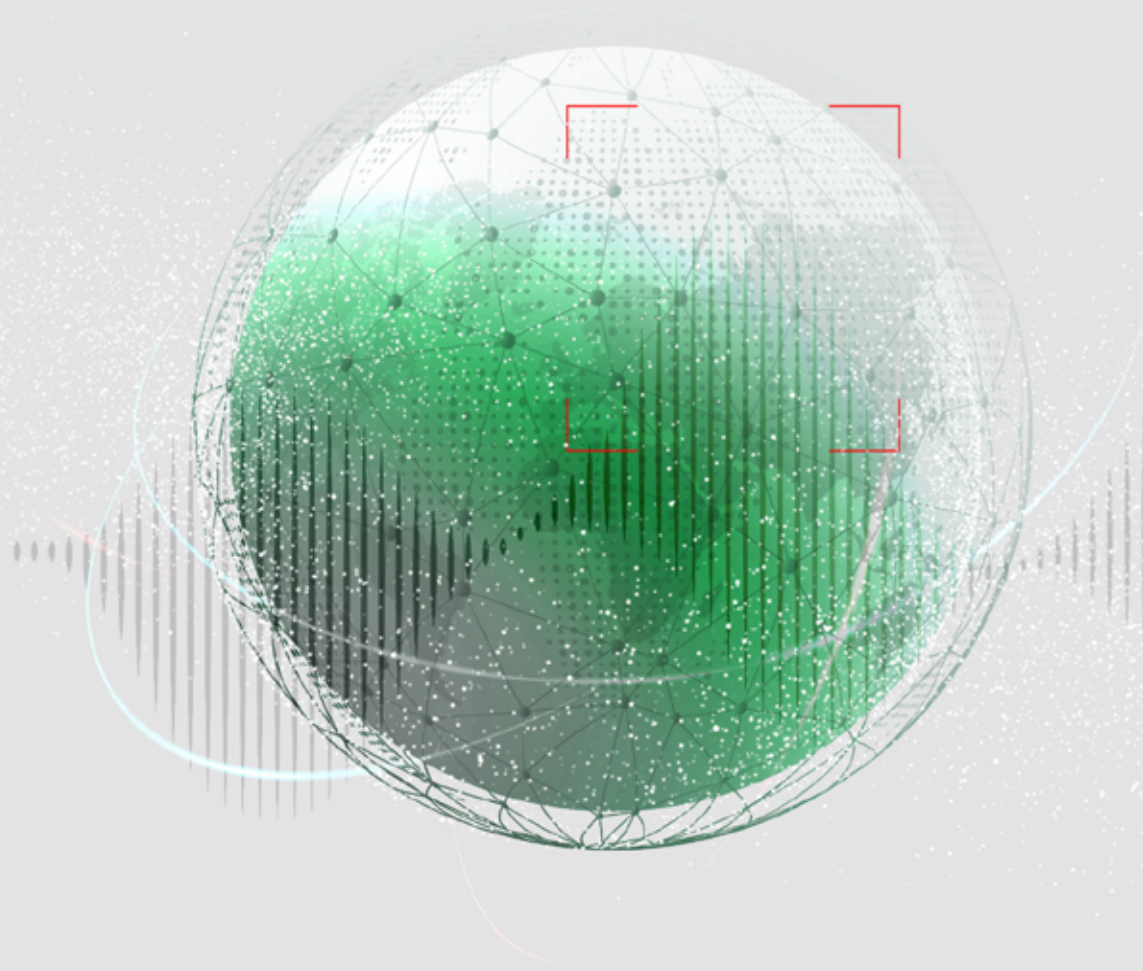
Countries with information exchange

60

Countries with MOUs signed
and information exchange

- Countries with MOUs signed
- Countries with information exchange
- Countries with information exchange (Egmont & Non Egmont)





05

OUTREACH AND COMMUNICATION

OUTREACH AND COMMUNICATION

EXPANSIVE OUTREACH ACTIVITIES

Engaging stakeholders to strengthen compliance and collaboration

The UAEFIU has been actively performing a broad spectrum of outreach activities aiming to raise awareness of reporting entities and foster collaboration with stakeholders. Moreover, the UAEFIU works closely with the relevant regulators and reporting entities to address common goals, exchange insights, and discuss areas of improvement.

In 2022-2023, the UAEFIU conducted 60 Workshops on financial crime typologies involving approximately 10,000 Attendees from LEAs and FIs

“ The UAEFIU’s outreach activities are designed to support the UAEFIU stakeholders through different approaches including workshops, one-on-one engagements, roundtable discussions, and other events ”

01



Outreach Programs to Reporting Entities

The UAEFIU creates and conducts specialized workshops and outreach sessions for reporting entities, guiding them in understanding their reporting obligations and compliance with AML/CFT laws and regulations as well as international standards. This includes jointly developing awareness programs with regulators to enhance stakeholders’ understanding and coordination in combating financial crimes.

02



Engagements with Stakeholders from Reporting Entities and Regulatory Authorities

A new approach to communication was introduced by the UAEFIU in 2022 that focuses on one-on-one engagements with reporting entities to discuss the quality of their submitted STRs/SARs, address any challenges they experience, and understand new products and associated risks.

03



Roundtable Discussions

This approach was introduced to construct focus groups to discuss and develop collaborative solutions in specific typologies and topics relevant to financial crime. It also involves activities relevant to collecting feedback to promote an effective and interactive reporting process between reporting entities and the UAEFIU.

