FIU

وحدة المعلومات المالية
Financial Intelligence Unit

Organized Financial Fraud

Trends and Enablers

A Strategic Analysis Report

P.O.Box: 854, Al Karamah Street – International Tower, Abu Dhabi.

Phone No: +97126915599

Email address: uaefiu@uaefiu.gov.ae

Disclaimer

All findings and contents of this report are the property of the United Arab Emirates Financial Intelligence Unit (UAEFIU) or the concerned entities credited as the provider of the data employed in this document. You may not reproduce, distribute, duplicate, alter, create derivative works, or make any modification in any form to exploit or change this document's content and identity.

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

TABLE OF CONTENTS

LIST OF ACRONYMS

BEC	Business Email Compromise
FATF	Financial Action Task Force
FIs	Financial Institutions
FIUs	Financial Intelligence Units
IEMS	Integrated Enquiry Management System
IRFI	Inward Request for Information
ISD	Inward Spontaneous Dissemination
KYC	Know Your Customer
LEA	Law Enforcement Authority
ML	Money Laundering
OCGs	Organized Crime Groups
RFR	Reason for Reporting
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
UAE	United Arab Emirates
UAEFIU	UAE Financial Intelligence Unit
UNODC	United Nations Office on Drugs and Crime

EXECUTIVE SUMMARY

Fraud incidents involving more complex schemes and more sophisticated methods have been dramatically increasing worldwide. Advancement in technology is recognized as a significant enabler of this growing scale of fraud.

The Financial Action Task Force (FATF), in partnership with Interpol and Egmont Group (2023), highlighted how criminals exploit new technologies and vulnerabilities of modern financial services to deceive their victims and execute their scams. Moreover, they underlined that fraud activities are often employed by fraud syndicates and organized crime groups (OCGs) structured in different hierarchies and distributed into smaller groups. Fraud is also observed to be linked with other crimes, such as human trafficking, forced laboring, and money laundering.[1]

According to the UAE's Second National Risk Assessment of Money Laundering, fraud remains a major threat that contributes to money laundering activities in the UAE. In this report, the UAE Financial Intelligence Unit (UAEFIU) updates its previously identified fraud trends in 2022 based on a range of data, including a thorough analysis of approximately 10% of the total fraud-related Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) received from reporting entities from 01/07/2023 to 30/06/2024. The UAEFIU analyzed 879 suspicious reports (comprising 553 STRs and 326 SARs) to identify emerging fraud types, trends, and other fraud attributes and risk factors. Moreover, the UAEFIU examined fraud-related cases disseminated to law enforcement authorities (LEAs) or initiated by them via the Integrated Enquiry Management System (IEMS). These are in addition to intelligence reports exchanged with counterpart FIUs that involve fraud-related crimes and concerns.

From July 2021 to June 2024, the number of fraud-related STRs/SARs significantly increased, from 5,621 during July 2021–June 2022 to 5,993 during July 2022–June 2023, jumping to **9,403 STRs/SARs during July 2023 – June 2024**, showing a 57% increase on the previous year.

Furthermore, based on a questionnaire circulated to domestic and international financial institutions in the UAE, wherein 135 positive responses were received, including quantitative data from (41) institutions relevant to processed domestic and international repatriation[2] amounts, **financial loss during 2021 – 2023 is estimated to be AED1,244,117,187**. The value of domestic fund recall requests relevant to fraud increased over the past three years from AED256 million in 2021 to AED302 million in 2022 and then up to approximately AED340 million in 2023. Simultaneously, the value of international repatriation requests increased from over AED178 million in 2021 to AED201 million in

[1] FATF – Interpol - Egmont Group (2023) Illicit Financial Flows from Cyber-Enabled Fraud, FATF, Paris, France. Available at: www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyberenabled-fraud.html

[2] Repatriation within the context of this report refers to a request sent by a remitting bank (victim's account) to a beneficiary bank (suspected perpetrator or fraud accomplice's account).

2022 and then up to around AED261 million in 2023. In terms of volume, domestic and international repatriation increased in 2023 to more than triple in comparison to 2021.

The UAEFIU also organized five focus groups involving practitioners from financial institutions, LEAs, and prosecution to understand the extent of fraud incidents as a national concern and identify its attributes, including perpetrators' characteristics, used methods and locations of their operations. As a result of these groups' discussion and STRs/SARs analyses, it was perceived that many of the observed domestic fraud activities are conducted through OCGs with different hierarchies, using a mix of enablers such as money mules, social engineering, clone and shell entities, identity theft, and social media and digital platforms, albeit with different frequencies and scales.[3] Among said enablers, money mules are perceived to be the most critical concern in facilitating the collection and movement of fraud proceeds in the UAE, as well as money laundering.

With regard to fraud methods, the UAEFIU identified (15) prevalent fraud types and their associated patterns, wherein phishing and vishing were the dominant techniques used in reported fraud incidents, according to STRs/SARs analysis, questionnaire responses, and the examined international intelligence. Other types also included impersonation fraud, business email compromise, account takeover, investment fraud, advance fee scams, employment/task fraud, online scams, and occupational fraud. However, the frequency of these fraud types varied based on the analyzed data points.

Eventually, the UAEFIU developed 60 risk indicators to guide reporting entities in monitoring, detecting and reporting suspicious transactions and activities possibly related to fraud.

Moreover, practitioners in the field from fraud units and AML departments within financial institutions, LEAs, and prosecution underlined major challenges encountered in fraud prevention at the national level while suggesting a set of recommendations to address the observed increased scale of fraud incidents. It was also concluded that domestic and international cooperation, information sharing between competent authorities and financial institutions, and suspicious transaction reporting are all essential factors in countering fraud at global and national levels. These are in addition to public vigilance of fraud types and techniques.

The findings of this report, including identified challenges and proposed recommendations, should also be reviewed with the relevant FATF recommendations, including the following:

1. Ensuring the implementation of a risk-based approach to monitoring the emerging risks associated with fraud new techniques identified in this report (Rec.1).

2. Fostering national coordination among investigative authorities and exchange of information relevant to fraud, empowering the role of pro-active parallel financial investigation, freezing and seizing actions, including cases where fraud occurs outside the UAE (Rec.2 and 30).

[3] Despite that, it should not be understood that all fraud schemes are necessarily perpetrated by organized criminal groups.

3. Reviewing and applying proper customer due diligence measures according to the observed and identified fraud enablers and techniques (Rec.10).
4. Assessing and applying appropriate measures to tackle potential risks associated with new technologies and payment service providers, as identified in this report concerning fraud schemes related to not only cryptocurrencies but also instant payment and new digital channels (Rec.15 and 16). As reported by the FATF – Interpol - Egmont Group (2023), "the FATF is considering potential revisions to Recommendation 16 (on wire transfers) to take account of the recent and upcoming developments in the architecture of payments systems".[4]
5. Adherence to adequate and timely reporting of fraud-related suspicious transactions and activities to the UAEFIU (Rec.20).
6. International cooperation in all forms, including tracing, freezing, seizing and confiscation of fraud proceeds, in addition to the exchange of intelligence spontaneously and upon request (Rec.38 and 40).

[4] FATF – Interpol - Egmont Group (2023), footnote 17 indicated in p.27.

Utilized Data		Covering Period 01/07/2023 to 30/06/2024	
879 STRs/SARs	59 Technical reports disseminated to LEAs and prosecution	41 Cases disseminated to LEAs	176 International intelligence reports
135 Responses from FIs through a questionnaire	Repatriation amounts from (41) FIs	Findings from (5) focus groups	Public international records and reports

Key Findings

Repatriations Estimate (2021–2023)

AED 765,082,030 Domestic repatriation	AED 479,035,157 International repatriation	AED 1,244,117,187 Estimated financial loss
20,854 No. Fund recall requests	4,669 No. International requests	

Fraud Enablers

Money mules	Clone and shell entities	Identity theft	Fraudulent documents
Social engineering	Digital platforms	Social media	Advanced technology

Prevalent Fraud Types

Phishing, Vishing, and Smishing	Impersonation fraud	Business e-mail compromise (BEC)	Fake online marketplace and shopping scams
Advance fee scams	Account takeover	ATM/card skimming fraud	Employment/task fraud
Investment fraud	Application fraud	Loan and insurance fraud	Occupational fraud

1. INTRODUCTION

Fraud is a serious crime and a global concern that affects individuals, businesses, and governments worldwide. It has a significant social and economic impact that requires constant collaboration among competent authorities, law enforcement, and financial institutions to detect and prevent fraud crimes worldwide.

There is no standard legal definition of fraud, whereas it is often defined from the perspective of acts and behaviors that constitute fraud, or the activities associated with its schemes.[5] Fraud is conceived as an intentional unlawful act of deception conducted by a party (perpetrator) to obtain unauthorized profit or gain, typically involving financial or material benefits and causing prejudice and loss to another party (victim).

The Association of Certified Fraud Examiners (ACFE) defines fraud as "*any activity that relies on deception in order to achieve a gain. Fraud becomes a crime when it is a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment*."[6] Simultaneously, the World Bank Group (2014) defines fraudulent practice as "*any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation*."[7]

In the UAE, fraud is a punishable criminal offence as per the UAE Penal Code on "*anyone who, by using fraudulent practice, assuming a false name or capacity, takes possession for himself or for others of any movable property or written instrument, or obtains any signature on such instrument, the cancellation or destruction thereof or an amendment thereto, whenever it is intended to deceive the victim and bring him to hand over such things*" (Article 451 of Federal Decree Law No. 31 of 2021, Promulgating the Crimes and Penalties Law).

The FATF (2022) emphasized four major predicate offenses that were identified as major contributors to money laundering in two thirds of countries that were subject to the 4th round of Mutual Evaluation: drug trafficking (18%), followed by corruption (16%), fraud and tax crimes (with 15% each).[8]

In the Middle East and North Africa (MENA), fraud risk and trends were found to be consistent with those in other regions, particularly phishing, impersonation fraud, and online scams, which are

[5] UNODC (2024b) "Organized Fraud: Issue Paper". Available at: https://www.unodc.org/unodc/es/organized-crime/intro/implementing-untoc/organized-fraud.html

[6] ACFE (no date) What is fraud. Available at: https://www.acfe.com. ACFE's fraud definition here is adopted from Black's Law Dictionary.

[7] World Bank Group (2014) Fraud and corruption awareness handbook: a handbook for civil servants involved in public procurement. Available at: http://documents.worldbank.org/curated/en/309511468156866119/Fraud-and-corruption-awareness-handbook-a-handbook-for-civil-servants-involved-in-public-procurement

[8] FATF (2022) Report on the State of Effectiveness and Compliance with the FATF Standards. Available at: https://www.fatf-gafi.org/en/publications/Fatfgeneral/Effectiveness-compliance-standards.html

recognized as high threats (FATF, 2023).[9] According to the UAE's Second National Risk Assessment (2024), fraud remains a major threat and is identified as a high-risk predicate offense that leads to money laundering.

FATF – Interpol – Egmont Group (2023) underlined cyber-enabled fraud as a growing transnational organized crime. Furthermore, cyber-enabled fraud was found to be linked to other crimes by organized groups, including human trafficking and forced labor by abusing vulnerable individuals to operate fraud call centers, in addition to hacking to obtain personal information and the utilization of forged and fraudulent documents.[10]

Consequently, the FATF emphasized the necessity for jurisdictions to consider more dynamic initiatives to encourage victim reporting and enhance suspicious transaction reporting, in addition to applying vital and holistic domestic cooperation mechanisms, as well as multilateral ones. [11]

It is estimated in a recent study (Nasdaq, 2024) that over three trillion dollars of illicit funds flowed through the international financial system in 2023. Said figure included an estimation of fraud losses that reached $485.6 billion globally, containing $442 billion in losses from payment, cheque, and credit card fraud, and consumer scams totaling $43.6 billion.[12]

Still, identifying the actual extent of fraud cost and severity remains a challenge due to fraud-inherent characteristics associated with its schemes, which rely on deception, the concealment of funds, and the recruitment of third parties, in addition to incidents underreported by victims. Nevertheless, as highlighted in this report, there is a global acknowledgement that fraud tactics have been shifted to more sophisticated schemes driven by advanced technology, vulnerabilities of the global financial climate, and the growing number of new instant payment methods and service providers.

While it is still challenging to obtain a complete picture of fraud cost and the extent of the problem, data utilized in this report, including a questionnaire circulated to domestic and international financial institutions in the UAE, showed that fraud remains a major concern for financial institutions in terms of cost and risk management.

The UAEFIU issued a typology report in 2022 highlighting fraud trends and schemes in the UAE (Fraud Crimes, Trends and Typologies, 2022). This report updates previous findings and provides a comprehensive analysis of figures and information relevant to fraud schemes. It adds different insights and observations to develop an understanding of emerging risks and the shift of organized financial fraud to more complex and innovative schemes.

[9] FATF – Interpol - Egmont Group (2023), Illicit Financial Flows from Cyber-Enabled Fraud, FATF, Paris, France. Available at: www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyberenabled-fraud.html

[10] Cyber-enabled fraud refers to fraud schemes that are facilitated through the use of technology or internet.

[11] FATF – Interpol - Egmont Group (2023).

[12] Nasdaq (2024) Global financial crime report. Available at: https://www.nasdaq.com/global-financial-crime-report

2. OBJECTIVES

As part of the Strategic Analysis Plan (SAP) and in line with the UAEFIU's efforts to address and identify patterns and typologies of financial crime, the UAEFIU is delivering its second report on fraud for the following purposes:

- Update previously identified fraud types and identify any emerging patterns across financial and non-financial sectors;
- Explore the potential link between identified fraud patterns and the involvement of organized crime groups;
- Identify fraud attributes, including involved nationalities, jurisdictions, legal persons, and perpetrator characteristics, among others;
- Explore the magnitude of fraud losses and reported fraud-related suspicious reports;
- Update the previous list of risk indicators;
- Highlight current fraud detection and prevention challenges and recommend possible solutions to policy and decision makers;
- Promote current awareness among the involved actors in fraud investigation and prevention.

3. METHODOLOGY

This report extends previously identified fraud crime patterns and typologies and addresses possible fraud attributes and potential monitoring gaps that enable fraudsters to execute their schemes. Furthermore, data utilized in the report draw a perception of the magnitude of fraud in terms of financial loss, frequency and threat. Nevertheless, the analysis results indicated in this report should be deemed as a fraction of the fraud scale, while constructing the complete picture requires the availability of further national and international data.

This report is compiled using three different approaches:

3.1. Available data within the UAEFIU's databases (covering a period of one year from 01/07/2023 to 30/06/2024), including the following:

i. Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) related to fraud received through the UAEFIU's reporting system during the study period.

ii. Fraud cases disseminated by the UAEFIU to law enforcement authorities (LEAs).

iii. Fraud cases initiated by LEAs and public prosecution (PP) through the Integrated Enquiry Management System (IEMS).[13]

iv. International intelligence received by the UAEFIU from counterpart FIUs, whether spontaneously or by request.

3.2. Questionnaire

A questionnaire of quantitative and qualitative questions on fraud was circulated to domestic and international financial institutions in the UAE (banks, money service businesses (MSBs), and insurance and finance companies), which aimed to:

i. Estimate the scale of fraud transactions processed through the UAE financial sector by collecting the volume and value of repatriation amounts over the past three years, 2021–2023, including successful repatriation.

ii. Develop an understanding of the most frequently observed fraud types, enablers, and payment methods.

iii. Identify major fraud detection and prevention challenges, as well as suggested solutions.

Positive responses were received from **135 financial institutions** — excluding responses that showed no occurrence of fraud or inapplicability — and analyzed to reach a statistical inference.

3.3. Focus Group(s)

The UAEFIU organized **five focus groups** involving fraud detection and investigation practitioners to discuss two themes designed for this report. Each group had 10 members, including fraud units and AML departments within financial institutions, fraud investigators from police departments, public prosecutors, and operational and strategic senior analysts from the UAEFIU. The first theme focused on understanding the problem and its extent, addressing specific attributes such as the reasons for the increase in fraud, the possible perpetrators, and where and how they operate. The second theme was dedicated to solving the problem by discussing fraud prevention challenges and potential solutions. Conclusions drawn from the five focus groups were verified with the above-indicated data and integrated into this report.

