Strategic Analysis Report on Fraud as a Component of Money Laundering Crimes

Financial Information Unit

(FIU)

February 2024

www.fiu-ye.com

Introduction:

Fraud is one of the most prevalent money laundering crimes that has spread in the Republic of Yemen due to the country's current political situation. Most victims are from the impoverished segments of society. These victims are often exploited when they seek the humanitarian assistance provided by charitable and humanitarian organizations. Other fraudulent methods – such as Ponzi schemes – are also being used to exploit the people of Yemen.

Since its reformation in 2020 through the end of 2023, the Aden-based Financial Intelligence Unit (FIU) received 54 Suspicious Transaction Reports (STRs), 29 of which were determined to involve fraud and forwarded to the concerned enforcement authorities. Article (31)(z) of Law No. (1) of 2010 (Yemen's AML/CFT Law) requires the FIU is to publish periodic reports on its activities, as well as statistical data and analytical studies in the field of combating money laundering and terrorist financing. In fulfilment of this statutory mandate, the FIU analyzed each of the STRs and took the following actions:

- Referred the STR and the financial analysis to the CBY's legal department for the conduct of a legal assessment;
- If the financial analysis and the legal assessment confirms the suspicion of the reporting entity: submitted the analysis and assessment - together with the relevant evidence - to the concerned authorities.
- If the suspicion of the reporting entity is not confirmed, maintained the STR in the FIU's records.
- Provided feedback to banks and other reporting entities to ensure continuous professional care and monitoring of their clients' financial transactions to prevent their accounts from being used to facilitate fraudulent activities.
- Report the STR to counterpart FIUs abroad if the subject of the STR is linked to persons operating outside Yemen.

The Objectives of this Strategic Analysis Report

This Strategic Analysis Report is the first produced by the Aden-based FIU since its reformation in 2020. Through its analysis of the detailed statistical data and information concerning STRs that are related to suspected fraud, the FIU has been able to determine the relevant indicators and to identify the trends and patterns with respect to fraud.

The objective of this report is to provide to financial and non-financial institutions and other reporting entities with the indicators that will assist them with recognizing the methods, sectors, schemes, and related circumstances that characterize fraudulent operations; and with developing controls to reduce fraudulent activities and protect the general public - especially vulnerable populations - from falling victim to fraud. As just noted, one aim of this report is to assist reporting entities with developing preventive measures that limit the opportunities for fraud, including (i) establishing training and capacity-building efforts that focus on the methods most often used to carry out criminal activity, (ii) identifying areas for improvement, and (iii) developing strategic initiatives to enhance methods for combatting money laundering.

The importance of this Strategic Analysis Report lies in fulfilling the FIU's obligations in combating financial crimes and protecting the integrity of the financial system. Additionally, this report provides valuable insights into the nature of the evolution of money laundering activities; and these insights will assist with shaping policies, legislation, and strategies.

The Legal Framework for The Crime of Fraud

According to the provisions of the Penal Code Article (310), "A person who, without right, obtains a financial benefit for himself or another by fraudulent means or by adopting a false name or untrue capacity shall be punished by imprisonment for a term not exceeding three years or by a fine."

As provided in the Penal Code, at the core of the crime of fraud is a lie that deceives a victim and results in the delivery of money from the victim's funds to the perpetrator. Despite its various forms, the core of the crime of fraud is the same, and the law specifies the following examples:

I. Using fraudulent methods to deceive people into believing in a false project or fabricated event, creating hope for fake profit or the repayment of the amount taken by fraudulent means, or deceiving them into believing in the existence of an invalid promissory note or forged settlement.
II. Dealing with immovable or movable property that is not owned by the perpetrator and in which they have no right to dispose of.
III. Adopting a false name.
IV. Adopting an untrue capacity.

Furthermore, Article (3) of Yemen's AML/CFT Law – and the executive regulations issued under that law – specify that the crime of fraud is considered a predicate offense that results in criminal proceeds.