OUTREACH AND COMMUNICATION

EXPANSIVE OUTREACH ACTIVITIES

First Advanced Strategic Analysis ▶
Training by MENAFATF/ECOFEL



Engagement Meetings
and Roundtable Discussions

2022 | ▶ 5

2023 | ▶ 19



Target
Audience

2022 | ▶ 360

from financial institutions

2023 | ▶ 882

Different stakeholders
including banks, exchange
houses and hawala service
providers, insurance,
VASPs, and CSPs



▲ Glimpse from the UAEFIU training
activities on advancing financial analysis



First training on ▶
Metaverse Investigation
by the EU Global Facility



06

APPENDICES

APPENDICES

UAEFIU REPORT TYPES

Report Types				Reporting Entity Sector						
Report type	Report Code	Report Name	Description	Financial Institutions	DPMS	Real Estate Agents & Brokers	Company Service providers	Lawyers & Notaries	Auditors & Accountants	VASPs
Suspicious reports	STR	Suspicious Transaction Report	Used when the Reporting Entity identifies a suspicion or a red flag during or after the transaction.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	SAR	Suspicious Activity Report	Used when the Reporting Entity identifies a suspicion or a red flag before conducting the transaction	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Additional Information reports	AIF	Additional Information File without Transaction(s)	Should the FIU require any further details while reviewing a STR/ SAR, then the reporting entity that originally submitted the said report may be solicited for further information by receiving an AIF request from the FIU through the Message Board.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	AIFT	Additional Information File with Transaction(s)	The AIFT report is similar to the structure of an AIF report, with the exception that this report type supports the submission of transactions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Threshold reports	DPMSR	Dealers in Precious Metals and Stones Report	A threshold report used for specific type of transactions (cash or international wire transfer)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	REAR	Real Estate Activity Report	A threshold report used for specific type of transactions (cash or crypto currency).	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Targeted financial sanctions reports	FFR	Funds Freeze Report	A targeted financial sanctions report used to report any freezing measure, prohibition to provide funds or services, and any attempted transactions related to 'confirmed matches' to the UNSC or the UAE sanctions lists	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	PNMR	Partial Name Match Report	A targeted financial sanctions report used when the Reporting Entities identifies a partial name match to the UNSC or UAE sanctions list.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
High-risk countries	HRC	High Risk Country Transaction Report	For transactions related to FATF high risk jurisdictions/countries.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	HRCA	High Risk Country Activity Report	For activities related to FATF high risk jurisdictions/countries.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

APPENDICES

LIST OF RISK INDICATORS BASED ON OUTCOMES OF RESEARCH AND STRATEGIC ANALYSIS SECTION'S PRODUCTS

1. The Abuse of Legal Entities in Money Laundering and Terrorist Financing (2021)

- Transactions that appear more complicated by use of impressive but nonsensical terms.
- Circulation of funds between linked or related entities accounts using different type of instruments (cheques, electronic transfers, etc.).
- Large volume of cash transactions through different branches of the financial institution, specially conducted by multiple individuals.
- Transactions structure appears unnecessarily layered and designed to obscure the true origin of funds.
- Multiple parties collaborating in a single transaction.
- Multiple entities remitting a single or repeated beneficiary (also entity) of which the funds subsequently remitted to offshore entity.
- A legal entity is reluctant to provide substantial information about the business nature and purpose, anticipated account activity and other relevant information at the account opening date and/or throughout the business relationship.
- A legal entity does not have adequate presence or the mere presence conveys ambiguity, i.e. online presence through websites that are vague.
- A legal entity has a UBO or associates with known dealings with counterparties residing in high risk or sanctioned jurisdictions.
- A legal entity or its UBO is linked to a negative/adverse media reports.
- A legal entity has a peculiar structure that is unreasonable and complex, i.e. potential involvement in shell companies, a parent or subsidiary of an offshore company.
- A legal entity uses intermediary or third-party extensively with no reasonable justification and providing inadequate supporting documents when requested to sustain the source and prove legitimacy of the transactions.
- A legal entity is newly established and observed to have engaged imminently to high volume of transactions and business activities.

2. The Abuse of Non-Profit Organizations: Guidance for Reporting Entities (2021)

- Transactions carried in NPO account does not commensurate with the purpose and objectives of stated activities.
- NPO or any of its controlling person(s), or its affiliates, found associated with a High-risk jurisdiction.

- NPO is reluctant to provide vital information while establishing the relationship, in particular, details of controlling person(s), list of beneficiaries (for Donation or Charitable accounts), and details of associate NPOs or organizations.
- Derogatory remarks/news found on any of the NPO's controlling person(s), including board members, managers or senior officers, as well as any associate organization, especially if the remarks indicate either exploiting the NPO by, or actively support, terrorists or terrorist organisations.
- Any of the NPO's controlling person(s), including board members, managers or senior officers, as well as any associate organization, is listed either in Domestic Terrorist list on UN Sanctions list.
- Local NPO receives multiple cash deposits of small amounts followed by either large cash withdrawal or outward remittances to other countries.
- Local NPO receives inward remittances from international counterparties without adequate rationalization.
- Intensive cash transactions in NPO account, or when cash is the only means of operating/ transacting in NPO's account especially if it involves cross-border cash movement.
- NPO providing 'service activities' (i.e. housing, social supports, education or health services) in close proximity to an active threat of extremism.
- Unjustified complexity of transactions and Diversion of funds through foreign counterparties or pass funds through Third-party intermediaries.
- "Sham" organizations relied on deception to mislead donors and other NPOs for terrorist financing purposes.
- An Individual or a Company account receives funds from foreign NPO.
- NPOs using alternative remittance systems or informal money transfers.
- Failure to provide documentary evidences to sustain the transactions, or providing vague justifications when being questioned by the Financial Institution.
- Sudden surge in the accounts activities without any proper justification.
- The NPO's controlling person(s), including board members, managers or senior officers, as well as any associate organization, has frequent travel history without reasonable justification to/from jurisdictions where terrorist groups are known to have a substantial presence.
- The NPO has obscure leadership or decision-making structure potentially aiming to disguise its ultimate controller.

APPENDICES

LIST OF RISK INDICATORS BASED ON OUTCOMES OF RESEARCH AND STRATEGIC ANALYSIS SECTION'S PRODUCTS

- The NPO's funds or assets are commingled with personal or private funds making it difficult to be traced and its purpose unidentifiable.