4. UNDERSTANDING FRAUD DEVELOPMENT AT THE GLOBAL LEVEL

Different international organizations recognized the growth in financial fraud in terms of scale and sophisticated methods utilized by fraudsters as technology and digital finance have significantly

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

evolved over the past years (e.g. UNODC, 2024a, 2022; Interpol, 2024; EUROPOL, 2023; FATF – Interpol – Egmont Group, 2023).[14] Among the indicated fraud techniques, phishing, business email compromise (BEC), investment fraud, advance fee payment, and romance and impersonation fraud were the most prevalent techniques used globally and regionally.

In the US, the US Internet Crime Complaint Center received roughly 758,000 complaints in 2023 concerning internet scams involving many individuals globally (IC3, 2023).[15] Said complaints were associated with significant financial loss that increased from $3.5 billion in 2019 to $12.5 billion in 2023. Among the reported scams in 2023, 21,489 BEC complaints were received with an estimated loss of over $2.9 billion, and impersonating customer support and governmental authorities caused over $1.3 billion in losses. Moreover, investment fraud was the most prevalent scheme, with an estimated 38% increase in financial loss, rising from $3.31 billion in 2022 to $4.57 billion in 2023, including a 53% increase in relation to investment fraud with a cryptocurrency reference to reach $3.96 billion in 2023.

Within the same context of misusing cryptocurrency in investment fraud, a recent study (Griffin and Mei, 2024) examined data from pig butchering victim reports in the US and traced over 4,700 scammed addresses, showing that criminals misused the virtual currency sector by swapping between tokens and transactions across blockchains using DeFi smart contracts, as well as deposits to centralized crypto providers below the threshold.[16] More importantly, the study highlighted that this type of fraud had a larger scope in terms of the involved amounts than did the typical phishing scams and that criminals moved approximately $75.3 billion into suspicious accounts from January 2020 to February 2024 through crypto exchanges outside of the US.

Similarly, the Interpol Fraud Assessment (2024) affirmed that cryptocurrency and their service providers are globally misused in investment and romance fraud. Furthermore, the ACFE (2024) reported that 47% of 1,921 occupational fraud cases received from 138 countries showed that perpetrators converted their stolen assets into cryptocurrency.[17]

In the UK, fraud crimes remain significant and represent over 40% of reported crimes, with the estimation of payment scams reaching £1.17 billion in 2023 associated with 2.97 million cases

[14] UNODC (2024a) Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape. Available at: https://www.unodc.org/roseap/en/2024/10/cyberfraud-industry-expands-southeast-asia/story.html; UNODC (2022) Digest of Cyber Organized Crime. Available at: https://sherloc.unodc.org/cld/en/st/resources/publications/Digest-of-Cyber-Organized-Crime; INTERPOL (2024) Interpol global financial fraud assessment. Available at: https://www.interpol.int/en/Resources/Documents#Publications; EUROPOL (2023) The other side of the coin. Available at: https://www.europol.europa.eu/publications-events/publications/other-side-of-coin-analysis-of-financial-and-economic-crime; FATF – Interpol - Egmont Group (2023).

[15] Internet Crime Complaint Center report (2023) Federal Burau of Investigation: Internet Crime Report 2023. Available at: https://www.ic3.gov/

[16] Griffin, J. M. and Mei, K. (2024) How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering, University of Texas at Austin. Available at http://dx.doi.org/10.2139/ssrn.4742235

[17] ACFE (2024) Occupational Fraud 2024: A Report to the Nations. Available at: https://legacy.acfe.com/report-to-the-nations/2024/

processed through unauthorized and authorized fraud.[18] Fraud loss from authorized push payments (APPs) was estimated to be £459.7m, while losses from unauthorized fraudulent transactions reached £708.7m.

In Australia, according to the Australian Payments Network (2024), the total value of card fraud alone increased by 32% in 2023 on the previous year to reach $762m, including card-not-present (CNP) fraud, which rose by 33% to $688m, representing 90% of all card fraud cases.[19] Within the same context of CNP, it is noteworthy to recall one of the cases — known as *Unlimited Operations* — shared by the UNODC in its published report (Digest of Cyber Organized Crime, 2022) about how a transnational OCG utilized this scheme, involving UAE banks. As reported, the criminal group managed to obtain debit card data and remove cards' withdrawal limits by hacking into international financial institutions' networks. Then, cards were shared among different runners in over 20 countries to withdraw the money through ATMs at a coordinated date and time.[20]

With regard to global fraud cost, as demonstrated by the World Economic Forum (2024), scammers acquired more than $1 trillion from victims around the world in 2023.[21] Based on another dataset that collected insights from 49,459 individuals from 43 countries, it was concluded that 78% of participants experienced at least one scam in 2022.[22] The dominant types included shopping scams (27%), followed by identity theft (21%) and investment fraud (20%), underlining that phishing (61%) and smishing— SMS phishing (58%) remain the top channels in facilitating these scams.

Another study (Nasdaq, 2024) estimated fraud losses in Europe, the Middle East, and Africa (EMEA) to be $113.1 billion in 2023. The most prevalent fraud types in said region were payment fraud ($94 billion), followed by advance fee scams ($8.2 billion), credit card fraud ($3.1 billion), and cyber-enabled scams ($3.1 billion). At the same time, the UNODC (2024a) estimated fraud financial losses from scams in East and Southeast Asia to be between $18 billion and $37 billion in 2023, which were mostly associated with OCGs.[23]

In terms of institutional cost, it is estimated that organizations lose at least 5% of their annual revenue to fraud, according to the Association of Certified Fraud Examiners (ACFE, 2020).[24] From the point of view of another study, it was estimated that global fraud costs could reach over $5.13 trillion annually

[18] UK Finance (2024) Annual fraud report. Available at: https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2024

[19] Australian Payments network (2024) Payment Fraud Report. Available at: https://www.auspaynet.com.au/resources/fraud-statistics/2023-Calendar-year

[20] UNODC (2022).

[21] World Economic Forum (2024) Pig-butchering' scams on the rise as technology amplifies financial fraud, INTERPOL warns. Available at: https://www.weforum.org/stories/2024/04/interpol-financial-fraud-scams-cybercrime/

[22] Global Anti-Scam Alliance (2024) The Global State of Scams Report (2023). Available at: https://www.gasa.org/downloads?scrollToProduct=global-state-of-scams-report-2023

[23] UNODC (2024a).

[24] ACFE (2020) Report to the Nations. Available at: https://legacy.acfe.com/report-to-the-nations/2020/

by calculating not only the actual losses from fraud incidents but also the cost spent on fraud solutions, systems and resources.[25]

Ultimately, the cost and risk of fraud remain prevalent, as per financial institutions' perceptions. According to a study that surveyed 264 risk and compliance professionals from different regions (NAMER, APAC, EMEA, and LATAM)[26] in 2023, 65% of those professionals anticipated an increase in fraud and money laundering in 2024 and underlined that identifying emerging fraud schemes is a top priority.[27]

For all of that, it is crucial to understand who are the actors and perpetrators in the growing global fraud schemes and how fraud schemes work. From the point of view of an academic study, the criminal fraud cycle could be divided into four stages: victim selection techniques, perpetration strategies, detection avoidance strategies, and securing the gains.[28]

FATF – Interpol – Egmont Group (2023) underlined that fraud is often performed by an organized network of co-perpetrators and varies between highly and loosely structured groups. Said organized networks (especially crime syndicates) function in hierarchical structures but also in decentralized cells with members joining and leaving as needed.[29] Roles played by organized co-offenders are often divided into recruiting financial professionals to develop complex fraud schemes, demographical targeting of victims, and laundering the proceeds of fraud through networks of individuals, shell companies, and legitimate businesses.[30] An example of cyber-enabled fraud criminal structure is indicated in **Diagram 1** below.

Similarly, EUROPOL (2023) underlined the engagement of mid-level management layers and experts from banking, law, finance, and IT in fraud schemes and professional money laundering of fraud proceeds. Furthermore, the UNODC (2024a) underlined that eventually OCGs would require the involvement of professional money laundering in employing different innovative methods to launder the proceeds of fraud, and the utilization of new business models and technologies.

Advanced technology tools integrated into OCG operations included the use of generative AI, deepfakes, automated phishing attacks, designing fake online profiles, and real-time multi-language scripts. Methods of laundering the proceeds of fraud were noted to target unregulated and vulnerable sectors, including underground banking, unregulated casinos, and illegal online gambling using cryptocurrency provided by high-risk virtual asset service providers.[31]

[25] SEON (no date) The Total Opportunity Cost of Fraud is Bigger Than You Think. Available at: https://seon.io/resources/total-cost-of-fraud/

[26] NAMER stands for North America and Latin America, APAC for Asia-Pacific, EMEA for Europe, the Middle East and Africa, LATAM is for countries in Latin America.

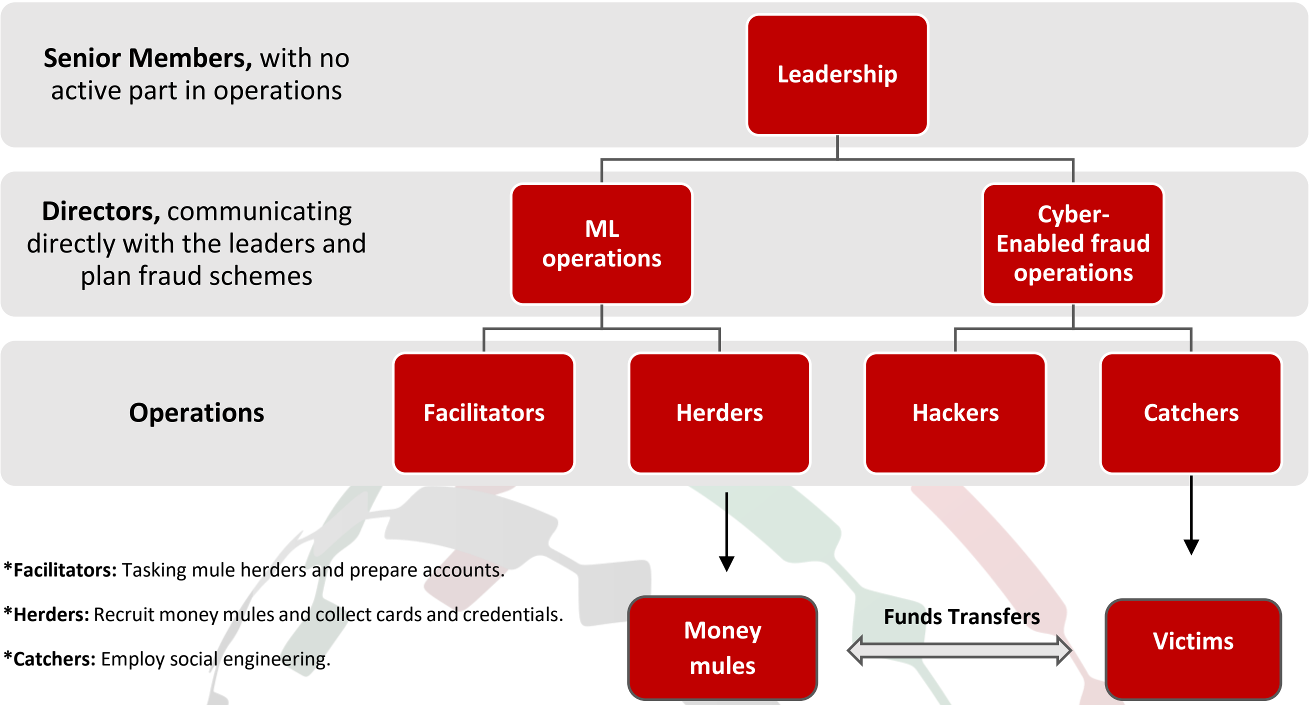
[27] Unit 21 (2024) State of fraud and AML Report, Volume 02. Available at: https://go.unit21.ai/download-state-of-fraud-and-aml-2023

[28] Button, M., Lewis, C., and Tapley, J. (2009) "Fraud typologies and the victims of fraud: literature review". National Fraud Authority.

[29] FATF – Interpol - Egmont Group (2023).

[30] INTERPOL (2024).

[31] UNODC (2024a).


Senior Members, with no active part in operations
Leadership
Directors, communicating directly with the leaders and plan fraud schemes
ML operations
Cyber-Enabled fraud operations
Operations
Facilitators
Herders
Hackers
Catchers
Money mules
Funds Transfers
Victims

***Facilitators:** Tasking mule herders and prepare accounts.

***Herders:** Recruit money mules and collect cards and credentials.

***Catchers:** Employ social engineering.

Diagram 1 - Source: FATF – Interpol - Egmont Group (2023, p.12)

It was concluded that these methods would potentially spill over to different jurisdictions and regions chosen by OCGs. This is in addition to emphasizing the shift of criminals' behavior to purchasing essential components such as malware coding and software or personal information from service providers in unregulated sectors, instead of obtaining these requirements themselves, which ultimately enable cyber-fraud at a greater speed and volume.[32] Still, as underlined by the UNODC (2024b), the understanding of the intersection between fraud and organized crime remains obscure, especially with the involvement of cybercrime, white-collar crime, and money laundering.

5. PERCEPTION OF FRAUD MAGNITUDE AT THE NATIONAL LEVEL

According to the UAE's Second National Risk Assessment of money laundering, foreign and domestic fraud remain a major threat contributing to money laundering activities in the UAE.
Data utilized in this report underline that the UAE is experiencing a surge in fraud incidents and scam activities, enabled by the rise of advanced technology, the growth of instant and digital payment channels, and sophisticated cybercrime schemes. The following refers to the scale of fraud-related suspicious reports, cases disseminated and referred from LEAs, and international requests of

[32] Ibid.

information exchanged with counterpart FIUs, in addition to (domestic and international) repatriation amounts during 2021 – 2023, as collected from financial institutions in the UAE through a questionnaire.

5.1. Perception of fraud scale in the UAE

Discussion amongst focus groups underlined that actors involved in fraud investigation in the UAE (FIs, UAEFIU, LEAs, and prosecution) are observing an increase of fraud cases on a large scale, in terms of not only volume but also the frequency of fraud types, leading to new emerging trends. Simultaneously, fraud is often observed as a predicate offense for money laundering activities.

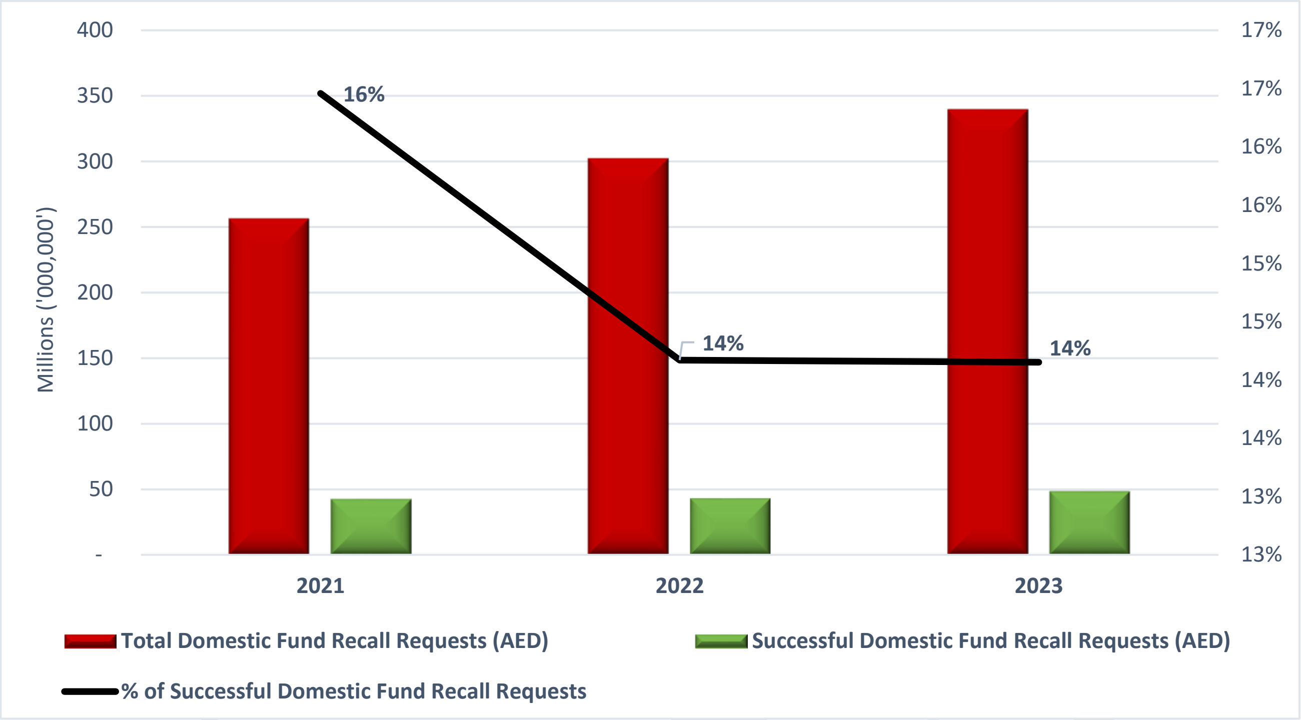
Participants underlined different global and domestic factors that could be a cause of such an accelerated scale. Examples of these factors included: the swift shift to digital banking following COVID-19, the simplicity and swiftness of online banking, the advancement of technology such as AI tools and deepfake technology, and the wide spread of social media and digital platforms. These are in addition to the vulnerability of instant payment channels, payment wallets, data safeguards, the lack of verification and authentication tools and public awareness.

