# TRENDS REPORT

January – June 2023

## Table of Contents

## 1.0 PURPOSE

1.1 The Financial Intelligence Agency (FIA) is the central authority in Botswana to receive, request, analyse financial information and disseminate intelligence relating to suspicion of money laundering, terrorism financing, proliferation financing (ML/TF/PF) and other financial crimes to relevant authorities for investigation. This report provides a summary of the trends and patterns in suspected financial crime as observed in the suspicious transactions filed with the FIA.

1.2 The objective of this Trends Report is to share information on common suspected predicate offences in suspicious transaction reports and the methods employed to launder the proceeds of crime. This Report seeks to assist stakeholders in the anti-money laundering, countering financing of terrorism and proliferation financing (AML/CFT/CFP) sphere to better understand trends and methods employed by suspected criminals to launder the proceeds of crime.

## 2.0 SUSPICIOUS TRANSACTION REPORTS (STRs)

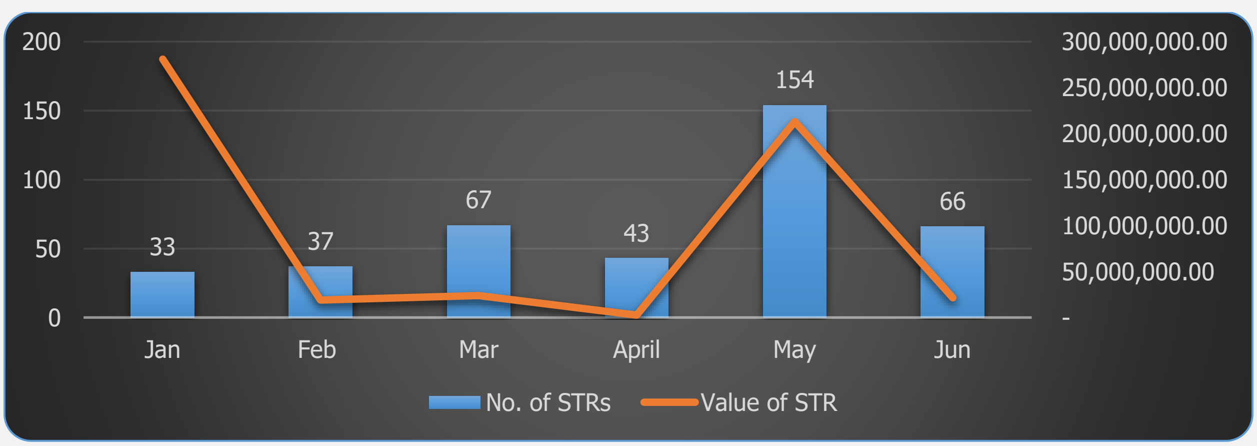
2.1 Recommendation 20 of the Financial Action Task Force (FATF) requires a financial institution to report promptly, to the Financial Intelligence Unit, suspicious transactions if it suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorism. Pursuant to this, Section 38 of the Financial Intelligence Act, 2022 obliges specified parties and accountable institutions to report suspicious transactions to the FIA. This report analyses STRs received from the various reporting institutions for the period January to June 2023.

**Table 1: Number and Value of STRs Received from January – June 2023**

| Business Type | Amount (BWP) | No. of STRs Received |
|---|---|---|
| Accountant | 276,056,233.00 | 3 |
| Asset Management | 25,000.00 | 1 |
| Attorney | 2,246.00 | 1 |
| Bank | 282,876,107.68 | 325 |
| Bureau de Change | 181,582.98 | 19 |
| Casino | 87,150.00 | 4 |
| Credit Unions | 1,017,000.00 | 2 |
| Money Value Transfer Service Providers | 644,313.50 | 43 |
| Virtual Asset Service Provider | 486,054.25 | 2 |
| **Grand Total** | **561,375,687.41** | **400** |

2.2 Table 1 above shows that during the period January to June 2023, a total of 400 STRs were received from various entities out of which banks accounted for 81.25%, followed by Money Value Transfer Service Providers with 10.75% and Bureau de Changes with 4.75%. The total value of STRs amounted to P561,375,687.41. Banks accounted for 50.39%, Accountants 49.17% followed by Credit Unions at 0.18% of the total value of STRs. Chart 1 below gives monthly data on the number and value of STRs received.