3. Strategic Analysis on Trade-Based Money Laundering (2021)

1. Trade Structure and Organization

- The corporate structure of a trade entity appears unusually complex and illogical, such as the involvement of shell companies or companies registered in high-risk jurisdictions.
- A trade entity is registered or has offices in a Country with weak AML/CFT compliance.
- A trade entity is registered at an address that is likely to be a mass registration address, e.g., high-density residential buildings, post-box addresses, commercial buildings or industrial complexes, especially when there is no reference to a specific unit.
- The business activity of a trade entity does not appear to be appropriate for the stated address, e.g., a trade entity appears to use residential properties, without having a commercial or industrial space, with no reasonable explanation.
- A trade entity lacks an online presence or the online presence suggests business activity inconsistent with the stated line of business, e.g. the website of a trade entity contains mainly boilerplate material taken from other websites or the website indicates a lack of knowledge regarding the particular product or industry in which the entity is trading.
- A trade entity displays a notable lack of typical business activities, e.g., it lacks regular payroll transactions in line with the number of stated employees, transactions relating to operating costs, tax remittances.
- Owners or senior managers of a trade entity appear to be nominees acting to conceal the actual beneficial owners, e.g., they lack experience in business management or lack knowledge of transaction details, or they manage multiple companies.
- A trade entity, or its owners or senior managers, appear in negative news, e.g., past money laundering schemes, fraud, tax evasion, other criminal activities, or ongoing or past investigations or convictions.
- A trade entity maintains a minimal number of working staff, inconsistent with its volume of traded commodities.
- The name of a trade entity appears to be a copy of the name of a well-known corporation or is very similar to it, potentially in an effort to appear as part of the corporation, even though it is not actually connected to it.
- A trade entity has unexplained periods of dormancy.
- An entity is not compliant with regular business obligations, such as filing VAT returns.

2. Trade activities

- Trade activity is inconsistent with the stated line of business of the entities involved, e.g., a car dealer is exporting clothing, or a precious metals dealer is importing seafood.
- A trade entity engages in complex trade deals involving numerous third-party intermediaries in incongruent lines of business.
- A trade entity engages in transactions and shipping routes or methods that are inconsistent with standard business practices.
- A trade entity makes unconventional or overly complex use of financial products, e.g. use of letters of credit for unusually long or frequently extended periods without any apparent reason, intermingling of different types of trade finance products for different segments of trade transactions.
- A trade entity consistently displays unreasonably low profit margins⁵ in its trade transactions, e.g. importing wholesale commodities at or above retail value, or re-selling commodities at the same or below purchase price.
- A trade entity purchases commodities, allegedly on its own account, but the purchases clearly exceed the economic capabilities of the entity, e.g., the transactions are financed through sudden influxes of cash deposits or third-party transfers to the entity's accounts.
- A newly formed or recently re-activated trade entity engages in high-volume and high-value trade activity, e.g., an unknown entity suddenly appears and engages in trade activities in sectors with high barriers to market entry.

3. Trade documents and commodities

- Inconsistencies across contracts, invoices, or other trade documents, e.g., contradictions between the name of the exporting entity and the name of the recipient of the payment; differing prices on invoices and underlying contracts; or discrepancies between the quantity, quality, volume, or value of the actual commodities and their descriptions.
- Contracts, invoices, or other trade documents display fees or prices that do not seem to be in line with commercial considerations, are inconsistent with market value, or significantly fluctuate from previous comparable transactions.
- Contracts, invoices, or other trade documents have vague descriptions of the traded commodities, e.g., the subject of the contract is only described generically or non-specifically.
- Trade or customs documents supporting the transaction are missing, appear to be counterfeits, include false or misleading information, are a resubmission of previously rejected documents, or are frequently modified or amended.

APPENDICES

LIST OF RISK INDICATORS BASED ON OUTCOMES OF RESEARCH AND STRATEGIC ANALYSIS SECTION'S PRODUCTS

- Contracts supporting complex or regular trade transactions appear to be unusually simple, e.g., they follow a "sample contract" structure available on the Internet.
- The value of registered imports of an entity displays significant mismatches to the entity's volume of foreign bank transfers for imports. Conversely, the value of registered exports shows a significant mismatch with incoming foreign bank transfers.
- Commodities imported into a country within the framework of temporary importation and inward processing regime are subsequently exported with falsified documents.
- Shipments of commodities are routed through several Countries without economic or commercial justification.

4. Trade Accounts and Transactions

- A trade entity makes very late changes to payment arrangements for the transaction, e.g., the entity redirects payment to a previously unknown entity at the very last moment, or the entity requests changes to the scheduled payment date or payment amount.
- An account displays an unexpectedly high number or value of transactions that are inconsistent with the stated business activity of the client.
- An account of a trade entity appears to be a "pay-through" or "transit" account with a rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons, including:
 - An account displays frequent deposits in cash which are subsequently transferred to persons or entities in free trade zones or offshore jurisdictions without a business relationship to the account holder.
 - Incoming wire transfers to a trade-related account are split and forwarded to non-related multiple accounts that have little or no connection to commercial activity.
 - Payment for imported commodities is made by an entity other than the consignee of the commodities with no clear economic reasons, e.g., by a shell or front company not involved in the trade transaction.
 - Cash deposits or other transactions of a trade entity are consistently just below relevant reporting thresholds.
 - Transaction activity associated with a trade entity increases in volume quickly and significantly, and then goes dormant after a short period of time.
 - Payments are sent or received in large round amounts for trade in sectors where this is deemed as unusual.
 - Payments are routed in a circle – funds are sent out from one country and received back in the same country, after passing through another country or countries.