The focus groups also perceived that the scale of fraud is associated with other factors such as economic factors (e.g., unemployment rate and economic uncertainty in some regions), social and cultural factors, and industries' regulatory frameworks and business models.

5.2. Data obtained through questionnaire

Data obtained from (41) financial institutions in the UAE showed the increased value of domestic fund recall requests relevant to fraud over the past three years, from 2021 to 2023. As indicated in **Chart 1**, fund recall requests increased from AED256 million in 2021 to AED302 million in 2022 and then up to approximately AED340 million in 2023. On the other hand, successfully repatriated amounts of fraudulent funds slightly decreased from 16% in 2021 to 14% in 2023. The total financial loss for said **(41) reported financial institutions** from domestic funds recall requests is estimated to be **AED765,082,030** for the three-year period of 2021 – 2023.

Chart 1: *Overview of received domestic fund recall requests during 2021–2023*



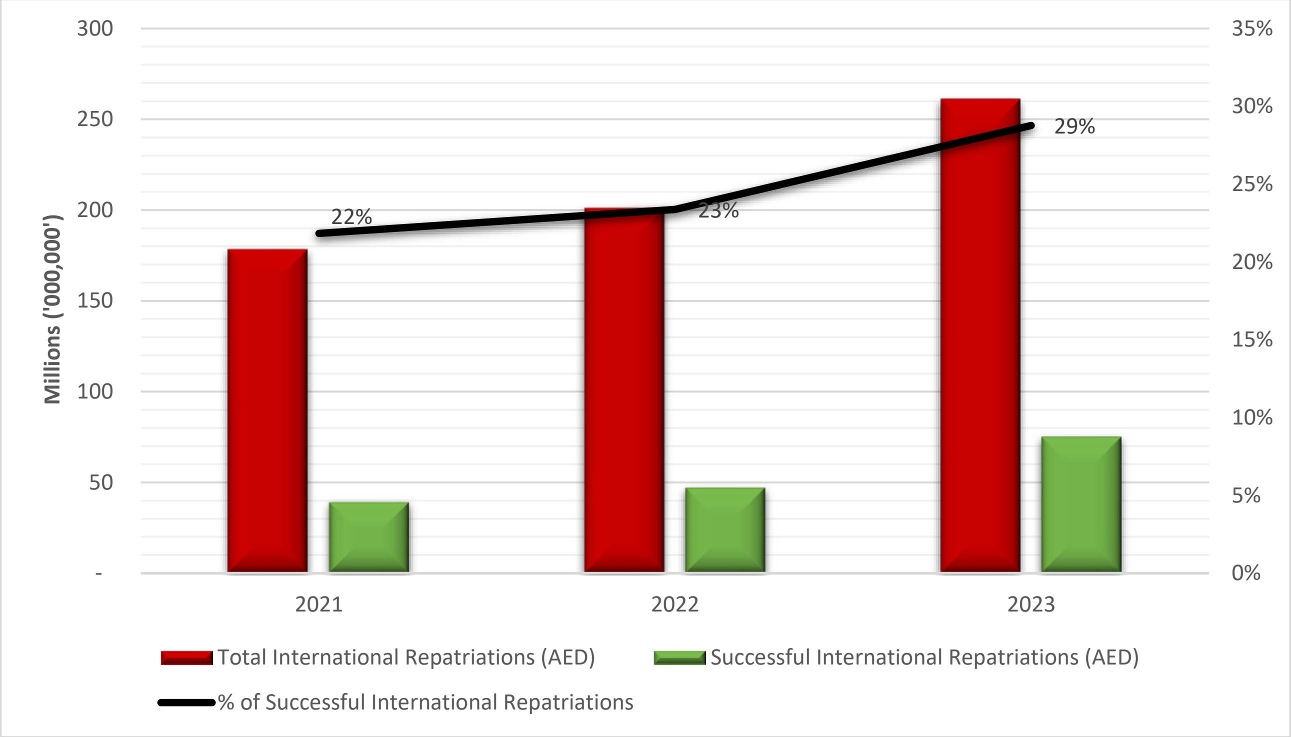
With regard to volume, the number of domestic repatriation requests had increased to more than triple over the past three years, from 2,763 in 2021 to 8,647 requests in 2023, with a low success rate from around 9% in 2021 to 6% in 2022 and then escalating to more than 14% in 2023 (**Table 1**).

Table 1: *Number of fund recall requests*

2021		2022		2023	
No. of Repatriation Requests Received	No. of Successful Repatriations	No. of Repatriation Requests Received	No. of Successful Repatriations	No. of Repatriation Requests Received	No. of Successful Repatriations
2,763	**241**	**9,444**	**604**	**8,647**	**1,261**

As indicated in **Chart 2**, the value of repatriation requests increased from over AED178 million in 2021 to AED201 million in 2022 and then up to approximately AED261 million in 2023. At the same time, successfully repatriated amounts of international requests increased from 22% in 2021 to 29% in 2023. The total financial loss for said (41) reported financial institutions from international repatriation requests is estimated to be **AED479,035,157** for the three-year period of 2021 – 2023.

Chart 2: *Overview of received international repatriation requests during 2021–2023*



With regard to volume, the number of international repatriation requests, similar to the domestic ones, had increased to more than triple over the past three years, from 888 in 2021 to 2,809 requests in 2023, with a fluctuating success rate from 16% in 2021 to around 10% in 2022 and then surging to more than 50% in 2023 (**Table 2**).

Table 2: *Number of international repatriation requests*

2021		2022		2023	
No. of International Repatriation	No. of Successful Repatriations	No. of International Repatriation	No. of Successful Repatriations	No. of International Repatriation	No. of Successful Repatriations
888	143	972	93	2,809	1,419

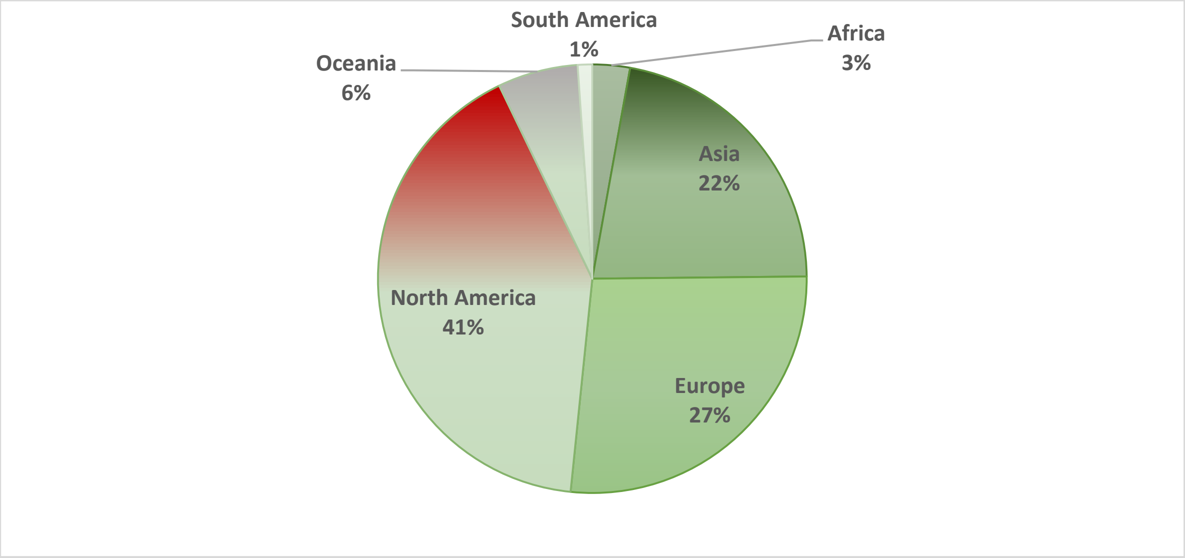
The tables below provide further details of the received international repatriation requests by jurisdiction in terms of their estimated value and volume.

Table 3 below and **Chart 3** provide further details of the received international repatriation requests by region in terms of their estimated value and volume.

Table 3: *Volume and value of international repatriation requests by region during 2021–2023*

Region	No. Repatriation Requests	No. Successful Repatriations	Total Amount Involved (in AED)	Total Amount Successfully Repatriated (in AED)	Success Rate
Africa	186	137	18,098,125	4,429,790	24%
Asia	1187	623	140,843,831	60,464,840	43%
Europe	1523	496	171,418,738	43,761,624	26%
North America	1413	263	263,867,809	47,634,076	18%
Oceania	248	42	38,764,680	956,633	2%
South America	112	94	6,998,552	3,709,616	53%
Grand Total	**4,669**	**1,655**	**639,991,735**	**160,956,578**	25%

Chart 3: *Value of international repatriation requests by region during 2021–2023*

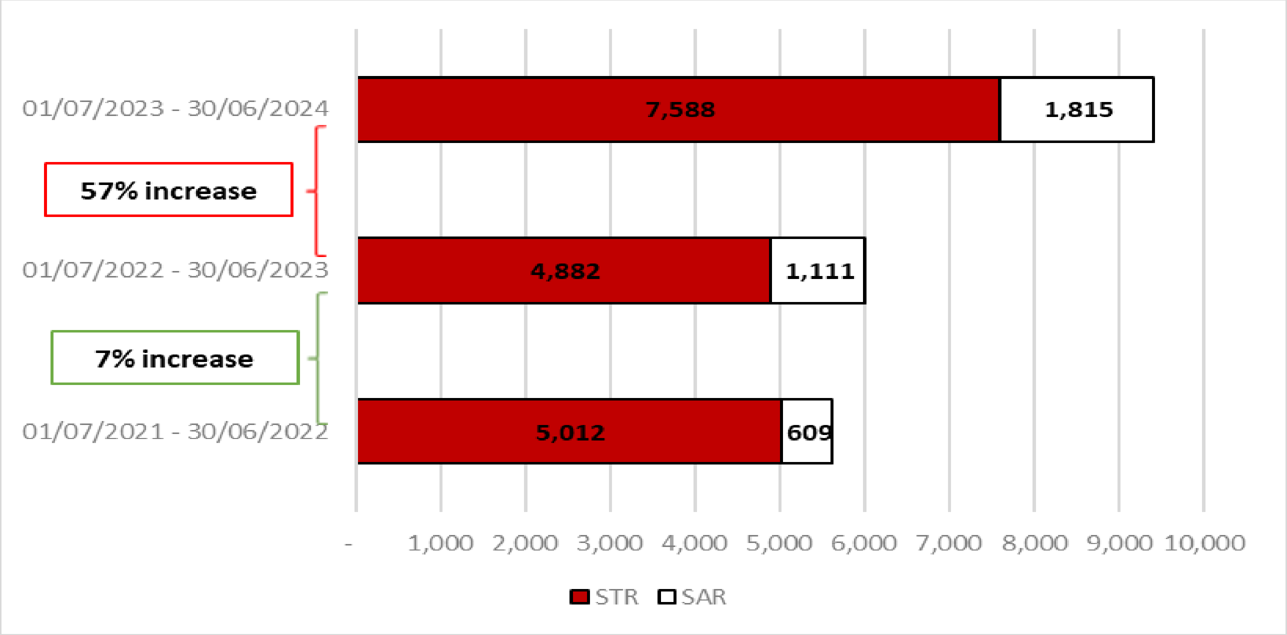


5.3. Data available with the UAEFIU

The UAEFIU received **9,403 STRs/SARs** related to possible fraud activities during the one-year review period from **01/07/2023 to 30/06/2024**. An in-depth strategic analysis was conducted on around **10%** of the total received reports (**879 reports, comprising 553 STRs and 326 SARs**) to identify emerging fraud types, trends, and other fraud attributes and risk factors.

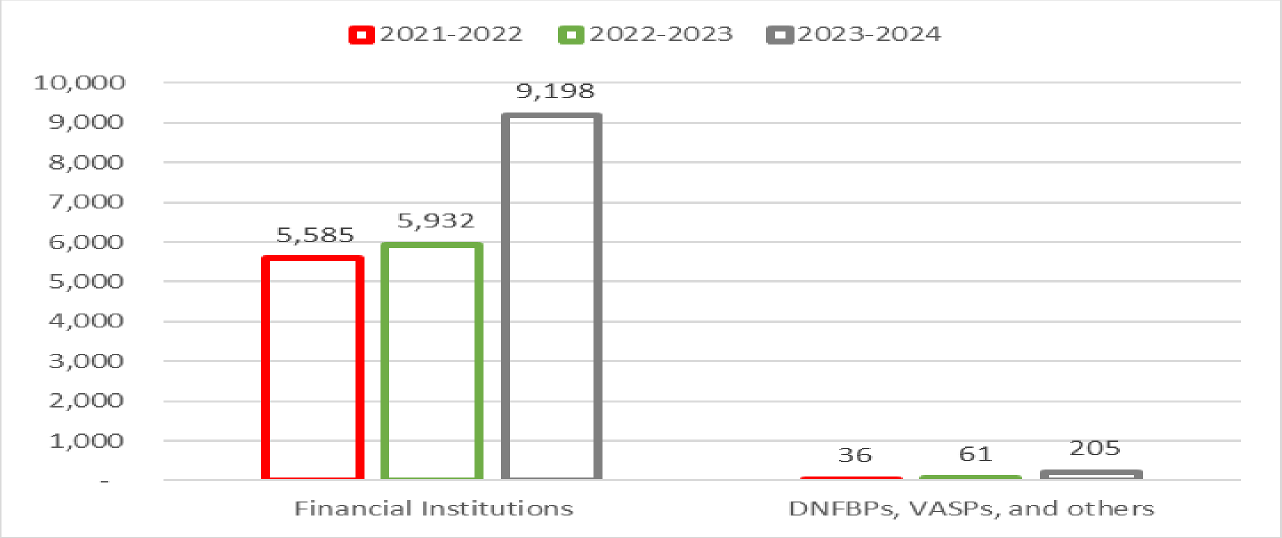
The below **Chart 4** demonstrates the increasing volume of fraud-related STRs/SARs received from all reporting entities over the past three years.

Chart 4: *Figures of received fraud-related STRs/SARs from July 2021 to June 2024*



The below **Chart 5** demonstrates a breakdown of received reports according to the reporting entities'[33] category over the three years.

Chart 5: *Figures of fraud-related STRs/SARs by reporting entity*



[33] A practice of reporting suspicions as fraud-related incidents in 'bulk' was observed in some domestic banks. Hence, the figures do not represent the actual volume of fraud incidents that occurred within the reporting entities.

The UAEFIU disseminated **41 cases** concerning fraud (be it by predicate offense or typology) to local LEAs during the reviewed period, compared to 30 cases in the previous year, noting that a case may combine one or more suspicious reports. These cases were mainly related to different types of cyber-enabled fraud, including phishing, identity theft, online scams, and business email compromise.

Simultaneously, during the same reviewed period, the UAEFIU received **450 cases initiated by LEAs** related to fraud, **associated with 1,750 requests**, via the IEMS. An in-depth analysis was conducted on (25) cases, where the UAEFIU provided **(59) technical reports** in this regard, **involving 46 individuals and 13 legal entities**. Analysis of said reports indicated a high credit turnover of suspected perpetrator accounts with a total amount of AED 2,315,903,880, noting that this amount included business activities relevant to legal entities, such as construction, real estate, and investment activities. Nevertheless, at the time of analysis, the total available amount in the accounts was AED 22,184,454, representing 0.96% of the total turnover. Based on the UAEFIU recommendations and investigation results, a total of **AED 12,173,969** was frozen.