Impact Of Fraud on Society:

Victims of fraudulent activities experience various negative consequences, such as:

- Financial losses.
- Psychological pressure, which may cause emotional distress that affects the victim's mental health and quality of life.
- Many victims feel embarrassment or shame in society due to falling victim to fraud, leading to the underreporting of incidents.
- Lack of trust in the institutions through which the fraud occurred.

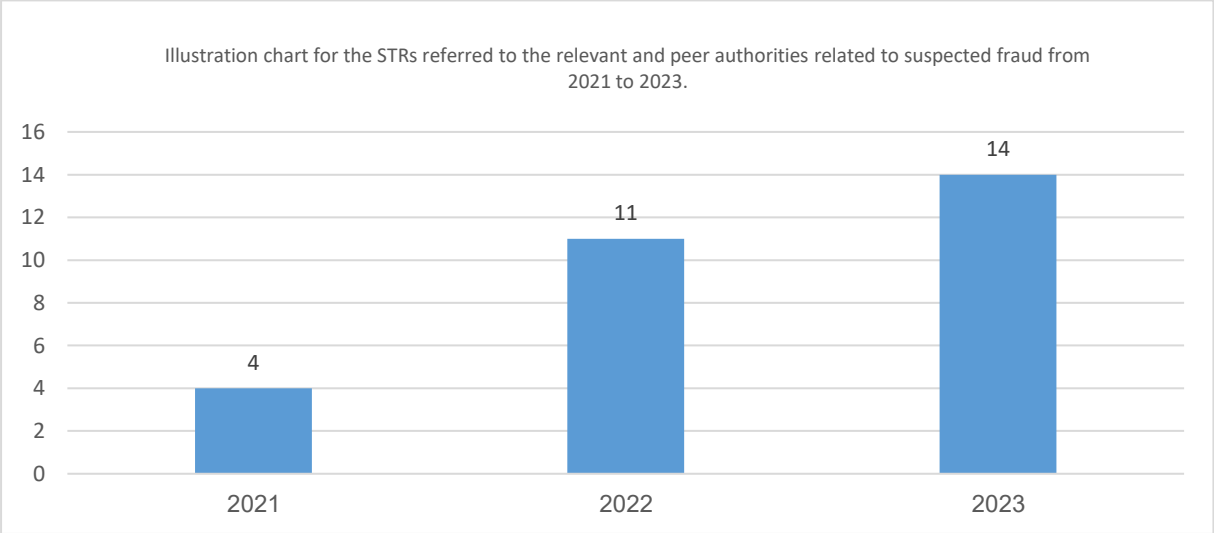
Environment of the Strategic Analysis Report Study:

The FIU analyzed 29 STRs received during the period 2021-2023 that were determined to involve fraud. The analysis of these STRs identified indicators that were determined by the FIU to confirm the suspicion of fraud. The FIU referred the STRs and its analysis to the CBY's legal department for the conduct of a legal assessment, which was then forwarded to the competent authorities.

Results of Analysis of Reports Related to Suspected Fraud During the Period from 2021 to 2023

Statistical Data:

The Number of STRs Received and Referred to The FIU Regarding The Crime Of Fraud From 2021 To 2023.				
Data	**2021**	**2022**	**2023**	**Total**
Received STRs	**12**	**16**	**26**	**54**
STRS referred to the relevant authorities.	**4**	**10**	**14**	**28**
Spontaneous STRs from counterpart FIU	**0**	**1**	**0**	**1**