4. Strategic Analysis on Money Value Transfer Services (MVTs) and Registered Hawala Providers (RHP) (2021)

- Customer conducting their business relationship or transactions in unusual circumstances, such as, customer:
 - A. travels unexplained distances to locations to conduct transactions;
 - B. defined groups of individuals conducting transactions at single or multiple outlet locations or across multiple services;
 - C. owns or operates a cash-based business that appears to be a front or shell company or is intermingling illicit and licit proceeds as determined from a review of transactions that seem inconsistent with financial standing or occupation.
- Customer remits money internationally and then receives back an equal value of the amount.
- Customer presents single DRIC as supporting document for multiple transactions.
- Customer receives multiple transfers from unrelated parties, specifically individuals residing in foreign jurisdiction, on which a "Fund Recall Request" has been received.
- Using MVTs or MSB's accounts to send or receive funds which are suspected to be fraudulent proceeds.
- Customer (sender) appears to have no direct or economical relationship with the receiver of the transfer.
- A group of customers uses similar contact information with unreasonable explanation (e.g. address, mobile number, e-mail address).
- MVTs/RHP customer is suspected to be acting on behalf of a third party but not disclosing that information or is being controlled by someone else.
- Transactions conducted in the account are unnecessarily complex with no apparent economic rationale.
- Transactions are seemingly of pass-through nature – funds received directly debited via wire transfers leaving low balance in the account.
- Several transfers from multiple remitters directed to a single beneficiary with no reasonable explanation.
- Individual account is receiving small amounts from different unrelated individuals, and eventually transferring the sum to another individual account or LE's account.
- Multiple entities remitting to a single or repeated beneficiary (also an entity), of which the funds are subsequently remitted to an offshore entity.
- Receipt of international remittances from foreign counterparties inconsistent with its own business activities.

APPENDICES

LIST OF RISK INDICATORS BASED ON OUTCOMES OF RESEARCH AND STRATEGIC ANALYSIS SECTION'S PRODUCTS

- Large cash deposits or large cash withdrawals from or to MVTs/RHP/LE's (suspected UHP) account.
- MVTs/RHP uses intermediary or third-party extensively with no reasonable justification and providing inadequate supporting documents when requested to sustain the source and prove authenticity of the transactions.
- RHP/UHP's account is receiving multiple remittances from another LE's or individual's accounts, and eventually transferring the sum to another LE's account located in another jurisdiction.
- RHP or LE (suspected UHP) conducts an unusually high number of transactions with counterparties (known HP) in high-risk jurisdictions, or providing services to customers from high-risk jurisdictions.
- RHP or LE (suspected UHP) structures transaction in an attempt to break up amounts to avoid reporting or interrupt tracing of funds.
- RHP or LE's (suspected UHP) transaction volume is inconsistent with its stated business activity, scope or its past transaction volume.
- RHP or LE's (suspected UHP) owners, shareholders, or authorized signatories, or any of its counterparties has been the subject of adverse news of a trusted media source. MVTs/RHP/UHP or any of its controlling person(s), or its affiliates, is found to be associated with a High-risk jurisdiction.
- RHP or LE (suspected UHP) is heavily engaged into cash-border transactions, which involved high-risk jurisdictions.
- RHP/UHP seems to use trade transactions to settle accounts between jurisdictions, precisely TBML techniques like over-invoicing or under-invoicing.
- MVTs/RHP is observed to be operating with poor compliance measures.
- MVTs/RHP has been the subject of law enforcement investigations (known publicly) or adverse news in relation to any ongoing investigation.
- Business accounts used to receive or disburse large sums of money but show virtually no normal business-related activities, such as payment of payrolls, invoices etc.

5. Strategic Analysis on Professional Money Laundering (PML) and Foreign Proceeds of Crimes (2021)

- An individual setting up multiple companies dealing in different lines of business simultaneously (one individual initially establishes the businesses; same address registered for most of the businesses; actual business activity not verifiable; each business is actually controlled by different individuals).

- Repeatedly depositing large cash amounts in the account which is supported by 'Cash Declaration forms' or also known as DRIC forms (Declaration regarding importation of Cash).
- Derogatory remarks or negative news found in external sources/public domain on the account holder or any of its counterparties, associates, signatories, UBOs, etc.
- Opening repository bank accounts under the name of a Legal Entity (to transmit funds from one jurisdiction to another swiftly; transfers justified as part of a normal business activity; used as pass-through accounts).
- Circulation of funds between several Entities accounts without any apparent reason, that might also suspected to be as 'shell companies' (no real business activity; incorporated for ML purposes exclusively).
- Setting up and using front companies (presence of real business activity; use to commingle legitimate and illegitimate funds, mainly used effectively in cash-intensive businesses).
- Transactions that involve 'Gatekeepers' which is found to be with no rationale or any apparent reason, specially to engage in several investments and purchase assets specifically high-value items.
- Transactions with an Entity of a complex structure, in which the UBO is hard or cannot be identified (main purpose is to hide the UBO; to disguise funds transfers as capital transfer or normal business transaction).
- Funds received from offshore party(ies) subsequently routed to different personal or business accounts.
- Providing fictitious documents to sustain the legitimacy of transaction (i.e. trade-based ML, seemingly "real" trade transactions supported by forged supporting documents, e.g. invoices, contract agreement, bill of lading, etc.).
- A group of customers uses similar contact information with unreasonable explanation (e.g. address, mobile number, e-mail address).
- The account holder suspected to be acting on behalf of a third party but not disclosing that information or is being controlled by someone else.

6. Fraud Crimes, Trends and Typologies Report (2022)

- A customer submitting documents suspected to contain any materially false, fictitious, or fraudulent statement or entry.
- A customer knowingly falsifies, conceals, or covers up via any trick or scheme a material fact or makes any materially false statement or representation.
- Discrepancies observed between reported facts, observed data, and/or supporting documentation.

APPENDICES

LIST OF RISK INDICATORS BASED ON OUTCOMES OF RESEARCH AND STRATEGIC ANALYSIS SECTION'S PRODUCTS

- Inadequate or apparently altered supporting documentation (such as, alterations to any vital information, scraps, spelling mistakes, etc.).
- Supporting documents that contains vendor receipts and/or other supporting documents that appear to be altered (obvious white-out areas, cuttings, deletions).
- 'Funds recall requests' received from different remitting banks on the same beneficiary.
- Funds received via wire transfers (international or local) from unrelated parties, followed by immediate withdrawals or outward remittances.
- Incoming funds transfer followed by 'Funds recall request' from the remitting bank.
- Frequent incoming funds transfers from unrelated parties to a newly opened account(s).
- Insufficient justifications obtained from the account holder on the received funds, or a customer that clearly unaware of the purpose and source of funds received in the account.
- Accounts opened for 'Salary' purpose especially individuals as low-income workers with no actual salary income witnessed in the account, instead the account receiving multiple remittances or deposits from unrelated parties.
- Other 'Red flag' indicators (Financial/Behavioral):
- Unusual transactions or inter-account transfers (including relevantly small amounts).
- Rising costs with no explanation or that are not commensurate with an increase in revenue.
- Employees who appear to make a greater than normal number of mistakes, especially where these lead to financial loss through cash or account transactions.
- Employees who are subject to complaints and/or tend to break the rules and who also request details about proposed internal audit scopes or inspections.