In relation to international intelligence, the UAEFIU exchanged **325 intelligence reports** with counterpart FIUs, possibly related to fraud and other relevant offenses, during the reviewed one-year period. For the purpose of this report, **80%** of all the incoming (received) intelligence reports have been thoroughly analyzed, comprising (**116 Inward Requests for Information ('IRIs') and 60 Inward Spontaneous Disseminations ('ISDs')**) to assess current fraud types in the UAE linked to transnational schemes or international organized fraud. In total, the reviewed sample included **five cases disseminated to the LEAs.**

6. UNDERSTANDING FRAUD ATTRIBUTES AT THE NATIONAL LEVEL

The following information underlines observed fraud features and attributes of analyzed data available and obtained from the UAEFIU stakeholders, including reporting entities.

6.1. Possible perpetrators

Discussion amongst the focus groups illustrated fraudsters' understanding of payment structures and financial institutions' vulnerabilities. Similar to what is observed globally, domestic fraud activities are perceived to be conducted through a network/organized crime with different hierarchies. These criminal networks are usually well organized and complex, consisting of operational masterminds and perpetrators who use third party accounts (including money mules) to receive and layer the funds. The mastermind of the fraud scheme would provide these third parties with a designed informative script so that they can convince their victims. Nevertheless, it should be noted that not all fraud incidents are necessarily perpetrated by organized criminal groups, as indicated later in fraud type (Section 8).

It is also understood from the focus group discussion and other data, that fraudulent activities are committed domestically, but foreign fraudulent proceeds are also routed to the UAE's financial institutions for money laundering. Such an observation is also consistent with the global understanding that recruited money mules and launderers of fraud proceeds are not necessarily located in the same country as that of the fraudsters. [34]

A sample analysis of 10% (879 STRs/SARs) of the total received fraud-related reports (9,403 STRs/SARs) showed that **90% of the identified possible perpetrators are natural persons, while only 10% are legal persons**.

Below are the characteristics of these natural and legal persons as per the analysis.

Natural persons

Ninety percent of the analyzed STRs/SARs sample involved natural persons as suspected perpetrators. **Table 4** and **Chart 6** illustrate the age group and professions of involved individuals in suspicious reports.

Table 4: *Age group of involved individuals in STRs/SARs*

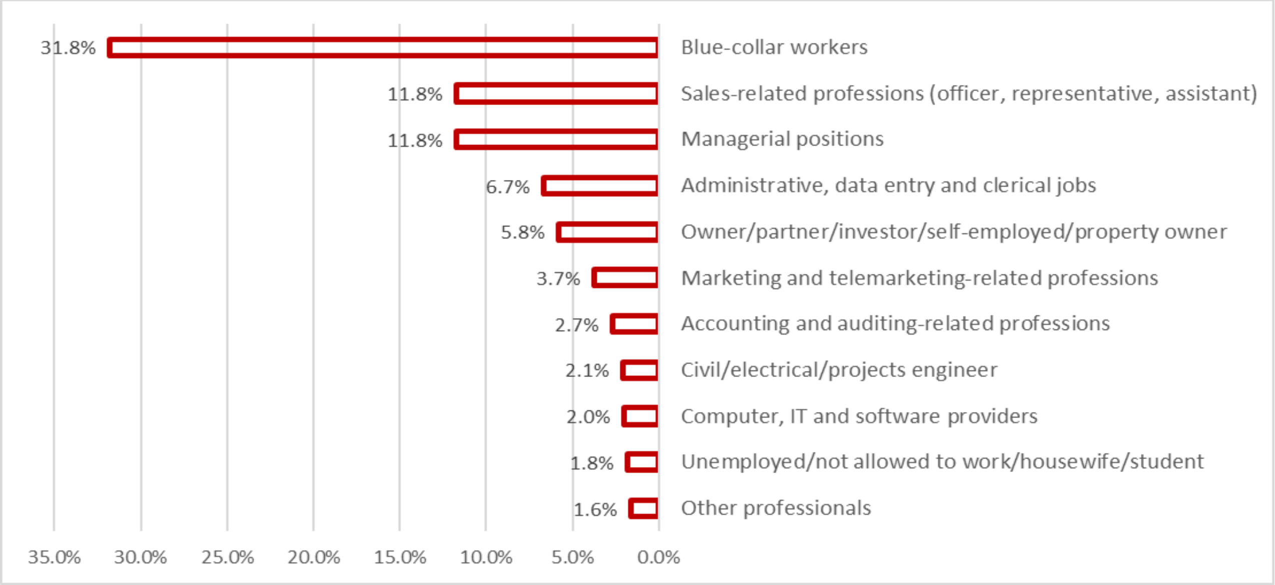
Age Group	No. of Subject Individuals	Percentage
19-20 years old	4	0.4%
21-30 years old	**356**	**32%**
31-40 years old	**361**	**32%**
41-50 years old	154	14%
51-65 years old	44	4%
Unknown	201	18%

As illustrated, 64% of the suspected individuals were noted to be in their early 20s to 40s. Said age groups (often referred to as Millennials and Gen Z) imply the involved individuals' knowledge of and familiarity with modern technology channels and systems, including social media, digital platforms, and online and instant payment methods, which could be exploited for cyber-enabled fraud. However, it should also be noted that the indicated age groups are relevant to STRs/SARs involving some suspected subjects who are not necessarily the main perpetrators or the controller/ architecture of fraud schemes (e.g., the case of mule accounts/blue collars, which were significant in the sample, as shown in the following chart).

[34] (EUROPOL, 2023).

Chart 6 below shows the main professions of individuals involved in the examined sample of (STRs/SARs), including blue collar jobs, white collar jobs, and other professions. [35]

<u>Chart 6</u>: *Professions of suspected individuals in STRs/SARs*



The analysis revealed that among all involved individuals, the first dominant category of professions was blue collars, contributing 32% of the examined sample. Among them, **19% were identified as workers** in building and construction, with declared salaries ranging from **AED 1,000 to AED 6,500**, **4% were cleaners**, **3% were drivers, and the remainder were under different kinds of blue-collar jobs**. The second and third dominant professions observed in the sample were relevant to the **sales field and managerial positions** — mostly involved in forgery and application fraud, representing **12% each**. It is worth highlighting that many of the indicated professions in the chart above might have direct access to customers' personal information that could be misused in fraudulent activities such as sales and marketing. However, no direct link was found based on examining STRs/SARs that could affirm whether these professions misused their customer data.

Lastly, in relation to international intelligence, 61% of the examined (176) incoming intelligence relevant to fraud involved natural persons as the main subject of inquiry or information spontaneously received – be it the main perpetrator or third-party.[36]

[35] A significant percentage (18%) of individuals' professions were unidentified, mainly due to a lack of sufficient details (i.e., personal identifiers like passport number, EID number, and date of birth).

[36] In this context, 'third party' refers to an individual or entity possibly acting as an accomplice or a party involved in routing fraudulent proceeds of crime.

Legal persons

Ten percent of the STRs/SARs sample involved legal persons in the suspected fraud schemes. Most of these legal persons were **newly** established, suggesting possible intentional misuse of legal persons for designed short-span schemes. Moreover, majority of said legal persons were established on the **mainland (48%)**, followed by entities established in **Free Zones (15%)** of which 14% were in commercial free zones and only 1% were in offshore zones. These are in addition to **7%** established in **foreign jurisdictions** and were identified as suspected perpetrators targeting victims in the UAE. In terms of frequently identified legal forms, **40%** of these entities were formed as a **'Limited Liability Company'** followed by **20%** as a **'Sole Establishment'**. In relation to business activities, it was frequently observed that these entities were licensed for activities consistent with the professions observed in suspected natural persons, such as portal and web designing, social media and internet content applications, IT network/services, marketing and advertising services, and building and construction activities.

Within the same context, 39% of the examined (176) incoming intelligence relevant to fraud involved legal persons domiciled in the UAE as possible perpetrators (52%) or acting as third-parties (47%).[37] Of these identified entities, 56% were established in commercial free zones, followed by 37% on the mainland.[38] Moreover, **76%** were formed as Limited Liability Companies (LLCs), and the remaining were among other legal forms. Said involved entities were licensed to practice different business activities, including general trading, investment and asset management, consultancy companies, software, media web and portal development.

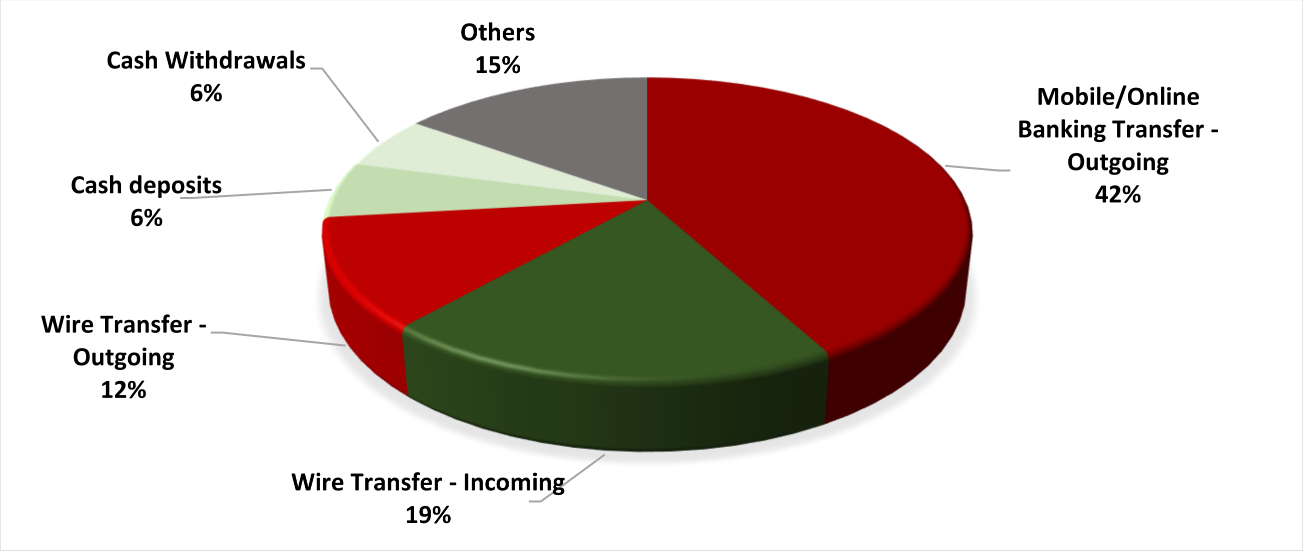
6.2. Mode of suspected fraudulent transactions

Sample analysis of STRs/SARs indicated that nearly half of reported fraudulent transactions involved the means of **outward mobile/internet banking transfers (42%), inward wire transfers (19%), outward wire transfers (12%)**, cash deposits (6%), cash withdrawals (6%), among other modes of transactions, as illustrated in **Chart 7** below.

[37] In the context of received international intelligence, the 'main perpetrator' is an individual or entity involved in the commission of the actual fraudulent activity, while the 'third party' is an individual or entity who is possibly acting as an accomplice in legalizing or routing the fraudulent proceeds of crime.

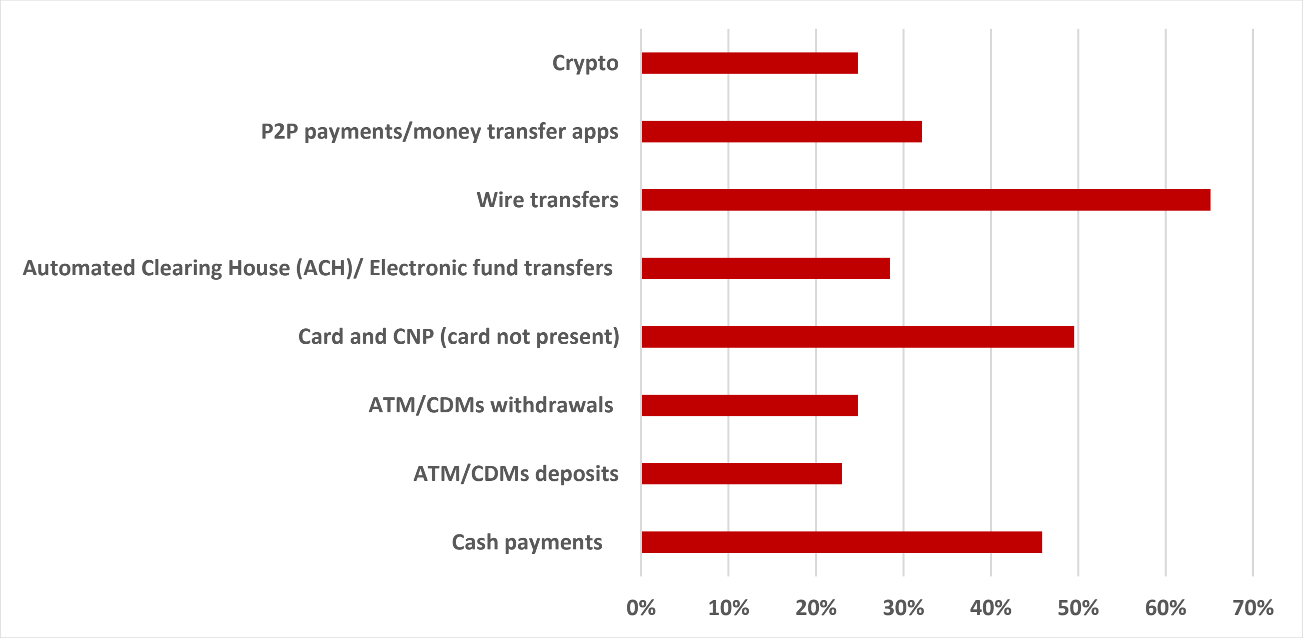
[38] A percentage of 6% was identified as 'unknown' due to the limited information provided by counterpart FIUs.

Chart 7: *Mode employed in fraud-suspected transactions, according to STRs/SARs analysis*



At the same time, analysis of the questionnaire circulated to financial institutions in the UAE obtained similar information concerning observed payment methods involved in fraudulent transactions, **as responded to by 109 financial institutions** and illustrated in the chart below.

Chart 8: *Payment methods observed in fraud transactions, according to the questionnaire*



6.3. Triggers for reporting fraud-related STRs and SARs

The table below shows the top 10 **Reasons for Reporting (RFRs)** in the reviewed sample of STRs/SARs, as selected by reporting entities (REs) in submitting fraud-related suspicious reports to the UAEFIU.

Table 5: *Top 10 Reasons for Reporting (RFRs)*

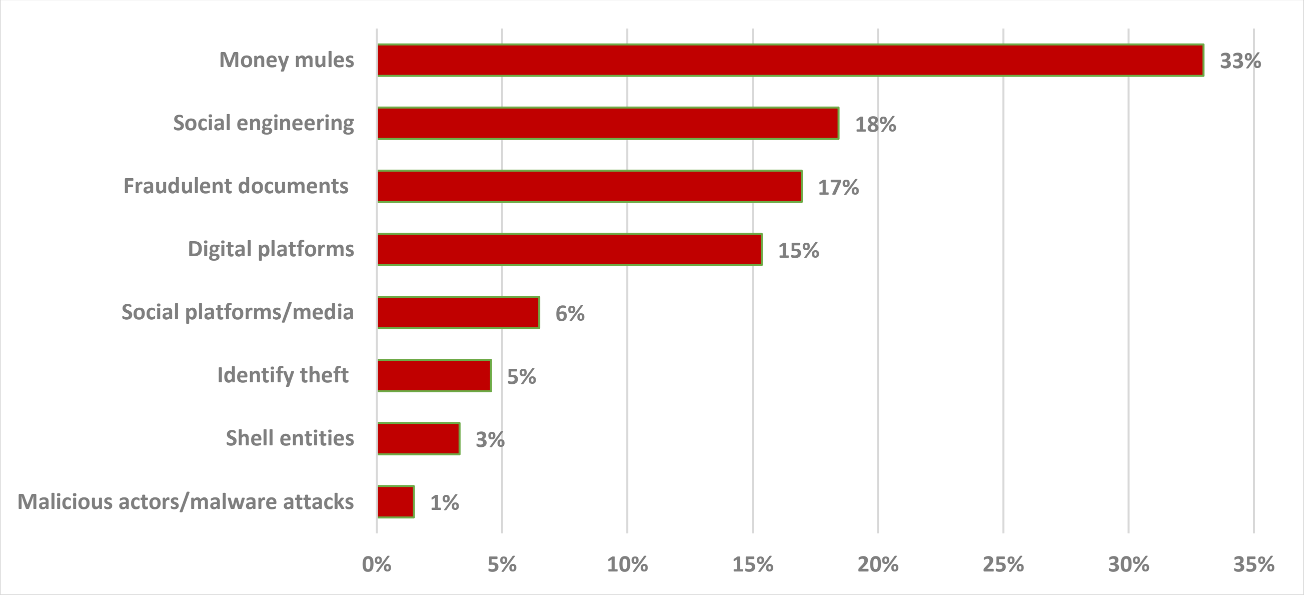
RFR Code	Reason for Reporting	% of examined sample
AFFRD	Advance fee fraud/Phishing or email fraud/Inheritance fraud/fake prizes frauds/romance fraud	26%
SAMIF	Systems/accounts/mobile SIMs/internet or mobile banking fraud/hacking	21%
FDFRR	Fund Recall Request - Domestic	20%
FDFRI	Fund Recall Request - International	11%
FALSI	Use of false identification - Fraud/Forgery - Identity theft	8%
FORCD	Customer provides forged record of past or present employment on a loan application	5%
TAICE	Transactional activity (credits and/or debits) inconsistent with a customer's alleged employment, business or expected activity, or where transactions lack a business or apparent lawful purpose	5%
FRDRR	Customer receives multiple transfers from unrelated parties, specifically individuals residing in foreign jurisdiction, on which a “Fund Recall Request” has been received	4%
IDVER	Customer tries to conceal/forge identification documents or declines to produce originals for verification	4%
FCCFI	Falsification of certified cheques, cashiers cheques or non-cash item cheques drawn against a borrower/buyers account, rather than from the account of a financial institution	4%

7. UNDERSTANDING FRAUD ENABLERS

The analytical approach followed in this report focused on identifying factors enabling fraud schemes. In this context, a fraud enabler refers to individuals, groups, technologies, tools, or other vulnerabilities that wittingly or unwittingly facilitate or contribute to the execution of fraudulent activities.