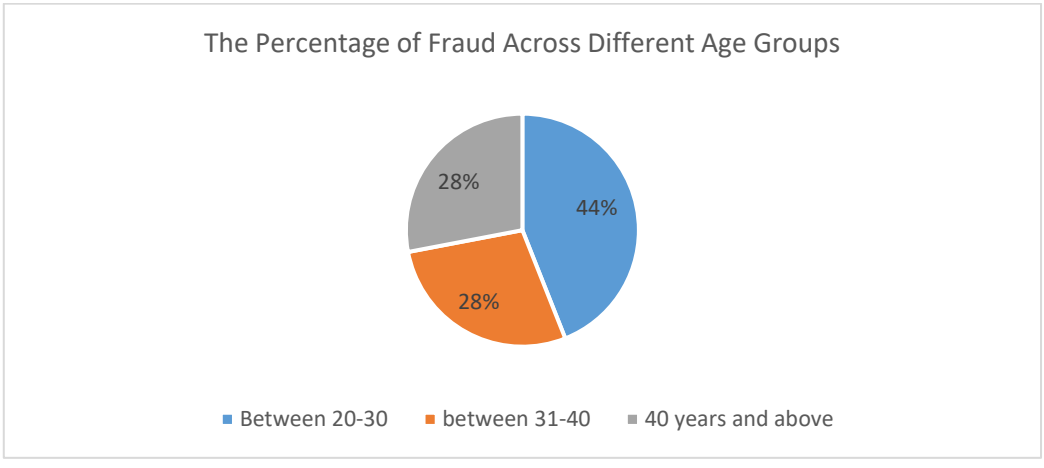


Key Findings from The Analytical Examination of Data on Reports Related to Suspected Fraud:

1. Fraudulent activities are often perpetrated by organized groups or companies rather than individuals, especially in cases related to Ponzi schemes.
2. There is no consistent pattern regarding the amounts fraudulently obtained by individuals as profits from pyramid marketing groups. The amounts vary depending on several factors, including the

seniority of the person, the internal policy of the group/company in profit distribution, and the hierarchical network of affiliated persons.

3. Fraudsters exploit the desperate need of vulnerable and poor individuals for humanitarian, relief or medical assistance by soliciting money in exchange for completing registration or subscription cards with relief organizations. They aim to benefit from the humanitarian services or medical assistance provided by these organizations, whether domestically or internationally.
4. The average fraudulent amounts obtained under the pretext of registration fees or subscription cards related to exploiting people's need for humanitarian and relief assistance range from 80 to 100 Saudi Riyals, or their equivalent in other currencies, which may fluctuate.
5. There is no consistent pattern for the amounts obtained fraudulently from victims in exchange for promises of medical treatment, lottery tickets, competition prizes, or other mythical rewards.
6. Fraudulent solicitation of money by impersonating prominent figures in Yemen, such as ministers, security and military leaders, or their office managers, tends to involve relatively large amounts. This method typically targets close friends, traders, and acquaintances of those figures.
7. The age of those seeking financial returns from fraudulent operations ranged between 20 and 66 years old. Of all perpetrators, those aged 20-30 accounted for 44%. Those aged 31-40 accounted for 28%, as did those aged 40 years and above. The following chart illustrates this:



8. Males represent the majority of those using fraudulent methods: males accounted for 83% compared to females at 17%.

9. Suspects in fraudulent activities prefer using financial transfers (remittances) for sending and receiving fraudulent amounts primarily through exchange companies and secondarily through banks, with 54% using exchange companies compared to 46% using banks.
10. Fraudsters use multiple phone numbers to receive fraudulent funds, with some numbers used by more than one person, indicating that some fraudulent activities occur within organized networks.
11. Fraudsters impersonate individuals or employees belonging to corporate entities (banks - exchange companies) and request the victim to send their personal login code to the electronic service under the pretext of providing technical support services, updating or upgrading the service or system, performing maintenance, or other false reasons solely for the purpose of fraud.
12. Fraudsters exploit the ignorance and lack of knowledge of the public about the legal status of some financial transactions or obligations, such as selling frozen or cancelled dollars at less than the market price, especially if they are not counterfeit.
13. Fraudsters use temptations and fictional/mythical beliefs in fraudulent schemes.
14. Fraudsters deceive victims into believing they will receive financial prizes from well-known and reputable corporate entities such as those offered by the Alwaleed bin Talal Foundation and others.
15. Fraudsters deceive victims into believing they will receive financial prizes through luck or chance.
16. Fraudsters utilize technological means to complete fraudulent operations as illustrated in the following table:

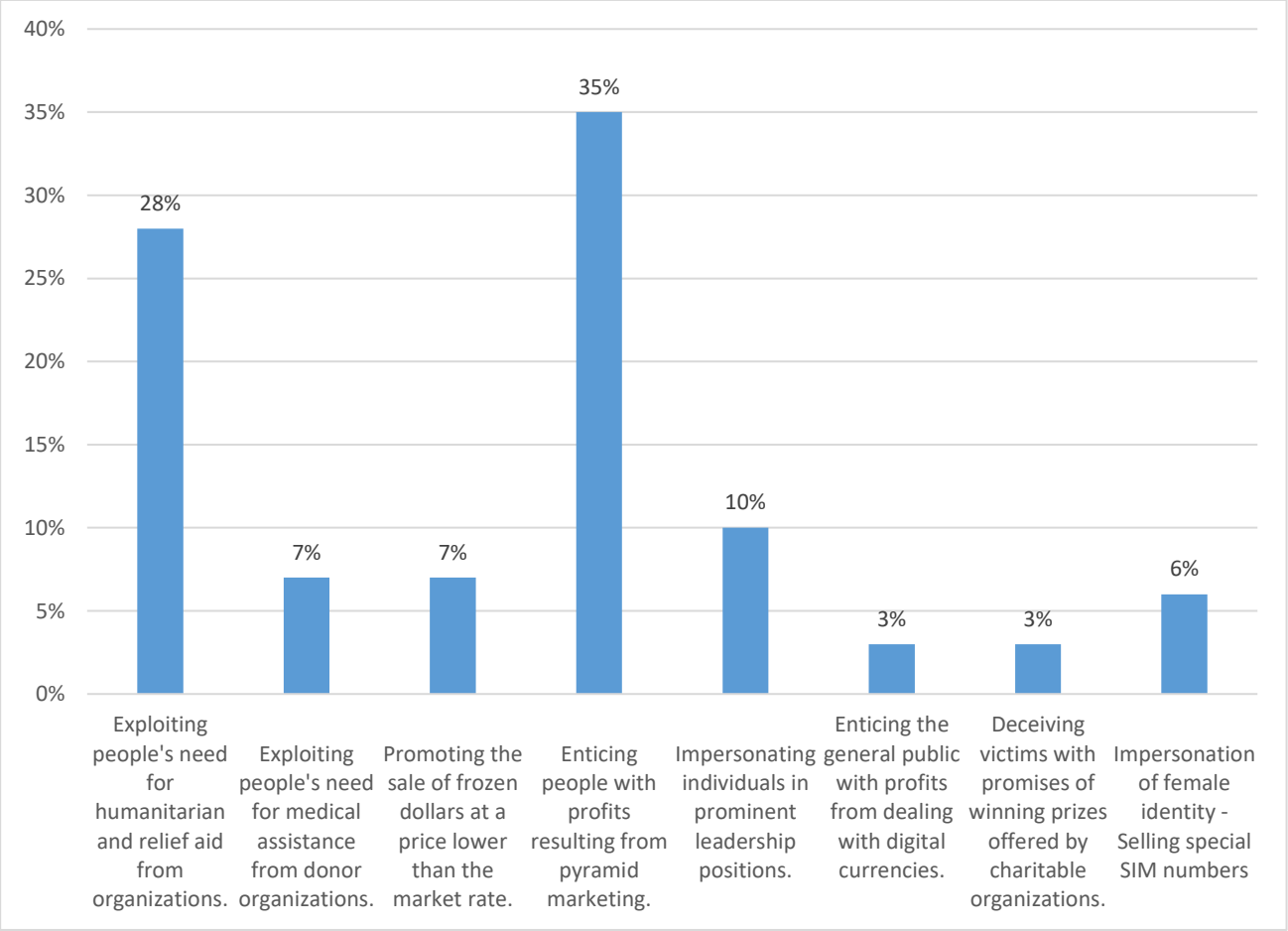
The means used to commit fraud	**Percentage**
Phone Calls	10%
SMS	28%
Using social media platforms (e.g., WhatsApp, LinkedIn, Facebook, YouTube)	62%