7. Strategic Analysis Report on Dealers in Precious Metals and Stones (DPMS) (2022)

- DPMS entity has a peculiar structure that is unreasonable and complex, e.g., there is potential involvement of shell companies, a parent or subsidiary of an offshore company, in which the UBO is difficult to identify or cannot be identified (whose main purpose is to hide the UBO and/or disguise fund transfers as a capital transfer or normal business transaction).
- DPMS set up as a front company (presence of real business activity; use to commingle legitimate and illegitimate funds, mainly used effectively in cash-intensive businesses).
- Large and complex transactional behaviors for newly established entities as DPMS.
- Unnecessarily maintaining multiple bank accounts for the same entity (DPMS), or opening accounts under the names of employees.
- DPMS entity or its representatives are transacting outside of the normal monetary system, or are making excessive use of cash transactions.
- DPMS or its representatives are using gold as a medium of exchange.
- The circulation of funds between multiple DPMS accounts, or between 'unrelated' parties which are in different lines of business that might also be suspected of being 'shell companies' (no real business activity; incorporated for ML purposes exclusively).
- The transaction structure appears to be unnecessarily layered and designed to obscure the true origin of funds.
- DPMS entity's owners, shareholders, or authorized signatories, or any of its counterparties, have been the subject of adverse news from a trusted media source.
- DPMS or any of its controlling persons, or its affiliates, have been found to be associated with a high-risk jurisdiction.
- DPMS entity that is heavily engaged in cross-border cash movement.
- DPMS entity repeatedly depositing large cash amounts in an account, or exchanging foreign currencies, which is supported by 'cash declaration forms,' also known as DRIC forms (Declaration Regarding Importation of Cash).
- DPMS or its representatives fail to provide a 'customs declaration' in relation to a local/foreign currency cash deposit related to buying/selling precious stones.
- DPMS entity engages in transactions and shipping routes or methods that are inconsistent with standard business practices.
- Contracts, invoices, or other trade documents provided by a DPMS have vague or missing descriptions, appear to be counterfeit (including false or misleading information), include a resubmission of previously rejected documents, or are frequently modified or amended.
- DPMS entity or any of its counterparties appear to import precious metals and stones that originate from a country in which there is limited production or no mines at all.
- Deposits or transfers are received in a DPMS account followed by the immediate transfer of similar amounts to another jurisdiction.
- DPMS entity and its associates, or multiple individuals (external parties), excessively conduct foreign exchange transactions (FOREX) without any business rationale.
- Payment for imported PMS made by an entity other than the consignee for no clear business reason, e.g., by a shell or front company not involved in a trade transaction.
- Cash deposits or other transactions of a DPMS entity (or its representatives) are consistently just below the relevant reporting thresholds (transactions conducted by multiple individuals to avoid reporting requirements).
- Transactions in a DPMS account(s) are seemingly of a pass-through nature, with funds directly debited via wire transfers leaving a low balance in an account.
- DPMS entity(s) excessively obtain loans or credit facilities, which are settled before the due date through cash or cheque repayments.

APPENDICES

LIST OF RISK INDICATORS BASED ON OUTCOMES OF RESEARCH AND STRATEGIC ANALYSIS SECTION'S PRODUCTS

- DPMS entity(s) transfer payments amongst each other, which are related to 'borrowings' or 'loans' that is referred to as 'back-to-back' or 'loan-back'.

8. Far East Typology Patterns and Schemes – White Paper (2022)

- A rapid movement of funds via inward wires from multiple counterparties, internal transfers, cash and cheque deposits, or customers' own external accounts, followed by outward wires toward other corporate or customers' own accounts in the UAE or in Far East and North American countries.
- A new established legal entity (licensed for trade activities, as mentioned previously) with a significant difference between the reported turnover in the KYC and the actual turnover.
- A change in name and ownership of an entity following its establishment.
- UBOs who are most likely in their late twenties or early thirties and from, but are not limited to, South Asian countries.
- No rationale behind a large volume of inward and outward transactions from/to the identified Far East route over a short span of time (on the same day or on consecutive days, or over a few months).
- Inconsistency between account activities and turnover and the profile of the customer and the nature of the business.
- Employing dormant accounts or accounts with no observed business transactions until a sudden surge in the flow of funds by means of the Far East route.
- No actual business activity or operational expenses being observed in the company account.
- Corporate accounts being opened in different currencies to receive or send money while left with a low or nil balance.
- Difficulty in identifying or establishing the relationship between the customer and trading counterparties or ultimate buyers.
- A high volume of currency exchanges involving the US or Canadian dollar, and AED.
- Phantom shipments including trade document fabrication, the misrepresentation of goods and services, and price manipulation.
- Customer failure or reluctance to provide a complete set of documents to substantiate account activity (such as the shipment of goods, valid bills of lading, clear trading settlement arrangements, custom clearance certificate, etc.).
- The business background of a UBO or the nature of a business cannot be validated in the public domain (e.g., no website for the business).
- Counterparties having a different line of business and there being difficulty in establishing the nature of customers' business.

- Funds being layered between accounts of mutual counterparties.
- The customer having been found to be transacting (internally/externally) with previously reported entities where the relationship had been terminated due to various ML concerns.
- The supplier of the customer being previously reported due to ML concerns.
- High Value of local remittances and clearing cheques received from (registered) hawaladars/MSB where the information relating to ultimate source of funds could not be established.
- Potential link to using unregistered hawaladars (i.e., involvement of third parties while the ultimate source of funds or remitter details are not known).
- Conducting business with or through high-risk jurisdictions and OFAC-sanctioned entities.