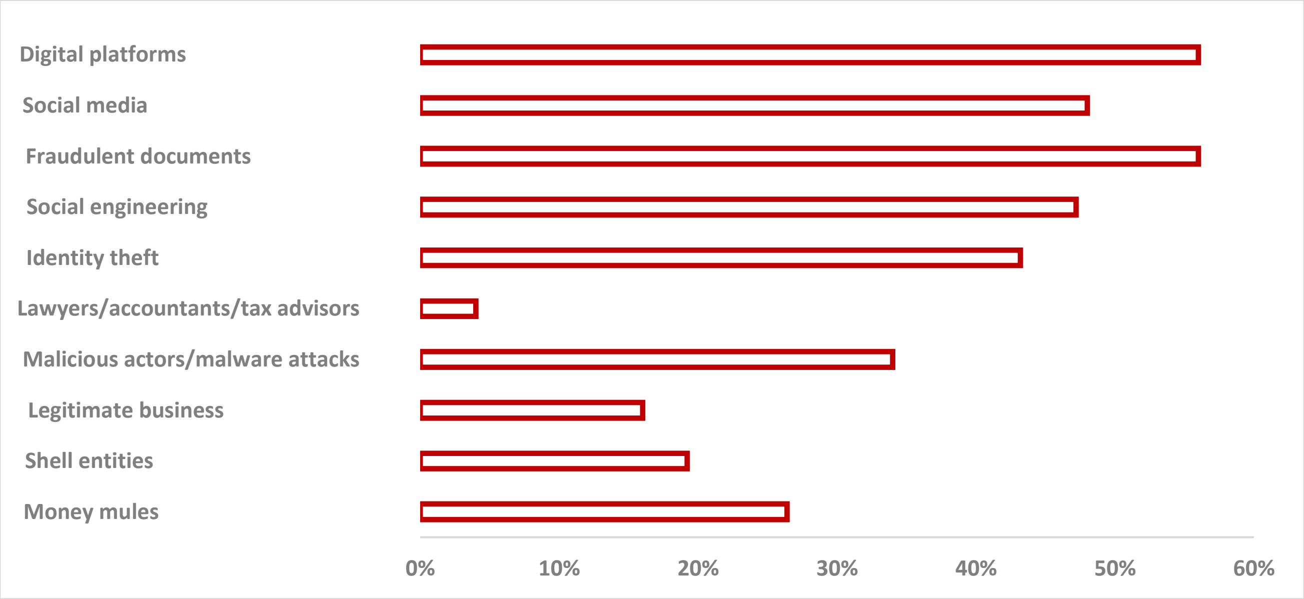
The sample analysis of (879) STRs/SARs revealed that **33%** of the examined suspicious reports were connected with the employment of possible **mule accounts** in various types of fraud and cybercrimes, followed by **social engineering** techniques and the use of **fraudulent documentation** and **digital platforms**, among others, as indicated in the chart below.

Chart 9: *Fraud enablers, according to STRs/SARs analysis*



Similarly, analysis of the questionnaire circulated to financial institutions in the UAE obtained further information concerning frequent observed fraud enablers and facilitators based on the perceptions of **125 financial institutions**, as illustrated in the chart below.

Chart 10: *Fraud enablers, according to the questionnaire*



Lastly, analysis of incoming intelligence reports also highlighted possible fraud enablers, wherein **38%** of the examined reports involved the application of **social engineering** techniques, **21%** contained **fraudulent documents**, **14%** were connected to **mule accounts**, **14%** employed **shell entities**, **11%** utilized **digital platforms**, and 8% were carried out with malicious actors/malware attacks.

The following provides more explanation on frequent fraud enablers observed in STRs/SARs analysis and common in the survey results, as well as analysis of international data.

7.1. Social engineering

Social engineering is not a cyberattack itself, but rather a psychological technique of persuasion and manipulation of victims' minds to trust the scammer and then undertake risky actions.[39] It is "*the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system or to steal personal and financial information. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information*."[40] Scammers would approach the victim in one or more steps, notably by using phishing, vishing and smishing techniques.

7.2. Malicious actors/malware attacks

Within the context of this report, malicious actors or malware attacks refer to cases of account compromise through hacking, and then fraudsters would use it to request payments from customers or vendors and process remittance transactions through online channels, or the case of data theft instead of financial gain.

7.3. Fraudulent documents

Fraudulent documents refer to the act of forging or altering a document (e.g., salary certificates, invoices, shipment documents, insurance reports, financial statements) or tampering with an official document, often to avail financial facility from a financial institution.

7.4. Identity theft

This report interprets identity theft as an enabler (rather than a fraud type). Based on the analyzed data and observed scenarios, identity theft was perceived to be a means of different fraud types.

Identity theft in the context of this report refers to the case in which individuals' personal information is stolen, such as their name, date of birth, passport or identification details, bank account

[39] Cisco (no date) What Is Social Engineering? Available at: https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html

[40] Carnegie Mellon University (no date) Social engineering. Available at: https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html

information, and credit card details, with the intent to commit fraud typically to gain unauthorized gain or benefit. The fraudster then uses the stolen information to impersonate the victim for financial gain, such as opening new accounts, making unauthorized transactions, applying for loans or credit cards, or committing other criminal acts in the victim's name. Usually victims of identity theft find out that their identity has been stolen when they try to obtain their credit reports.

Based on the analysis, it is apparent that fraudsters gain access to the victim's sensitive data through various methods, mainly phishing or social engineering. Identity theft was also perceived from many suspicious reports to be a versatile crime that acts as a starting point from which to execute different fraud schemes, including account takeover and loan and credit card fraud, among others.

7.5. Mule account

The UAEFIU has significantly observed the recruitment of third parties and the employment of mule accounts in different typologies relevant to financial crime, including drug trafficking, fraudulent activities, and laundering the proceeds of crime. For the purpose of this report, a mule account has been interpreted as an enabler of fraud (rather than being a fraud type itself). Most of the data used in this report indicated the utilization of a mule account in conducting different types of fraudulent activities and/or laundering their proceeds by using the account (knowingly or unknowingly by the account holder) in receiving, moving and layering fraud proceeds across and outside of UAE financial institutions.

A significant number of the examined STRs/SARs (**33%**) showed certain characteristics and indicators that are often common in mule activities and were associated with over **400 individuals**—majority were blue-collar workers.

For example, mules were frequently observed in part-time job scams and task or employment scams. Fraud perpetrators would purportedly recruit individuals wittingly or unwittingly, acting as mule accounts to receive fraudulent funds, subsequently requesting to resend the funds to a specific or different account after deducting a specific amount as a commission. Multiple STRs/SARs suggested that these mules are operating within a network.

Cases disseminated to LEAs underlined the use of 'mule accounts' as one of the major fraud enablers. These accounts were mainly used to either receive fraudulent funds from abroad or add more layers to the movement of funds. In such cases, the typical observed transactional pattern involved receiving funds from unrelated (local and international) parties, followed by swift cash being withdrawn to interrupt the money trail or transferred to other accounts in rapid succession. The account is then left with a minimal or zero balance. The second transactional pattern for layering would involve receiving multiple funds via transfers or ATM cash deposits from various locations, mostly in the UAE, followed by immediate withdrawal. Therefore, the account is utilized as a pass-through for illegal movement of funds.

Similarly, the examination of fraud cases initiated by LEAs and, in particular, the UAEFIU technical reports associated with these cases illustrated the role of the ‘mule account,’ which was heavily utilized in investigated fraud schemes. The transactional pattern was indicated previously and implied that these mules would operate at multiple levels to layer the funds, while the first level is possibly where the victim was deceived and transferred/authorized the funds.

Data collected through the focus group discussion also underlined the trend of slipper fraud. Slipper fraud entails the case in which mules open accounts, maintain these accounts in good standing, perform usual transactions for 12 – 24 months, and then use these accounts later to facilitate the layering of fraudulent proceeds.

Ultimately, discussion amongst the focus groups underlined the frequent use of money mules in fraud schemes, indicating that blue collars might sell these accounts to criminals for insignificant amounts with no (complete) knowledge as to how their accounts are misused in criminal acts. Another example is observed through some legal entities recruiting blue collar workers from abroad to obtain credit facilities and open bank accounts to be misused in fraudulent activities, and then those recruited laborers will return to their home countries. A similar scenario is when an employer takes control of an employee’s account to facilitate laundering the proceeds of fraud (disguised as structured salary payments). After the ‘salary’ has been paid, the employer withdraws it as cash. These observations are consistent with what is recognized at the global level, concerning how mules are often motivated by criminals’ threats or a commission for contributing to an illicit activity or simply tricked for what seems to them as a legitimate purpose.[41]

7.6. Legal persons

Legal persons as fraud enablers may include shell, front and clone companies or legitimate businesses. A shell company refers to an “incorporated company with no independent operations, significant assets, ongoing business activities, or employees,” usually structured to conceal the beneficial ownership. On the other hand, a front company refers to a “fully functioning company with the characteristics of a legitimate business, serving to disguise and obscure illicit financial activity.”[42] Clone companies entail firms established by scammers under a similar name or address of a genuine

[41] (UNODC, 2022).

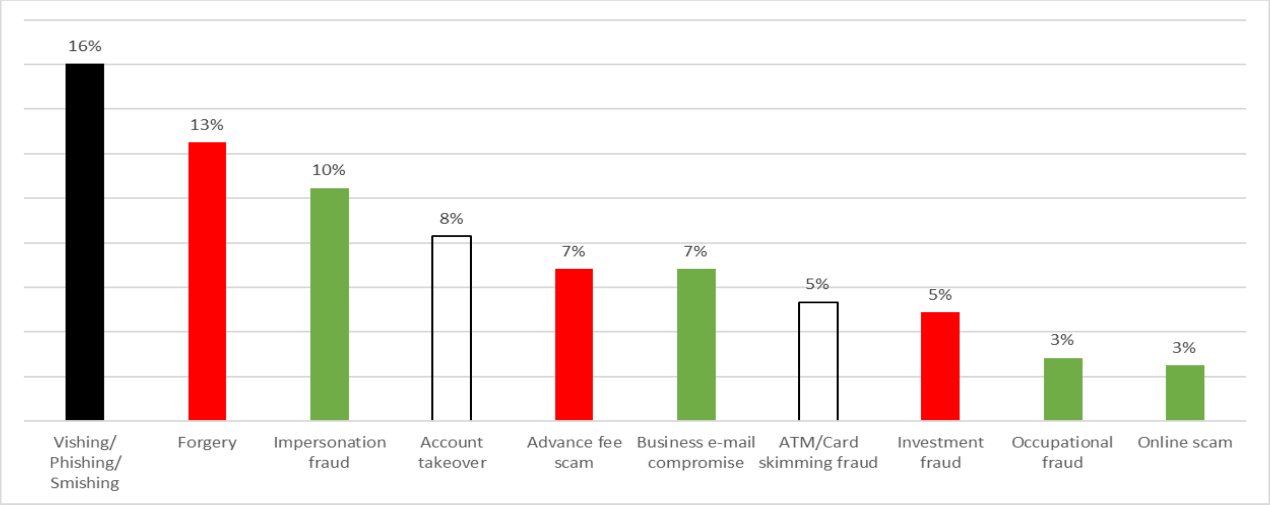
[42] FATF (2018) Concealment of Beneficial Ownership. Available at: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Concealment-beneficial-ownership.html

business or a popular brand or chain.[43] A legitimate business, within the context of fraud enablers, refers to the case in which a legitimate company is tricked (e.g., for an investment opportunity) by fraudsters to receive or redirect fraudulent proceeds into different accounts controlled by criminals.[44] Legitimate businesses also might be wittingly involved in enabling fraud schemes in return for a promised profit or commission — similar to money mules.

8. PREVALENT FRAUD TYPES AND PATTERNS

Sample analysis of STRs/SARs indicated fraud types and techniques in reported fraudulent transactions. The top fraud type concerned **vishing and phishing**, in addition to some cases involving **smishing**, **contributing 16% of the sample**, followed by 13% related to forgery/counterfeit and 10% to impersonation fraud, and 8% involved account takeover, advance fee scams, and business email compromise, with 7% each. It should be noted, however, that some of said types overlapped, where two or three types of fraud were used sequentially.

Chart 11: *Top 10 fraud types observed in STRs/SARs analysis*

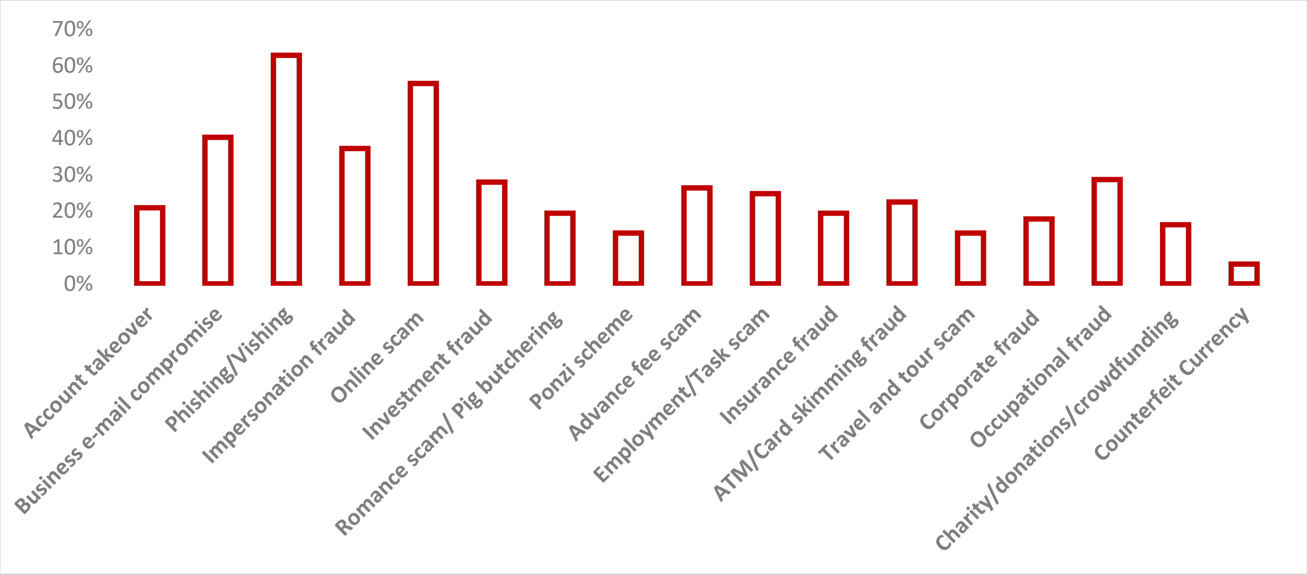


Based on the results of the questionnaire circulated to financial institutions, phishing and vishing were also the most frequent fraud types, with 129 financial institutions responding. However, as illustrated in the chart below, other types of fraud were perceived relatively differently in terms of frequency and volume from what was indicated in the analysis sample of STRs/SARs.