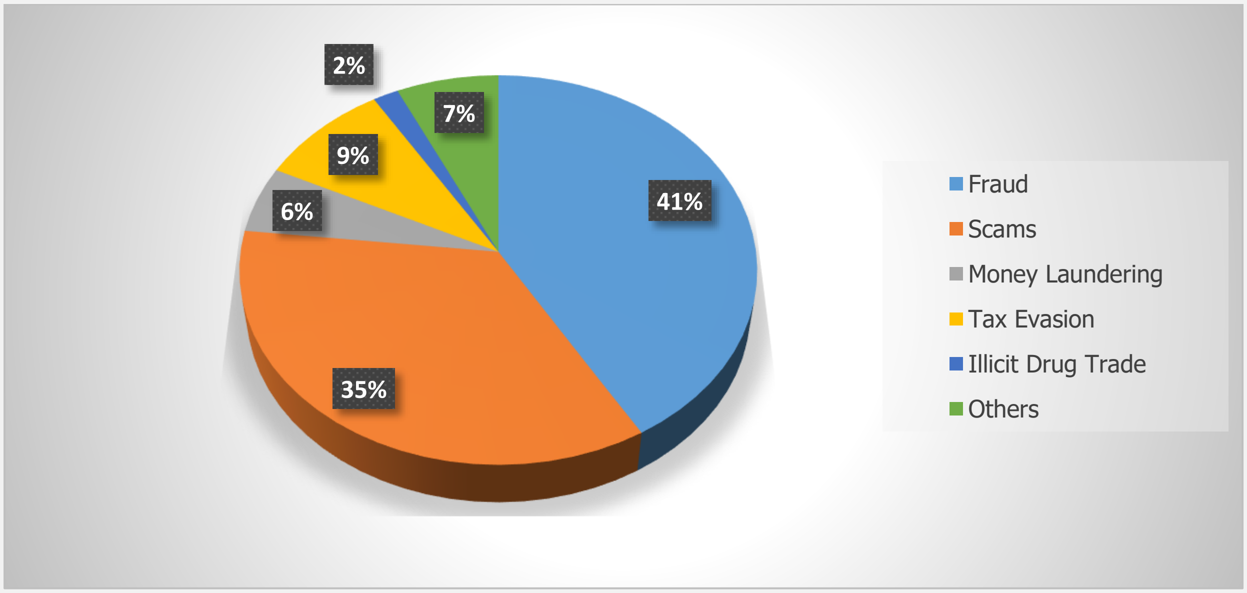
**Chart 1: Number and Value of STRs per Month**



2.3 Monthly data of the review period shows that the lowest number of STRs was 33, received in January 2023 and the highest number of reports was 154 received in May 2023. The high number of reports received in May were mainly linked to the Ecoplexus scam. The highest value of STRs was around P281 million recorded in January 2023 owing to a number of high value STRs filed. The average number of reports received monthly was 67.