9. The Abuse of Legal Persons and Arrangements in Illicit Activities (2023)

- A legal entity has a peculiar, unreasonable, complex structure. It involves multiple ownership layers (especially when offshore or foreign entities are also part of the ownership), combined with difficulties in identifying the UBO(s).
- A legal entity registered under a misleading name indicates different activities than what the business activity is licensed to practice.
- A legal entity is registered under a misleading name that appears to imitate other recognized companies' names, particularly high-profile multinational corporations.
- Potential involvement of a 'shell company,' especially an offshore one, under whose name multiple assets and other entities are being registered, with a suspicion that the primary purpose is to hide the UBO or to disguise fund transfers as a capital transfer for setting up new entities.
- A legal entity is set up as a front company (the presence of actual business activity; used to commingle legitimate and illegitimate funds, mainly used effectively in cash-intensive businesses).
- A legal entity's director(s), controlling shareholder(s), and/or beneficial owner(s) or any of its counterparties has been the subject of adverse news from a trusted media source.
- A legal entity's director(s), controlling shareholder(s), and/or beneficial owner(s) or any of its counterparties who has a nexus to a prominently high-risk jurisdiction that is considered to pose a high risk of money laundering or terrorist financing.
- A legal entity's director(s), controlling shareholder(s), and/or beneficial owner(s) is listed against the accounts of other legal persons or arrangements, indicating the use of professional nominees.
- A legal entity or any of its controlling persons or its affiliates is associated with a high-risk or sanctioned jurisdiction, individual or entity.

APPENDICES

LIST OF RISK INDICATORS BASED ON OUTCOMES OF RESEARCH AND STRATEGIC ANALYSIS SECTION'S PRODUCTS

- A legal entity frequently or unnecessarily changes shareholders, increases capital, and changes its business name without an obvious rationale.
- A legal entity heavily engaged in cross-border cash movement, especially if the LE is not registered as a hawala provider, indicates possible illegal hawala activities.
- Documents provided by a legal entity, such as contracts, invoices, or any trade documents, have vague or missing descriptions, appear to be counterfeit (including false or misleading information), include a resubmission of previously rejected documents, or are frequently modified or amended.
- Deposits or transfers are received in a legal entity's account, followed by the immediate transfer of similar amounts to another jurisdiction, seemingly a pass-through, leaving a low balance in the account.
- The circulation of funds between multiple legal entity accounts or between 'unrelated' parties in different lines of business might be suspected of being a 'shell company' (no actual business activity; incorporated for ML purposes exclusively).
- The number and value of transactions in the legal entity's account do not correspond to the company's activity and transaction history.
- The transaction structure of a legal entity's account is unnecessarily layered and designed to obscure the true origin of funds, especially high-volume transactions that move rapidly.
- A legal entity that unnecessarily maintains multiple bank accounts, through which multiple transactions are conducted to circulate the same funds, also involves personal accounts under the name of the LE's shareholders, signatories or UBOs.
- Several related or unrelated legal entities transfer funds amongst one another, which are referred to as 'borrowing' or 'loan' payments.
- Establishing/registering multiple entities in a similar or different line of business and activity that are all commonly controlled or registered under the same/repeated shareholder, signatory or UBO(s) name.
- A legal entity that declares many shareholders and beneficiaries, all of whom are noted to be holding less than 25% of shares, and also many other controlling persons like POAs and authorized signatories.
- A legal entity account that has demonstrated a long period of inactivity following incorporation, followed by a sudden and unexplained increase in financial activity.
- A legal entity that fails to declare that any of its directors, controlling shareholders, and/or beneficial owners are politically exposed persons (PEPs) or have familial or professional associations with counterparties that might be linked to PEPs.
- A legal entity that conducts a large number of transactions (especially wire transfers) with international legal entities supported by trade documents (trade-based) without sufficient

corporate or trade justification or when the provided documents are found to be doubtful.

- A legal entity sends and/or receives frequent payments to/from foreign professional intermediaries without any business justification.
- A legal entity that receives large funds and subsequently transfers the funds to the personal account of the entity, controlling director(s), shareholder(s), and/or declared beneficial owner(s), or family members.

10. Patterns of Abusing Financial Institutions in Drug Trafficking and Laundering its Proceeds (2023)

- An individual opens an account where the purpose is for a salary transfer with no actual salary credits found in the account.
- An individual opens multiple accounts with different financial institutions without reasonable purpose or inconsistent with the customer profile and income.
- An individual account opened for salary or savings purposes shows multiple cash deposits inconsistent with the customer profile, followed by immediate structured withdrawals from different locations on the same day.
- An individual account shows transactions that are inconsistent with the customer profile and has an occupation that could be associated with or has a role in drugs supply chain.
- An individual uses a personal account instead of the company account for business transactions.
- An individual receives through a money service business frequent multiple small remittances without reasonable purpose.
- An individual or a group of individuals conducts multiple foreign currency exchange transactions with a money service business involving multiple currencies.
- An individual or a group of individuals approaches a money service business to send multiple transfers to a single or frequent beneficiary, especially if the beneficiary is located in a jurisdiction known for drug trafficking.
- A company account shows frequent cash deposits in relatively small amounts, followed by multiple transfers to different individuals and legal persons where the relationship of the parties and the purpose of transactions are not established.
- A company account that does not show any actual business transactions.
- A company account which exceeds its declared annual turnover with the rapid movement of funds.
- A company that trades in drug substances receives payments from a foreign legal person(s) based in a jurisdiction known for drug trafficking.