[43] Financial Conduct Authority (no date) Clone firms and individuals. Available at: https://www.fca.org.uk/consumers/clone-firms-individuals#:~:text=Clone%20firms%20aren't%20authorised,example%2C%20to%20the%20phone%20number)

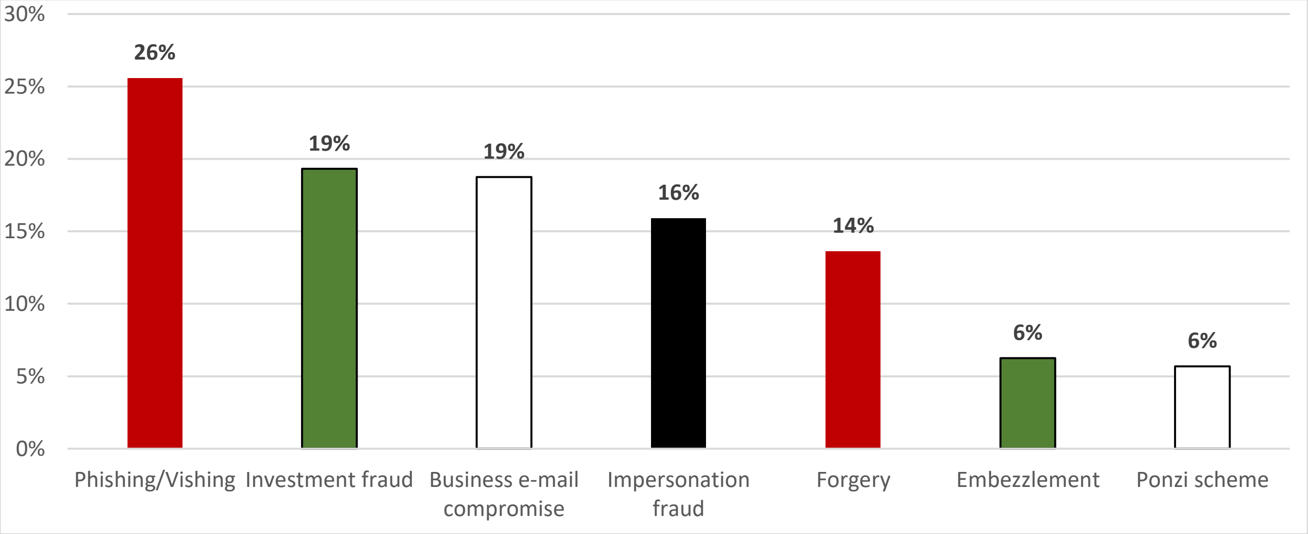
[44] FATF-INTERPO-Egmont Group (2023).

Chart 12: *Fraud types, according to the questionnaire*



As indicated in the chart below, analysis of incoming international intelligence reports also demonstrated phishing and vishing as the most prevalent technique, contributing to 26% of the total examined sample. Some cases of such phishing/vishing fraud revealed a link with **OCGs**.

Chart 13: *Main fraud types observed in the examined international intelligence*



The following describes the identified fraud types and techniques in depth to assist reporting entities and other stakeholders in anticipating potential fraud-related scenarios and risks. As explained, the majority of the indicated types highlight the increasing shift to cyber-enabled fraud, considering the advancement of technology (including its modern channels and payment methods).

8.1. Phishing, vishing, and smishing

Fraudsters use various deceptive methods to deceive victims to reveal sensitive personal information, exploiting their trust, essential needs, or lack of awareness. Below are some of the common deceptive techniques related to cyber-enabled fraud (as concluded from the analysis).

Phishing: This is one of the most widespread forms of cyber-enabled fraud. It involves sending malicious communications, typically emails which appear to come from legitimate sources. The goal is to trick the recipient into providing sensitive information such as passwords, financial details, or personal identification numbers (PINs). For example, victims would receive an email that appears to come from their bank, asking them to verify their account details via a link. The email typically contains a link directing the victim to a fake website (replicating the bank's official website) designed to steal login credentials or other information.

Vishing (voice phishing): This method involves using phone calls to deceive victims. Scammers pretend to be representatives from legitimate organizations (such as law enforcement agents and FI representatives, among others) to obtain sensitive information via the telephone or convince a victim to conduct certain transactions. Often they create a sense of urgency, pressuring the victim to act quickly without verifying the legitimacy of the request.

Smishing (SMS phishing): This is similar to phishing but conducted via SMS or text messages. Victims receive text messages that contain malicious links or requests for personal information.

Based on the analysis of international intelligence, many instances indicated that phishing was combined with business email compromise (BEC), while vishing was linked with either impersonation fraud/spoofing or investment fraud.

8.2. Impersonation fraud

This type of fraud occurs when a scammer pretends to be someone else, such as a trusted individual, organization or authority, in order to deceive victims into revealing personal, financial or sensitive information and credentials. There were two main types of impersonation fraud frequently noticed during the analysis: one involves impersonating a governmental authority, wherein scammers pose as police officers or a governmental official to obtain vital information and personal details, while the second type is concerned with impersonating financial institutions, wherein scammers pose as a bank's official to trick victims into sharing their credentials, account details, and verification codes. Such fraudulent activity occurs along with other deceptive methods explained previously, like phishing or vishing. On the other hand, a few suspicious reports indicated instances of impersonation related to legitimate organizations, suppliers, and mail delivery offices.

Impersonation fraud is also prevalent, as concluded from the international intelligence reports received from counterpart FIUs (covering 16% of the total sample reviewed). The majority of the observed techniques involved impersonating suppliers, followed by purporting governmental agencies and their officials and financial institutions. Analysis of such scenarios showed that impersonation fraud was frequently combined with BEC and phishing.

8.3. Business e-mail compromise (BEC)

Business email compromise — also called payment diversion fraud — is a sophisticated fraud technique that targets legitimate businesses and organizations by exploiting email communication channels. Fraudsters often compromise a legitimate email, use it to send malicious emails, and manipulate payment instructions to trick the victim into making payments to fraudulent accounts. In many cases, BEC is found to be linked with ‘payment redirection’ and ‘payment diversion,’ in which perpetrators alter payment or beneficiary details, redirect invoices, or transfer funds to an unfamiliar account.

Analysis of STRs/SARs illustrated that this method is often used by compromising the emails of a wide range of businesses, including financial institutions, real estate agencies, and audit firms, to ask their customers or suppliers to transfer funds to other new accounts or change their bank account details. Emails sent by fraudsters would mimic legitimate organizations’ emails but with some slight differences that usually go undetected by the victim.

It was noted that in multiple incidents, the recipient account often belonged to a ‘money mule’ who moved the funds in exchange for a small commission or a member of a larger network, while funds would eventually be sent to accounts controlled by the main fraudster. In such cases, the reporting entities noticed a mismatch between the actual name of the funds’ recipient and the intended beneficiary, as verified in the supporting documents provided by the victim. Additionally, account analysis in other cases revealed suspicious activities associated with the funds’ recipient (i.e., newly established entities), where the funds ultimately end up in the shareholders’ accounts, suggesting the involvement of a shell company.

Another scenario observed is when the victim’s email (registered with the FI as one of the official communication channels) is hacked, after which the fraudster sends fraudulent/unauthorized emails to the victim’s bank (with which the victim holds an account), requesting changes to the account details and/or the added beneficiary(ies). These attempts were often accompanied by falsified documents, such as altered invoices, with the bank receiving multiple revised invoices to support the fraudulent request.

Still, it was apparent from the analysis that perpetrators relied heavily on social engineering techniques more than technical hacking. For instance, the victim would receive an email from the fraudster instructing to update the known supplier's IBAN details or redirect the payment to the amended bank details of the alleged same supplier, while the new bank accounts provided are controlled by the fraudsters. To create an impression that the email sender is legitimate, the fraudster would share details along with a forged document containing the company's official logo and company employee's signature. The fraudster might also use an email address similar to the genuine supplier's (with a noted difference in the email domain extension) when sending the updated payment details to the victims.

BEC is also one of the most observed types in international intelligence reports exchanged with counterpart FIUs, from which it was perceived that perpetrators of this fraud type are usually located in the UAE.

8.4. Fake online marketplace and shopping scams

In this type of fraud, fraudsters set up fake trading websites or operate via social media platforms to sell products and services that do not actually exist. Victims are lured in by attractive prices or limited-time offers and end up making payments without receiving the goods or services that they were promised.

Victims were noted to be tricked into purchasing products like tickets, educational courses, cult brands, or out-of-stock medications. After payment is made, the goods are never delivered and the scammers disappear. Few suspicious reports also indicated that scammers create a convincing online storefront with a professional design, product listings, and customer reviews.

Furthermore, online scams were observed to be combined with impersonating popular, legitimate brands and corporates (e.g., food chains, telecommunications services, and shipment and delivery companies, among others) by creating fake URLs that mimic the domain names of these brands. These fake URLs are typically embedded within phishing emails, malicious websites, or online advertisements. When users click on the spoofed URLs, they are redirected to fraudulent websites designed to steal sensitive information such as login credentials, credit card numbers, or personal data.

8.5. Account takeover

Another type of cyber-enabled fraud observed in the data is account takeover. An account takeover refers to the case in which someone gains unauthorized access to someone else's bank account and controls it to move funds and facilitate illicit activities. Therefore, it is deemed to be a type of identity theft. Phishing, impersonation fraud, SIM swapping, stolen and purchased credentials through dark webs and illegal platforms, and leaked data from financial institutions are often used to gain such access.

Analysis of suspicious reports indicated that fraudsters use social engineering techniques to deceive victims into compromising their personal details. Examples of techniques orchestrated by fraudsters include impersonating a financial institution and claiming that customers need to update their KYC details. Similarly, impersonating a governmental entity by asking victims to update their personal information; otherwise their residency status will be revoked. Another form of popular manipulation involves a claim relevant to a money laundering investigation, with a victim needing to cooperate in providing the required personal information to clear their suspicion and then transfer their funds into a repository or dummy account until the investigation is concluded.

Some observations indicated that fraudsters use the ‘forgot user ID’ and ‘forgot password’ options to reset the victim’s credentials and fully obtain control of the accounts. Moreover, there are several cases suggesting that callers (fraudsters) have already acquired victims’ personal details beforehand (Emirates ID number, issue date, and expiry date), indicating possible data leakage by unidentified sources. Analysis showed cases in which financial institutions were able to detect the different IP addresses used by the fraudsters when logging in to the victim’s account browser or mobile banking.

8.6. ATM/card skimming fraud

Criminals use devices known as ‘skimmers’ to illegally capture card information from the magnetic stripe of debit or credit cards when they are used in ATM transactions or swiped at point-of-sale terminals.

Some suspicious reports indicated that card details were stolen using a card skimming device, and the funds were then transferred overseas through exchange houses’ mobile application. Other reports suggested the use of skimmed card details for conducting fraudulent remittances when remitters’ profiles with a low-income segment (mostly blue collars) were settling the remittance amounts within a short timespan through multiple credit cards issued by different banks.

Few other reports also suggested the possibility of using the details of skimmed cards on cryptocurrency trading platforms. Furthermore, there were few incidents, as reported by exchange houses, concerning failed transaction attempts with multiple international cards, suspected to be connected with card skimming.

8.7. Advance fee scam

Advance fee scams involve the promise of a significant benefit (like a lottery win, inheritance, fake employment, or investment opportunity, among others) in exchange for an upfront payment. The scammer typically claims that the victim needs to pay a processing fee, tax, or some other type of upfront charge to receive the promised reward or benefit. However, once the fee is paid, the victim never receives the benefit. This scheme is often combined with the impersonation of governments, private institutions, or popular commercial brands.

The analysis revealed that victims were deceived into paying upfront fees to a claimed entity to provide services or investment opportunities in order to secure a deal/offer, but no services or offers were rendered. Victims in such a scheme are not necessarily individuals but also businesses; analysis showed that legitimate businesses could be misled by fraudsters who pretended to be eager to invest in the victim's company or make a significant, high-profit business deal. Fraudulent documents and fabricated information are usually utilized in such a case (i.e., fake SWIFT messages) to show that funds have been transferred while no transactions have taken place. Based on the analysis, the forged SWIFT suggested that the perpetrator may be located abroad.

This type of scam was associated with other fraud types such as employment fraud, loan and investment scams, as explained shortly in the following types. These are in addition to tourism scams, where scammers collect victims' contact details from shopping malls and call them claiming that they have won the draw for tourism packages and that in order to claim the offer, the victim needs to deposit or transfer some money to the promoter.

8.8. Employment/task fraud

Work seekers are frequently the target of these types of scams that offer the victims part-time jobs, work-from-home opportunities, and investments with high returns. Scammers would contact the victims via email, message applications, social media, or other online platforms and often involve the impersonation of human resource departments of reputable corporations and request the victims to pay fees for job applications or enrollment for training. Afterward, the scammer disappears and the promised job or reward never materializes.

Moreover, scammers may request personal information such as bank account data and copies of identity documents for this type of fraud. Accordingly, this information will be utilized in fraud schemes. Some FIs reported a trend of customers receiving money from different accounts based on fake tasks assigned to the customers by fraudsters. Subsequently, fraudsters will request customers to invest with them in an investment platform or encourage customers to transfer additional funds to be allocated with more tasks, promising greater earnings or profits.

8.9. Loan fraud

As reported by FIs, fraudsters in this type of scam may approach victims offering them a high loan amount via social media. Afterward, fraudsters will request the victims to remit a certain percentage of the loan amount as security to release the funds. It was noted that specific nationalities were targeted by this type of fraud, where victims use mobile applications to remit advance payment to fraudsters.

Another scenario discussed by the focus group participants is where multiple employees of a certain company apply for vehicle loans on different occasions (from the same car dealer) and then suddenly default all at once. Intelligence would reveal that all of the vehicle loan takers had left the country and the vehicles had become untraceable, suggesting the misuse of legal persons' establishment and recruitment of these individuals for this scheme.

8.10. Insurance fraud

Insurance fraud was particularly reported by insurance companies concerning customers submitting false claims, e.g., collusion between two parties to fake a car accident and claim insurance coverage—this type is often known as "crash-for-cash fraud". Similarly, in terms of submitting fake medical documents to claim for insurance benefits or fabricating a death certificate in the case of life insurance.

Other scenarios involved the case of individuals added under group policies as employees while not having any employment relationship with the entity.

Insurance companies also revealed a fraud trend involving unauthorized agents selling scammed medical and workmen's compensation policies by altering details, such as the date, insured name, and policy amount, from existing company policies.

8.11. Investment fraud

This is a deceptive practice used to lure investors into making financial investments based on false promises of high returns and misleading information about the investment. This type of fraud involves different products such as securities, foreign currencies, and virtual assets — which were frequently observed. Proceeds of this fraudulent activity were also observed to be laundered through virtual currencies and crypto exchanges with the exploitation of money mules.

Within the same context, fraudsters also exploited social media to advertise investments in cryptocurrency. The victim was then redirected to communicate through a messaging application for more information and requirements. The fraudster created an illusory 'offer' of buying a certain amount of cryptocurrency payable in several installments, and promised a monthly profit. However, no profit nor returns were transferred to the victim's account on the due date.

Similarly, investment fraud through digital trading platforms was also noted, wherein fraudsters would create fake or deceptive online trading or investment platforms which might imitate a legitimate business. Fraudsters would offer different investment and trading opportunities in stock, foreign currencies, and cryptocurrencies. Afterward, victims would deposit funds into the platform, but the funds were either siphoned off or locked in and investors were incapable of withdrawing their money.

Analysis of STRs/SARs also indicated other examples of investment fraud, including Ponzi and pyramid schemes. At the same time, the majority of examined international intelligence suggested the utilization of suspected fraudulent proceeds (transferred to the UAE) from a Ponzi scheme operated abroad.

Furthermore, advance fee scams were found to be connected with investment fraud in cases of fraudsters deceiving investors and requesting them to transfer to the perpetrator or a complicit account (mule account) upfront fees for the investment.

In relation to the frequent transactional behavior observed, accounts were being funded by transfers from various individuals, after which funds were directed to another account. The initial reason for these transfers was purportedly indicated as being 'for investment purposes.'

8.12. Application fraud

Application fraud occurs when a party provides misleading or stolen information to access financial services and secure a loan or credit application by deceiving lenders (usually financial institutions) under false pretenses. As indicated in the data, this involves stolen or fabricated identities, falsified income, employment details or credit history, forged or counterfeited documents, and possible internal collusion (from the lender's personnel), among others.