## 3.0 SUSPECTED CRIMINAL ACTIVITIES

**Chart 2: Underlying Criminal Activity**

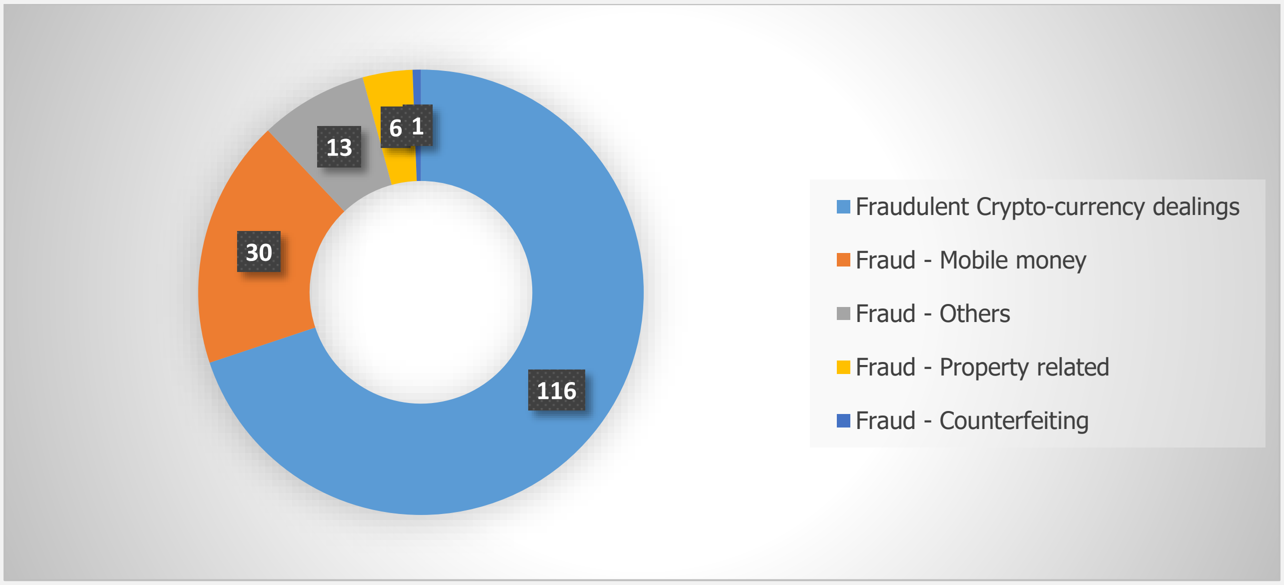



3.1 The most common suspected criminal activity was fraud at 41% followed by scams at 35% of the reported cases. Details are provided below:

## i) Fraud

Fraud means obtaining something dishonestly or by deception. The observed forms of fraud involved unauthorized acquisition of personal and financial information without the victim's knowledge. 165 STRs relating to such forms of fraud were received during the review period, as reflected in Chart 3 below:

**Chart 3: Number of STRs per suspected fraud type**




### a) Fraudulent Crypto-currency and Forex Dealings

Unsuspecting individuals were lured into sending money to criminals for supposedly investing in crypto-currencies or forex trading. The fraudsters present as brokers or forex trading educators who purport to invest and teach people how to trade online. In most cases, the fraudsters do not have operating licences nor training qualifications to offer the trainings. Out of 165 STRs received, 116 STRs were in relation to fraudulent crypto-currency and forex dealings.

**Modus Operandi:**

**Social Media:** The majority of crypto-currency and forex dealings are facilitated through social media. To illustrate, Victim A gave Trader X P68 000 as investment to trade in forex but later realised that she was being deceived as she had not benefited anything from the investment despite her large initial capital. Further, she realised that her Facebook account was hacked. The hacker was suspected to have been working with Trader X and contacting numerous culprits from Victim A's Facebook friends claiming that the Victim had financial problems and needed assistance. The culprits were requested to credit the money into Trader X's account.

Most of the funds were used for personal expenses or transferred into other bank accounts, with minimal going towards trading or investment. Often times, the fraudsters display their lavish lifestyles on social media. This is done to entice and lure people into "investing".

**b) Mobile Money Fraud**

With the increase in the use of mobile money services, the fraud associated with these services also continues to grow. It was observed that fraudsters used various methods such as bank to wallet fraud, fake give aways and fake SMSes.