APPENDICES

LIST OF RISK INDICATORS BASED ON OUTCOMES OF RESEARCH AND STRATEGIC ANALYSIS SECTION'S PRODUCTS

- Payment for imported/re-exported commodities is made by a third party for no apparent economic reasons, e.g., by a company that is not involved in the trade transaction.
- Inconsistencies in the trade entity's provided documents, e.g., discrepancies in the described imported/re-exported product name, quantity, and price.
- Incoming wire transfers to a company account followed by outward transfers to multiple unknown individual accounts or having declared no commercial purposes to the financial institution when the customer opened the account.
- Company trade documents, such as contracts and invoices have vague descriptions of traded chemicals or pharmaceutical products.
- A customer account that appears to function as a funnel account whereby it receives multiple frequent cash deposits followed by immediate withdrawals using different ATMs/CDMs across the UAE.
- An account is suspected of being used by a third party(ies), especially if the account holder appears to be outside the country.
- A customer (natural or legal person) who was found to be listed by foreign regulator authorities due to drug trafficking and money laundering, such as an OFAC Designated Narcotics Trafficker Kingpin.
- An account shows an unusual pattern of transactions that could be linked to adverse media on organized crime and drug cartels.
- Transfers that had an indirect receiving exposure to a wallet address linked to a dark website known for selling or advertising drugs.
- An account holder conducts structured deposits or transfers and issues frequent multiple cheques in favor of a legal professional or real estate broker, inconsistent with the customer profile.
- Inconsistencies between the information provided in the account KYC and the customer's transactional pattern.
- An account that is only funded via inward remittances and cash deposits.
- Source of funds and purpose of withdrawals cannot be ascertained.
- A company account that shows inconsistencies between the company transactions and trading supporting documents and provided invoices.
- An account owner cannot provide proper justifications or supporting documents to sustain the legitimacy of funds and transactions carried out in the account or attempts to close an account to avoid due diligence questioning.
- The use of an account for purposes other than the declared one when establishing the relationship with the financial institution.
- Account activity shows high velocity in the movement of funds.

11. Real Estate Money Laundering Typologies and Patterns (2023)

A. Risk Indicators Relevant to Real Estate Professionals

Customer Characteristics and Behavioral Pattern

- A customer with a low income wants to pay for a high-value property in cash.
- A customer asks a real estate agent to conduct a transaction/accept a cash payment on his/her behalf as soon as possible for a high commission percentage.
- A customer asks a real estate agent to conduct a transaction on his/her behalf due to personal reasons (i.e., being a non-resident or with a load of high-level work), using intimidating words like "working with high-level government organizations" and asking to keep this relationship confidential.
- A customer decides not to proceed with a transaction after being asked many questions about the background of the source of funds or the method of payment.
- A customer wants to invest in any high-value business as quickly as possible with no specific requirements, preferences, required location, or negotiation of the property price.
- A customer requests that a real estate agent register purchased real estate below its market value or lower than the paid amount with an offer of high commission.
- One or two individuals (buyer and/or seller) approach a real estate agent to finalize a real estate deal with a significant variation between the purchase price and the market value.
- A customer approaches a real estate agent to sell a property that was recently bought with a significant difference between the selling price and the market value (flipping).
- A return customer wants to buy a property that he/she recently sold (flipping).
- A group of individuals are paying together for one or multiple properties with no clear relationship.
- A customer who is listed on any list of targeted financial sanctions.
- A customer associated with countries at high risk of ML/TF or with a high level of corruption.
- A customer who is linked to a politically exposed person (PEP).
- Adverse media associate the customer with a criminal act or financial crime.

Transactional Pattern

- A rapid movement of funds via manager cheques toward real estate entities that does not match the customer profile.
- A customer wants to buy multiple high-value real estate units (including off-plan) via structured amounts of cash and/or other banking instruments (i.e., manager cheques) with no apparent source of funds.

APPENDICES

LIST OF RISK INDICATORS BASED ON OUTCOMES OF RESEARCH AND STRATEGIC ANALYSIS SECTION'S PRODUCTS

- A customer wants to buy multiple high-value real estate units (including off-plan) through cryptocurrency while the source of this cryptocurrency is unknown (i.e., using P2P cryptocurrency transfer) and/or does not match the customer profile.
- A customer pays the value of a property through a friend/family member or unidentified third party.
- A natural or legal person is paying for the customer's transaction with no clear relationship.
- A customer approaches the same real agent on subsequent days to buy multiple properties with no clear source of funds.
- A legal professional or tax advisor holds POA to act on behalf of a non-resident customer(s) or offshore entity in buying and selling properties in the UAE.
- A company with a complex ownership structure purchases one or multiple off-plan units.
- A company with no physical presence/address, contact number, or email address (shell entity) purchases a property.
- A customer changes the payment method at the last moment of the deal from the one agreed upon (e.g., paying in cash instead of a cheque).
- A group of individuals with the same nationality with no apparent source of income approach a real estate agent(s) to buy different properties in the same building.

Difficulty of Verification and Inconsistency of Information

- The source and legitimacy of the funds cannot be ascertained due to a lack of supporting documents.
- The source of the manager's cheque(s) is unknown due to insufficient corroborating evidence.
- A company manager buys a high-value residential property under the company name via his/her own account with no or minimum information on the beneficial owners.
- A company manager buys a high-value residential property under the company name in cash with no clear business reason and while not providing a source of income or company book/statement.
- A customer provides suspected forged documents or fabricated invoices to support the claimed source of funds.

B. Risk Indicators Relevant to Financial Institutions

Customer Characteristics and Behavioral Pattern

- A customer (natural or legal person) is dealing with multiple individuals and real estate agents in purchasing multiple high-value properties while they were not declared during

onboarding or in the trade license.

- A customer appears to be acting on behalf of third parties and is suspected to be using his/her account for fund placement and layering to be integrated into buying properties in the UAE.
- An unusual transactional pattern while the customer claims to be working as a freelancer in the real estate business.
- An account appears to be used for facilitating third party transactions on behalf of the employer.
- A third party holds POA from an offshore entity incorporated in a lax AML/CFT jurisdiction or that is the subject of open sources and which is acting on behalf of buying and selling properties in the UAE.
- An entity facilitating fund custodian, trustee and fiduciary services engages in real estate transactions/activities on behalf of third parties with no authorized business activity as per the license.
- A customer has multiple companies registered in the real estate business but uses his/her personal account, and all properties are bought in his/her personal name.
- A customer applies for an early home finance settlement without a clear reason, or the settlement amount is paid by an unknown third party.
- A customer purchases and sells a property(ies) in a short time period, or a property address is noted in the customer transaction to be sold more than once.
- The relationship between the counterparties involved in the account is not clear, while the account credit and/or debit entails transactions related to real estate firms.
- The purpose of routing funds to/from own accounts held in different banks and the source of funds in those accounts are not clear, while funds are being utilized in purchasing a property(ies).
- The purpose of routing funds to/from multiple individuals and/or entities in different foreign countries is not clear, while the account's outward transactions are utilized in purchasing a property(ies).
- No business-related expenses, such as salary/wages and other business expenses, are noted in the real estate firm's account.
- Negative media or positive screening results on the customer or third parties involved in the transaction.
- A customer is identified in the public domain or screening result as an associate in a criminal act, accused of financial crime or linked to a PEP.