Fraudsters may also create clone companies with names identical to those of reputable businesses. Several suspicious reports indicated the association of companies being set up for the purpose of selling residency visas and providing salary certificates to alleged 'employees' of the company to be used for applying for credit facilities with financial institutions. There were many irregularities found in these cases, such as inconsistency between the employee's declared and indicated salary, as well as between the employee's profession and employer's profile, and having an unreasonably high salary amount in comparison to the market value. These are in addition to spelling and grammatical errors found in the salary certificate. At the same time, no regular salary was credited into the account, or multiple salary amounts credited into the account were observed followed by immediate utilization of the funds. Other instances highlighted a connection with newly established entities in which multiple employees were approaching a financial institution to avail credit or loan facilities.

8.13. Occupational fraud and asset misappropriation

Occupational fraud is "*the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets*" (ACFE, 2024).[45] It includes asset misappropriation, corruption, and financial statement fraud. This fraud type exploits the trust given to the organization's employees in conduct or complicit in fraudulent activities, usually causing financial or reputational losses to the organization. It is often linked to unlawful acts such as embezzlement, unauthorized access to customer accounts and data, or colluding with external parties.

Several suspicious reports, particularly received from exchange houses, indicated the theft of cash (or supplies for personal use) in association with forging a customer's signature. Other few reports involved occupational fraud, wherein one employee would collude with a prospective supplier and receive a commission from a supplier in return for signing the customer into the organization's procurement system.

Within the same context, analysis of international intelligence reports suggested the use of UAE financial institutions to receive funds potentially generated from embezzlement abroad under the false pretense of business purposes or trade payments.

8.14. Forgery and counterfeiting

Forgery and counterfeiting broadly reflect the forms of fraud involving misrepresentation through fake documents, goods, or other instruments with the intent to deceive another party. While both are closely related, they refer to different types of fraudulent activities.

Forgery involves the falsification of a document, signature, or financial instruments such as cheques. In many cases, it involves an alteration (e.g., in the data of identification documents, such as the date of birth, name, and photo) or amendment (e.g., in letters, agreements and contracts) to make a document appear to be authentic. On the other hand, counterfeiting typically involves creating fake items/documents that imitate genuine ones, most notably currency, bank account statements, or salary certificates.

Most of the suspicious reports analyzed that related to forgery or counterfeiting were directly associated with manipulating income-proof documents, particularly salary certificates, to avail credit

[45] ACFE (2024) Occupational Fraud 2024: A Report to the Nations, p.7. Available at: https://legacy.acfe.com/report-to-the-nations/2024/

facilities. Different financial institutions conducted verification exercises in order to validate the authenticity of such documents by contacting the indicated employer in the document and, in some cases, conducting visits to the employee's (customer's) workplace, and found that these documents were forged or counterfeited. Furthermore, there were instances noted in which customers presented falsified bank statements to embassies of other countries to prove active bank accounts in the UAE and regular salary credits.

Other reviewed reports highlighted cases of forged cheques, bankers' drafts or managers' cheques. In some of those instruments, there were evident discrepancies, such as spelling mistakes in the FI's name, the absence of a serial number, an invalid date format, an invalid issuing branch, and wrong routing on the magnetic ink character recognition (MICR). Other instances also indicated the use of 'invisible ink' — also known as 'disappearing ink.'

The analyzed STRs/SARs showed that the majority of the involved individuals were purportedly holding managerial positions and were reported due to concerns related to a forged employment or salary letter in an attempt to avail banking services.

Forgery is also found to be one of the major concerns in the related international intelligence reports received from counterpart FIUs, wherein different scenarios involved fabricated documents such as personal identification documents (passports), invoices, and contract agreements, among others.

8.15. Pig butchering and romance fraud

Although analysis of STRs/SARs and international intelligence data did not reveal the use of this type of fraud during the reviewed period, few respondents to the questionnaire circulated to financial institutions indicated romance fraud and pig butchering among the observed fraud types. This includes a couple of incidents that were reported to involve romance scams through dating apps, which were associated with blackmailing the customer to pay the money requested by the scammer.

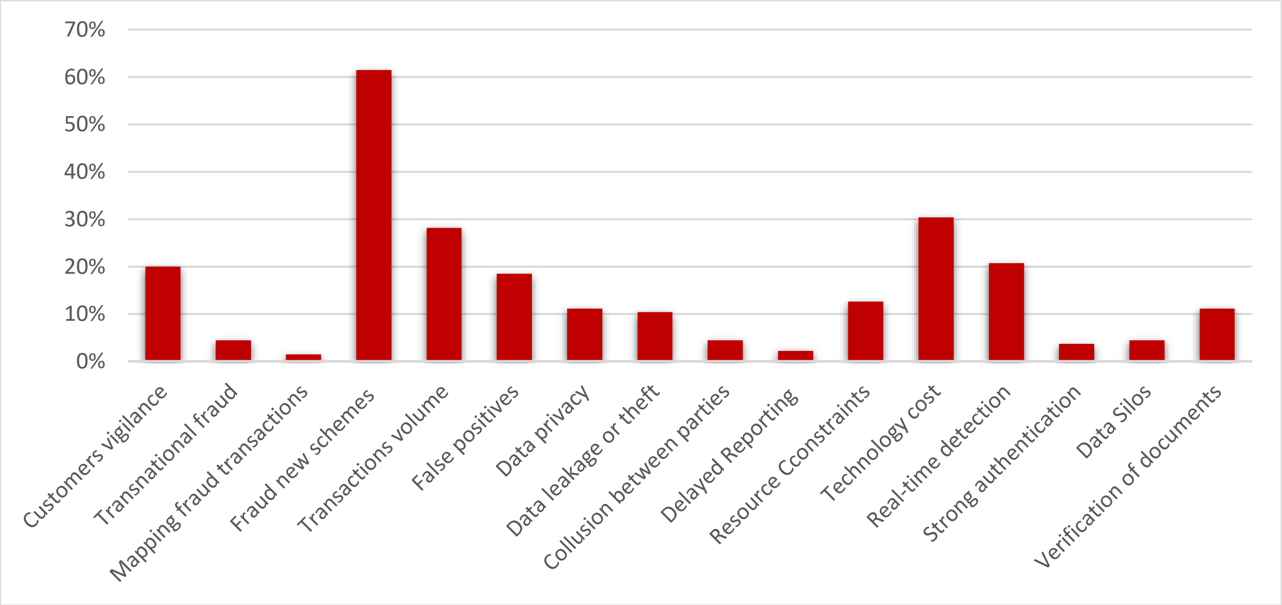
However, for the pig butchering scenario, most of the questionnaire responses concerning this type of fraud were noticed to be observed by international institutions in the UAE, suggesting that this type might have been associated with their branches abroad since this type of fraud was not seen in the examined sample of STRs/SARs or cases initiated from LEAs. Therefore, the extent of this type of fraud is indeterminate, noting that victims of this type of scam often feel embarrassed to report it.

Pig butchering refers to a combination of cybercrime with different fraud types, including romance and investment fraud. Fraudsters would create fake profiles and approach random potential targets using social engineering tactics to build the illusion of friendships, romantic relationships, and trust with victims (especially those with little or no knowledge of the crypto ecosystem) and convince them to make small investment opportunities in crypto — known as inducement payment. Investment might involve popular, trusted crypto providers in the beginning to build trust. Later, however, fraudsters would ask the victim to transfer their crypto funds to another (fake) platform, which will show significant fictitious gains for a while in the account to lure the victim into making further investments. Ultimately, once the victim transfers several amounts to the fraudster's platform and has no more funds to invest, they will be ghosted and lose contact with the scammers.[46]

9. IDENTIFIED CHALLENGES IN TACKLING THE SCALE OF FRAUD

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

Chart 14: *Operational and technical challenges identified by the respondents of the questionnaire*



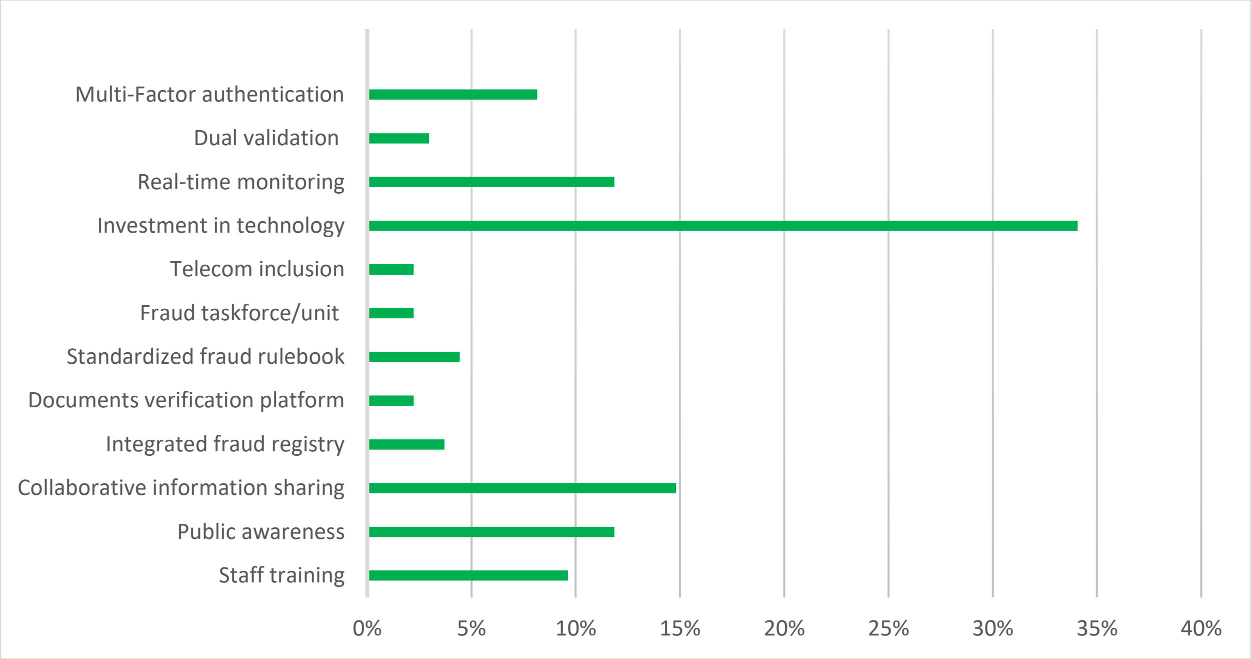
Responses received from 135 financial institutions in the UAE illustrated that over 60% of these institutions encounter a challenge in tackling new fraud schemes and trends, especially considering the transaction volume. At the same time, they emphasized the cost associated with advanced technology and enhanced security controls required to tackle identified techniques and proactively counter these schemes.

[46] Griffin and Mei (2024); ACAMS (2024) Pig Butchering: The Nexus of Fraud and Money Laundering. Available at: https://www.acams.org/en/media/document/37595

10. PROPOSED SOLUTIONS AND RECOMMENDATIONS

Within the context of previously discussed challenges, the following were proposed as action points that need to be considered in the national approach against fraud:

Chart 15: *Key solutions suggested by the respondents of the questionnaire*



As indicated in **Chart 15**, investment in technology was the top suggested solution by the questionnaire respondents, as well as the focus group participants. In particular, implementing AI-driven analytics can help to identify transaction patterns and anomalies relevant to fraud. These systems can adapt to new fraud tactics by learning from large datasets. This is in addition to exploring blockchain solutions to secure transparent transaction records, especially in areas like digital identity verification. These technological advancements can significantly boost an institution's ability to detect and prevent fraud more efficiently.

Respondents also highlighted the importance of applying multifactor authentication. Biometric authentication, including using fingerprints, facial recognition, and iris scans, can significantly identify fraud with multifactor authentication. Within this context, AI-driven document authentication systems are also essential and can provide an additional layer of security by verifying the authenticity of identity documents.

Moreover, enhancing systems to allow for real-time monitoring, including real-time authorization of suspected transactions and analysis of transactions, can significantly reduce the time that it takes to detect and respond to fraudulent activities.

Respondents also emphasized that time is critical in preventing funds from entering the layering stage of money laundering, and fraud reporting and customer support must be prioritized. Furthermore, the necessity of fraud training and raising awareness of the relevant staff through regular up-to-date training on the latest fraud tactics and prevention techniques can strengthen employees' first line of defense against fraud. Ultimately, industry-wide consortiums among financial institutions for sharing fraud information, as well as collaboration mechanisms between financial institutions and regulatory bodies, would foster identifying emerging fraud trends and responding more effectively.

11. DEVELOPED RISK INDICATORS

At the end of the analysis of this report, the UAEFIU developed a list of relevant risk indicators with the aim to assist its stakeholders, including reporting entities, in detecting unusual transactions and behaviors relevant to fraud. These risk indicators are crucial for financial institutions' risk-based approach and transaction monitoring, noting that criminal activity cannot explicitly be concluded based on a single indicator, but rather a combination of these indicators, in order to ascertain such suspicion.

Transactional patterns

1. Transactions that are significantly higher than the customer's typical activities over a short span of time.
2. A high volume of sudden remittances from a remitter (or different remitters) located overseas.
3. A single remitter sends to multiple beneficiaries or beneficiaries receiving from multiple remitters.
4. Unusual large transactions, or high frequent activities coupled with a high number of incoming electronic fund transfers in a newly opened account.
5. A dormant account that is suddenly engaging in large or high-frequency transactions with unknown parties.
6. A non-resident account showing high velocity in the movement of funds in small amounts over a short span of time.
7. Multiple transactions during unusual business hours, depending on the customer's time zone.
8. Sudden use of a high volume of payments through e-wallets or indicating virtual currencies by customers having no history of their usage.
9. A high volume of transactions suggesting gambling websites or virtual asset exchanges.
10. A sudden change in the merchant's transaction volume or business category, indicating potential involvement in fraudulent schemes.
11. Unreasonable modifications to payment instructions with inconsistent bank information.
12. Urgent or rushed changes in transaction instructions, especially when coupled with other risk factors.

13. The use of multiple cards or accounts for a single transaction over a short period of time.
14. A high volume of rejected payments.
15. A sudden increase in a customer's online transactions, telephone banking transactions, or mobile payments.
16. Multiple cash withdrawals from ATMs in geographically distant locations.
17. Unexplained transfers between multiple accounts across different domestic banks or other countries, especially if said transfers are subsequent to a large inward remittance.
18. SWIFT recalls raised by the remitter or 'funds recall requests' received from different remitting banks on the same beneficiary.
19. A remitting bank confirms that the funds are fraudulent in nature.
20. Multiple or unexplained remittances/transfers, especially to or from foreign accounts, or unrelated domestic accounts, followed by a 'funds recall request.'
21. The account activity indicates third party deposits/transactions involving individuals who are unrelated to the customer.
22. Funds being rapidly transferred or moved between multiple accounts (domestic or international) without legitimate purposes, indicating a possible layering tactic to hide or obscure fraudulent funds.
23. A customer transaction with a counterparty linked to adverse media or open source data, indicating possible engagement in fraudulent activities/schemes when conducting screening on the subject.

Behavioral patterns

24. Insufficient justifications obtained from the account holder on the received funds, or a customer being clearly unaware of the purpose and source of funds received in the account.
25. Multiple communications (via email) including revised invoices within a short period.
26. Accounts or online banking logins that are from unusual locations or from multiple geographical locations in a short period.
27. Accounts accessed from an unfamiliar device.
28. Multiple accounts or online banking profiles being accessed from the same device.
29. A sudden change in user profiles, transactions of beneficiary details, or personal information like the email address, physical address, or phone number shortly before the occurrence of suspicious transactions.
30. The activation of a dormant account shortly before conducting large or frequent transactions.
31. A high number of failed login or transaction attempts, indicating possible credential testing.
32. Sudden complaints, and multiple 'funds recall requests' received on a single account regarding unauthorized/fraudulent transactions, disputes, or account access.
33. The account holder is a newly hired individual but has immediately attempted to avail credit facilities with the financial institution.

34. Multiple individuals employed by a newly established entity apply for credit facilities in the same period of time.
35. A customer holds several accounts with multiple financial institutions either domestically or internationally without a reasonable purpose or business justification.
36. 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.
37. An investment promoter relates to new-tech or unregulated markets.
38. Open source data indicate a lavish lifestyle of the senior management of an investment promoting company.
39. A customer rejects or avoids authenticating/updating his/her identity and personal information.
40. An uncooperative customer in providing the documents required by the financial institution or rejecting when asked to use multifactor authentication to verify his/her data.