**Modus Operandi:**

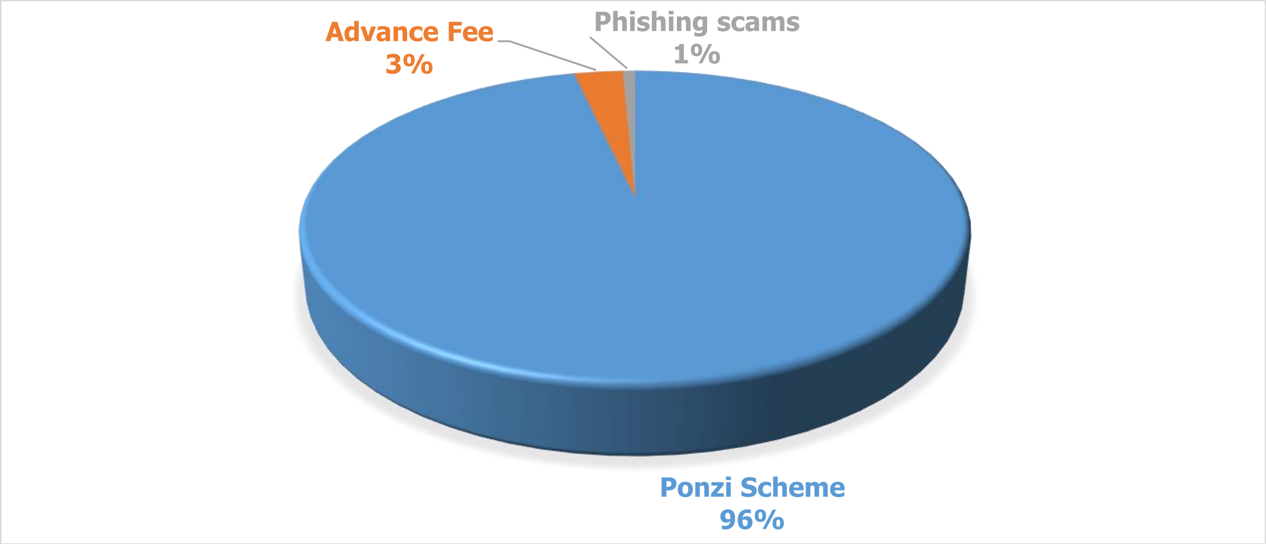
**Bank to Wallet Fraud:** Between the months of January and March 2023, there was a rise in bank to wallet fraud incidents involving illegal access to victim's sensitive personal and financial data in order to gain access to their bank accounts. The fraudsters transferred money from the victim's bank accounts to their own e-wallet accounts and thereafter withdrew funds through the automated teller machines.

**Fake SMSes**: This involves the sending of a fake SMS indicating a deposit into the victim's mobile money account. The fraudster then calls the victim claiming to have credited the wrong account and thereafter requests reversal of the funds. Victims who do not confirm their mobile money account balances before reversing the alleged transaction are swindled of their money.

**Fake Give-Aways:** Fraudsters make phone calls impersonating mobile network employees and trick victims into disclosing their financial information. The victims are usually told that their mobile number has won money from some competition and that the funds will be credited to their mobile money or bank account. This is used as a pretext to steal people's personal information. Once the fraudster gain access to the victim's account, they disappear without delivering the promised prize and exploit the victim's account usually through online purchases. In some cases, they would ask for the victim to pay a fee to cover "transaction cost" associated with delivering the prize.

## ii) Scams

**Chart 4: Scams observed in STRs**




a) **Ponzi scheme:** A Ponzi or pyramid scheme is a fraudulent investment, which involves using payments collected from "new investors" to pay off the "earlier investors". The scheme often promises to invest the participant's money to generate high returns.

**Modus Operandi:**

The bank accounts involved received frequent deposits from members of the public, mostly made through automated deposit taking machines and other platforms such mobile banking. The primary accounts receiving the funds were business and personal accounts. The individuals who used their personal accounts to run the scheme were Batswana, mostly aged 30 years and below and also had newly registered companies which were also used to receive funds from the public.