APPENDICES

LIST OF RISK INDICATORS BASED ON OUTCOMES OF RESEARCH AND STRATEGIC ANALYSIS SECTION'S PRODUCTS

Transactional Pattern

- A customer account is being used as a pass-through account, suggesting that a customer is acting as a front for multiple individuals.
- A customer's account transactions resemble purely a mule account's activities for third parties.
- A high value of ATM cash deposits from multiple individuals in different locations as well as cheque deposits from the customer's other own accounts, followed by immediate cash withdrawals, outward transfers, and high-value cheques to different real estate entities.
- Routing of funds without any business rationale.
- An internal self-transfer from the customer's other accounts abroad with no supporting documents on the source of funds.
- Substantial remittances in a short period of time from a family member(s) abroad to be utilized in real estate in the UAE.
- A customer account that is mainly funded via ATM cash deposits from multiple individuals in various locations in which the source of funds is unknown.
- An individual account (company owner) funded only through the company account and multiple unknown cash deposits.
- A payment service provider pays on behalf of an offshore company to purchase multiple properties in the UAE.
- Customer accounts receive significant amounts of cash deposits and/or inward remittances from unknown parties to be utilized in property purchases or installments.
- Credits into an individual account are only noted as manager cheques, while there is no information on the ultimate remitter of these funds and the beneficiary of the property.
- Funds are transferred to settle a credit card, followed by installments to purchase a property on behalf of a friend.
- Funds received are immediately spent whilst conducting various card payments toward real estate purchases or installments.
- A high volume of anonymous funding into the account from multiple unknown individuals and/or entities.
- High-value transactions pass through the account within a short period of time to be utilized in a real estate purchase.
- An individual account seems to be used as a funnel account through receiving multiple unknown deposits and remittances for real estate crowdfunding.
- A company (third party) lends or pays for a customer's property price while having no direct relation with the customer (borrower).

- The customer account credits are only through internal transfers from an individual(s) and/or sister company/counterparty(ies), and the same is used as outward transfers toward entities engaged in consulting services and real estate businesses.
- A personal account is used for routing business transactions.
- A customer uses his/her personal account for real estate business transactions without holding any license to practice such transactions/activities.
- Rapid movement of funds is observed in the customer's account, wherein the funds credited are immediately utilized.
- A huge surge in customer account turnover exceeds the declared income.
- A customer's transactions are not in line with the declared KYC profile of the customer.
- The account appears to be used as a funnel/pass-through account to route third party transactions.
- An unusual transactional pattern that does not match the customer profile, followed by investment in real estate.
- Customer transactions involve counterparties previously reported by the financial institution due to a suspicion of money laundering or criminal activities and are routed to multiple property developers to purchase properties.

Difficulty of Verification and Inconsistency of Information

- The source and legitimacy of funds remain unclear.
- The beneficial owner of the fund and property could not be ascertained.
- Difficulty in ascertaining the legitimate origin of the source of funds associated with a claimed sale/purchase transaction due to a lack of supporting documents (e.g., property sale and purchase agreement or title deed).
- The customer submits a suspected forged tenancy contract, title deed, sale and purchase agreement, or fabricated invoice and documentary evidence.
- A customer provides an invoice on a blank page which is not possible to authenticate against the suspected funds.
- A clear trade cycle cannot be established in the absence of complete shipment documents to support the source of claimed funds used in real estate transactions.
- Profile information on the property buyer (whether the customer is the buyer or seller) does not align with the volume of cash being paid for purchasing the property.

LIST OF ACRONYMS

ADGM	Abu Dhabi Global Market
AML	Anti-Money Laundering
AMLSCU	Anti-Money Laundering and Suspicious Cases Unit
CBUAE	Central Bank of the UAE
CFT	Countering the Financing of Terrorism
CoFIU	Chief of Financial Intelligence Unit
CSP	Corporate Service Provider
DFSA	Dubai Financial Services Authority
DPMS	Dealers in Precious Metals and Stones
DPMSR	Dealers in Precious Metals and Stones Report
ECOFEL	Egmont Centre of FIU Excellence and Leadership
EG	Egmont Group
EOCN	The Executive Office for Control and Non-Proliferation
DNFBP	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force
FFR	Funds Freeze Report
FI	Financial Institution
FIU	Financial Intelligence Unit
goAML	The Financial Intelligence Unit Reporting System
HRC	High Risk Country Transaction Report
HRCA	High Risk Country Activity Report
IEMS	Integrated Enquiry Management System
IRFI	Inward Request for Information
ISD	Inward Spontaneous Dissemination

LEA	Law Enforcement Authority
MENAFATF	Middle East and North Africa Financial Action Task Force
ML	Money Laundering
MOU	Memorandum of Understanding
NAMLCFTC	National Anti-Money Laundering and Combating Financing of Terrorism and Financing of Illegal Organizations Committee
ORFI	Outward Request for Information
OSD	Outward Spontaneous Dissemination
OSINT	Open-Source Intelligence
PF	Proliferation Financing
PNMR	Partial Name Match Report
PP	Public Prosecution
REAR	Real Estate Activity Report
RFI	Request for Information without Transactions
RFT	Request for Information with Transactions
SAR	Suspicious Activity Report
SD	Spontaneous Dissemination
SS	State Security
STR	Suspicious Transaction Report
TF	Terrorist Financing
UAE	United Arab Emirates
UAEFIU	UAE Financial Intelligence Unit
VASP	Virtual Asset Service Provider