Unusual and inconsistent information

41. Documents provided by the customer reveal several discrepancies, including but not limited to spelling mistakes, grammatical errors, font irregularities, and visible poor alignment, among others.
42. A transaction showing a mismatch between the beneficiary's entered account name/IBAN and the actual beneficiary name.
43. Discrepancies in identity documents provided during account opening or KYC updates.
44. A mismatch between the customer's identity and any other data relevant to the customer profile.
45. A customer provides/updates his/her profile through inconsistent different versions of his/her identity.
46. Multiple transactions to beneficiaries who share the same address or work with the same employer.
47. Rapid or frequent updates to vital personal information, account profiles, and signatures, suggesting that an account is being taken over or manipulated for fraudulent purposes.
48. Transactions that do not match the customer's stated purpose or profile, such as personal accounts conducting business transactions.
49. An individual's declared salary is not in line with the employer's profile and employee's profession and expertise.
50. An individual receives a salary from an entity different from the employer declared at the time of onboarding.
51. A personal account is opened for the purpose of receiving a salary and no such a payment was credited while other unexplained transactions are carried out in the account, which suggests the use of a 'mule account.'
52. A customer submits documents suspected to contain any materially false, fictitious or fraudulent statement or entry.

53. Supporting documents that contain vendor receipts and/or other supporting documents that appear to be altered (obvious white-out areas, cuttings, deletions).
54. A customer uses a different IP address from what is known in his/her profile.
55. A customer image looks unusual or is found under a different name/profile in open source data.

Crypto-related activities

56. Transactions involving an unlicensed virtual asset provider or unknown crypto exchange provider.
57. Significant unusual transfers of funds to or from crypto exchange providers, particularly when such transfers are not in line with the customer's usual transactional behavior.
58. Credits or deposits in the customer's account from multiple or unrelated parties and shortly transferred to cryptocurrency exchange-related entities.
59. The use of multiple cards under different names while purchasing crypto currencies.
60. Transactions involving cryptocurrency exchanges or large crypto purchases by a customer who has no previous known interest or transactions in digital assets.

12. CASE EXAMPLES

Case example 1: Possible money laundering of crypto- related fraudulent proceeds

The UAEFIU received multiple STRs from different reporting entities against **Subject A** and its affiliated companies where he/she is identified as the beneficial owner.

Open source data revealed that the subject was involved in a cryptocurrency scam. The subject was a founder of a fraudulent cryptocurrency platform abroad that led to legal procedures against the subject and charges of fraud, tax crimes, and money laundering by his/her home country.

Subject A opened multiple personal and business accounts in different currencies with several financial institutions in the UAE, as well as establishing multiple companies in the same period of time licensed for different services, including consultancy, software, and customer services.

The UAEFIU analysis showed that Subject A engaged in a series of complex financial transactions, wherein funds received in the subject's account were from multiple unrelated third parties. Subsequently, the funds were moved and layered between own personal and business accounts and counterparties. Furthermore, circular movement of funds was noted from one affiliated company account to other owned companies in a different currency. Thereafter, funds were remitted to other counterparties within the UAE and foreign jurisdictions.

Subject A was suspected of establishing a network of shell entities in the UAE with no actual genuine business to launder the foreign proceeds of fraud. The case was ultimately disseminated by the UAEFIU to the concerned LEA for further investigation and action.

Risk indicators:

1. Adverse media and a positive match suggest links to cryptocurrency scams and criminal charges.
2. The customer has multiple bank accounts in different currencies with several financial institutions.
3. The establishment of multiple companies in a short period showing no business operations.
4. Funds that are transferred in a circle between affiliated companies, personal accounts, and third parties.
5. Suspicious transaction patterns with funds received from multiple unrelated or unknown third parties engaging in complex financial transactions.

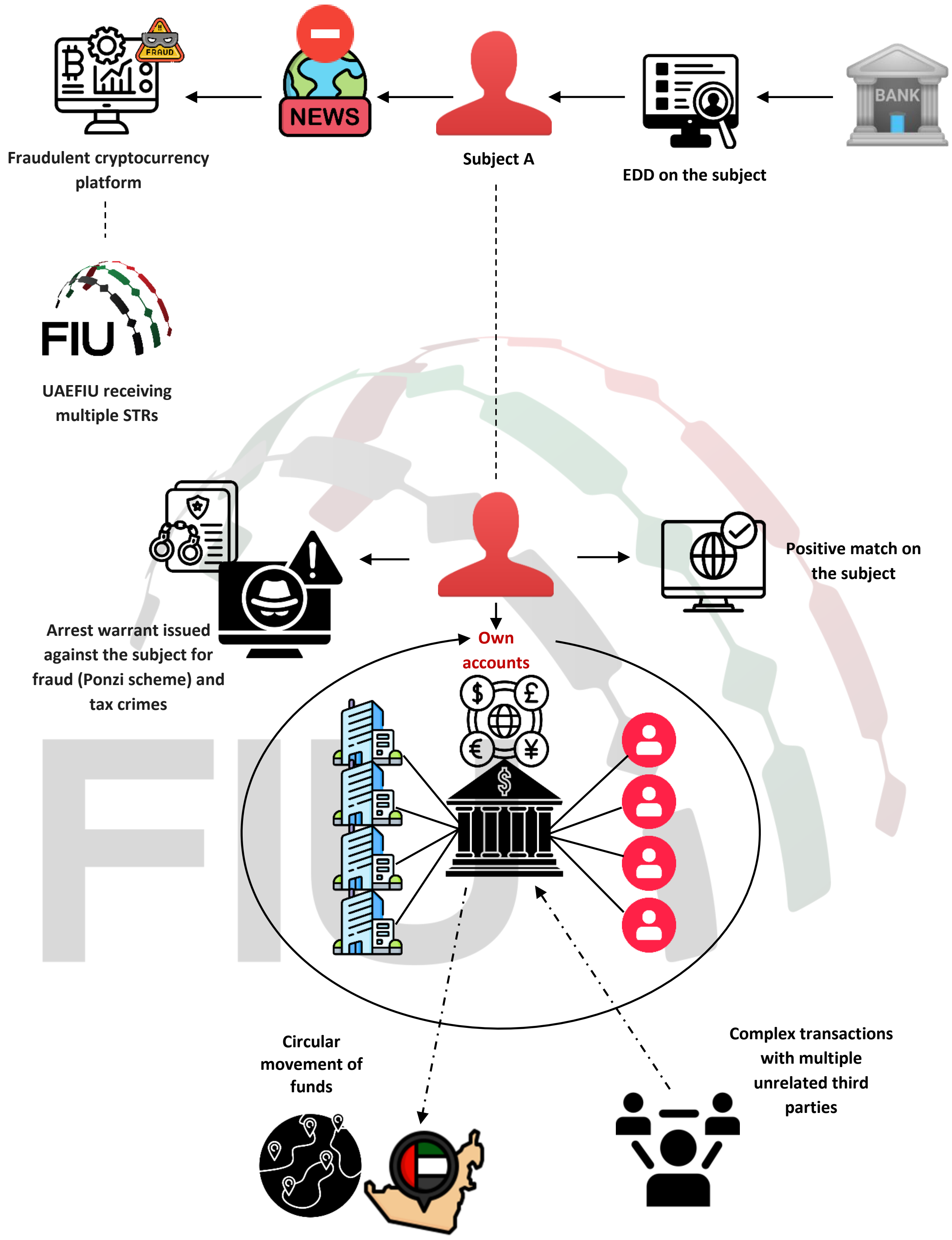

FRAUD
NEWS
BANK
Fraudulent cryptocurrency platform
Subject A
EDD on the subject
FIU
UAEFIU receiving multiple STRs
Arrest warrant issued against the subject for fraud (Ponzi scheme) and tax crimes
Positive match on the subject
Own accounts
Circular movement of funds
Complex transactions with multiple unrelated third parties

Diagram 2: *Possible money laundering of crypto- related fraudulent proceeds*

Case example 2: Laundering the proceeds of foreign fraud through money mules

International intelligence received from a counterpart FIU indicated that Company C, a foreign entity established in Country (X), was defrauded through the technique of business email compromise by foreign **Company A** and **Company B**, causing a financial loss of millions of dollars. Simultaneously, different UAE banks received recall requests from the remitting banks of Company A and Company B.

The UAEFIU analysis showed that multiple mule accounts in the UAE were recruited by the subject foreign companies, along with a network of local newly established entities, based on different STRs that were raised on some of said mule and corporate accounts. The common reason for reporting was that of receiving unusual wire transfers overseas from Company A and Company B.

Analysis also indicated that these mule and corporate accounts were recruited and established over a short span of time to receive the foreign fraudulent proceeds generated by said companies in Country X. Subsequently, the funds were circulated and layered among the involved suspected parties, in addition to other third parties and money mules. Afterward, funds were immediately utilized through cash and cheque withdrawals.

Additional international intelligence informed the UAEFIU that Individual X is a member of a foreign organized group found to be impersonating another person and using his/her identity in obtaining bank accounts of Company A and Company B in Country X.

Further investigation by the UAEFIU in cooperation with the concerned local LEA and the utilization of international intelligence linked Individual X with third parties in the UAE and revealed a further 15 new individuals in addition to previously identified mules and corporate accounts. It was also found that foreign fraudulent proceeds were suspected to be laundered through several jurisdictions, including the UAE, wherein some of these proceeds were also utilized for the purchase of high-value items such as luxury vehicles, watches, and real estate in the UAE.

Ultimately, freeze orders were issued on said local accounts and information disseminated to law enforcement and the counterpart FIU for further investigation and action.

Risk indicators:

1. Individuals with low income receiving multiple transfers from a business established in a foreign jurisdiction.
2. An account of a newly established legal person receiving a high volume of funds over a short period from foreign entities and unknown counterparties.
3. Accounts exhibiting large incoming remittances followed by immediate cash or cheque withdrawals.

4. Complex transactions designed to obscure the tracing of funds by moving them among multiple accounts.
5. Unclear sources and destinations of funds due to insufficient supporting documentation and deviation from the declared profiles.
6. Multiple ‘funds recall requests’ received from the remitting banks on the same subjects.
7. Individuals covering their faces while withdrawing funds from ATMs to avoid appearing in surveillance footage.

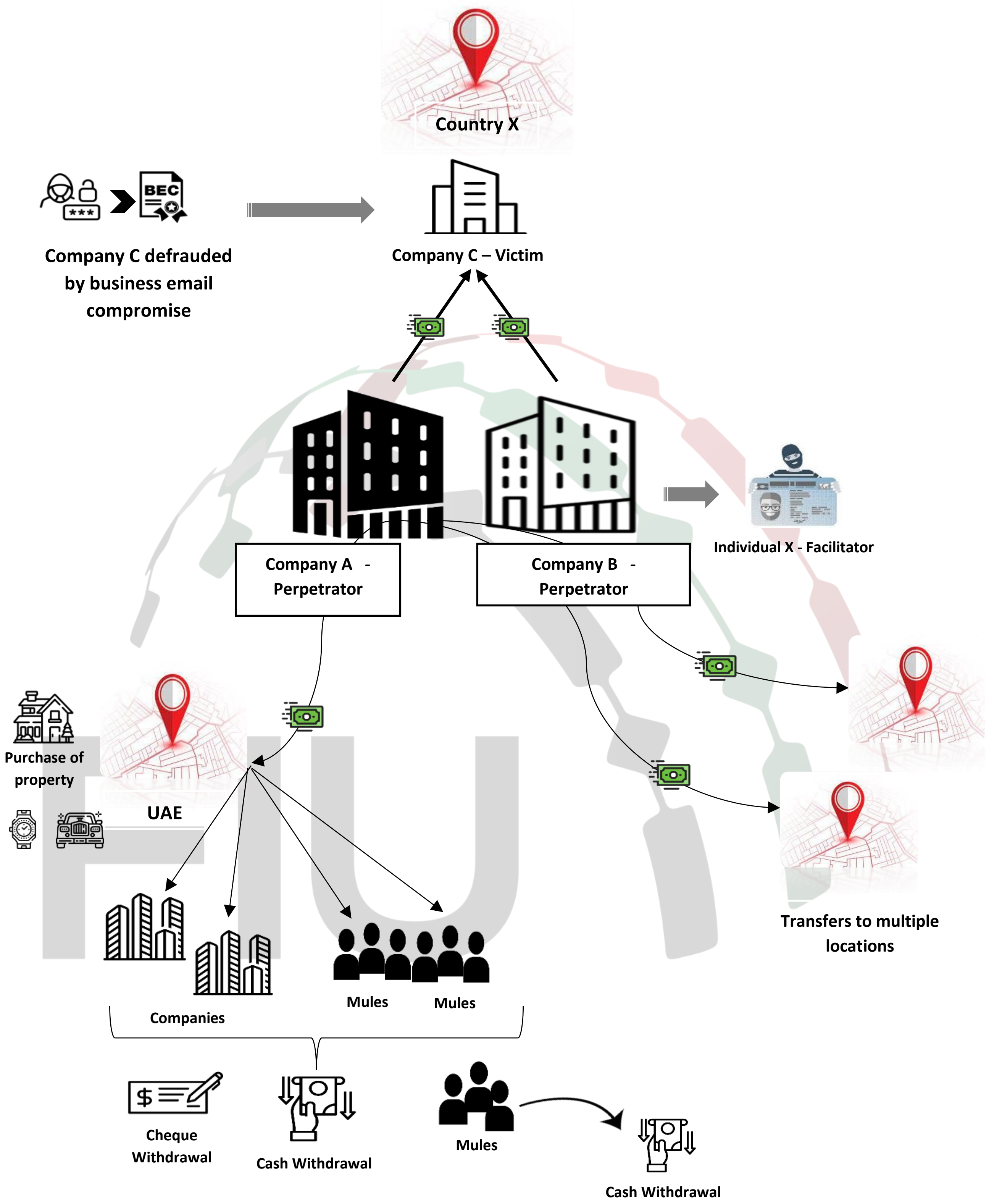


Diagram 3: *Laundering the proceeds of foreign fraud through money mules*

13. CONCLUSION

This report provided thorough information crucial to the UAEFIU stakeholder's understanding of fraud enablers and emerging techniques, and its risks involving organized crime groups, as well as its consequences in terms of financial loss. Furthermore, a list of risk indicators was developed to guide reporting entities and investigative authorities in detecting and investigating fraud incidents.

Despite the significant efforts and preventative measures against fraud, data utilized in this report affirm that fraud remains a significant threat at the national and global levels, leading to money laundering, mainly due to the complexity and sophistication of the used methods involving advanced technology. Fraud practitioners in the UAE from reporting entities, investigative authorities, and prosecutors not only indicated different challenges encountered in practice but also suggested valuable solutions and recommendations to UAE decision makers from both the public and private sectors.

Suggested solutions included not only actors involved in fraud prevention but also the public and the role of their awareness in protecting themselves from falling victim to fraudsters' schemes. These are in addition to the role of domestic cooperation, information sharing, and international collaboration in effectively tackling the observed increasing scale of fraud incidents at both global and national levels.

The following highlights some of the valuable recommendations and insights included in this report by the UAEFIU's stakeholders:

1. Identifying and understanding factors associated with fraud incidents would guide financial institutions in building their defense against potential system vulnerability and strengthening their anti-fraud mechanisms that could potentially prevent future incidents.
2. Continuing to identify and report potentially fraudulent transactions and unusual activities processed across financial institutions. Swift reporting following the fraud incident, the quality and comprehension of reported activities and transactions, and indicating all possible involved parties are key to enabling the UAEFIU and law enforcement authorities to build a successful case and trace and freeze criminals' proceeds in a timely manner. Fraud detection and investigation are time-sensitive and require evidence gathering and thorough analysis.
3. Promoting fraud awareness is a culture. Staying updated about emerging trends and risk indicators regarding fraud and testing institutions' monitoring systems against them are crucial in fraud prevention.
4. Ensuring that organizations have a clear policy and guidance on handling internal fraud claims involving organizational staff needs to be considered.
5. Password-based systems and OTPs are vulnerable to cybercriminals. Therefore, there is an essential requirement to move toward more effective and more secure mechanisms to

protect financial institutions’ customers, such as applying multifactor authentication, biometric and IBAN verification, real-time detection, and monitoring third party applications.

6. Tailoring institutional fraud risk management strategies and roadmaps based on the organization size and the scale and types of fraud schemes that it witnesses, as well as identified potential root causes, taking into consideration the organization’s measures for fraud control and monitoring activities and any associated corrective actions.
7. Frequently educating financial institutions’ customers about fraud schemes and how to avoid them.