17. Fraudsters prefer to use domestic and international transfers more than other banking products, with 64% of them using transfers compared to 36% using deposits and others.
18. Fraudsters exploit network marketing companies and platforms that are prevalent in the community, such as:
    - B4U Company

- Silwana Diamond Company
- Jocial Company
- StarLike Platform
- Royal-Q Platform

19. Fraudsters employ the method of offering investment services through purchasing digital or encrypted currencies like Bitcoin and other cryptocurrencies. These are decentralized, encrypted assets that operate continuously without interruption, immune to inflation, unaffected by monetary policies or bank decisions, and do not require intermediaries or credit cards for transactions, with minimal transfer costs.

The following chart illustrates the methods used in the fraud process and the percentage of usage for each method.



Recommendations To Mitigate the Risks of Fraudulent Activities:

1. Enhance awareness in Yemen about the importance of vigilance and caution to avoid falling victim to fraud crimes through educational initiatives, awareness campaigns, and various media channels.
2. Financial institutions and exchange companies providing money transfer services should adhere to the laws, regulations, and guidelines issued by the Yemeni Central Bank regarding transfers, financial transactions, combating electronic financial crimes, verify the real beneficiaries' identities, understand the purpose of financial transactions, and establish a mechanism to alert citizens of the possibility of becoming victims of fraud.
3. Establish an independent function to combat fraud and cybercrime in financial institutions, exchange companies, and other relevant authorities, and build their capacities in identifying indicators related to such crimes.
4. Urge financial institutions, exchange companies, and other relevant authorities to conduct periodic risk assessments of fraud and implement measures to mitigate these risks. Provide guidelines to alert customers of the possibility of falling victim to scams and provide them with the necessary procedures to follow if they suspect or become victims of such illegal practices.
5. Take steps to prevent the exploitation of their systems to commit scams and fraud and exercise due diligence to verify the legitimacy of transactions executed on their customers' accounts to ensure they do not involve any indicators of fraud and are consistent with the bank's information about customers and their activities.
6. Banks and exchange companies offering financial services through electronic means or payment systems should put more effort into educating their clients not to share any personal data such as user IDs or personal login codes with anyone.
7. Every reporting entity must report any actual of attempted fraudulent activity involving their clients to the FIU without delay and include all data and documents that will assist the FIU to conduct a financial analysis to trace the money.
8. Establish an independent function within the investigation and prosecution authorities responsible for investigating fraud and cybercrimes, provide them with the necessary qualified and trained resources, enhance cooperation with the financial information unit to provide them with reports submitted by citizens regarding the proceeds of such crimes abroad, and take necessary actions and communicate with counterpart units to request the recovery of those funds.

9. There should be effective and appropriate controls, instructions, or regulatory mechanisms within the regulatory authority for the communications sector regarding granting mobile phone lines or numbers. All SIM card and internet activations should be linked to a national identity number or a valid passport. This is of paramount importance in assisting security authorities and investigative agencies in tracking the numbers used in fraud and electronic crimes and other crimes.
10. There should be effective and appropriate controls, instructions, or regulatory mechanisms within the regulatory and supervisory authority responsible for licensing commercial entities, especially those operating as platforms in the multi-level marketing sector. This includes some of the sample entities discussed in the conclusions section.

The Financial Information Unit - Aden

www.fiu-ye.com