Numerous inter account transfers were observed among recipients and some transfers to early "investors" as purported return on investment. It was also observed that, following receipt of funds from the public, transfers were also made to another group of entities which then transferred the funds out of the country mostly to Asian countries. This group of entities were all under the shareholdership of a group of Chinese individuals.

b) **Phishing Scams:** This is a technique used to illegally acquire sensitive data such as financial information. The scam was perpetrated using email or websites in which the fraudsters masqueraded as a legitimate business or reputable person.

**Modus Operandi**

*Case Study:* Client Y and her purported boyfriend targeted a certain company through an email phishing scam. They were able to get hold of bank login credentials and other sensitive information for the company account. The client informed the bank that her boyfriend that she met through an online dating site used her bank account to scam the company. The client indicated that she was directed to keep a certain portion of the money and send the outstanding balance to a beneficiary in South Africa.

c) **Advance Fee Scams:** This scam typically involves promising a victim a significant amount of money or gifts, provided the victim pays a small advance payment.

**Modus Operandi**

To illustrate, a victim remitted funds to a female recipient in South Africa who turned out to be a scammer. The recipient befriended individuals through social media platforms. After a few months of chatting with the victims, and gaining their trust, they were informed that gifts such as money and goods will be delivered to them. The scammer would then give banking details for the victim to remit funds to cover the customs clearance fees, transport etc. Once the funds are remitted, the scammer disappear and the promised parcels are never delivered.

In other cases, victims sent funds to recipients located in Nigeria. The victims were members of a certain church and met pastor "Anna" on Facebook. Pastor "Anna" informed the victims that she had a company that offered loans to Christians all over the world. Victims were conned into making purported upfront payment as administrative fees for processing of the loans.

## iii) Money Laundering

**Chart 5: SUSPICION OF MONEY LAUNDERING ACTIVITIES**

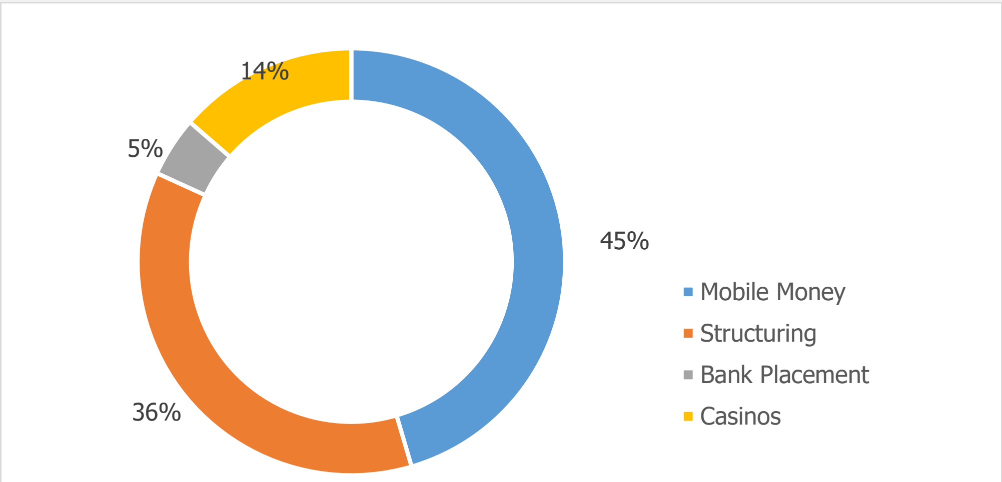



**Table 2: AMOUNTS INVOLVED IN SUSPECTED MONEY LAUNDERING ACTIVITIES**

| Suspected Money Laundering Methods | Amount Involved |
|---|---:|
| Casino | 37,150.00 |
| Mobile Money | 89,310.50 |
| Bank Placement | 190,000,000.00 |
| Structuring | 893,843.98 |
| **Total** | **191,020,304.48** |

The Agency has received several Suspicious Transaction Reports where it is suspected that some individuals are placing proceeds of crime in the financial system. The first chart shows that the highest number of STRs received relating to money laundering were in regard to laundering done through mobile money platforms. However, the amounts for these STRs are very low as indicated in Table 2.

**Modus Operandi:**

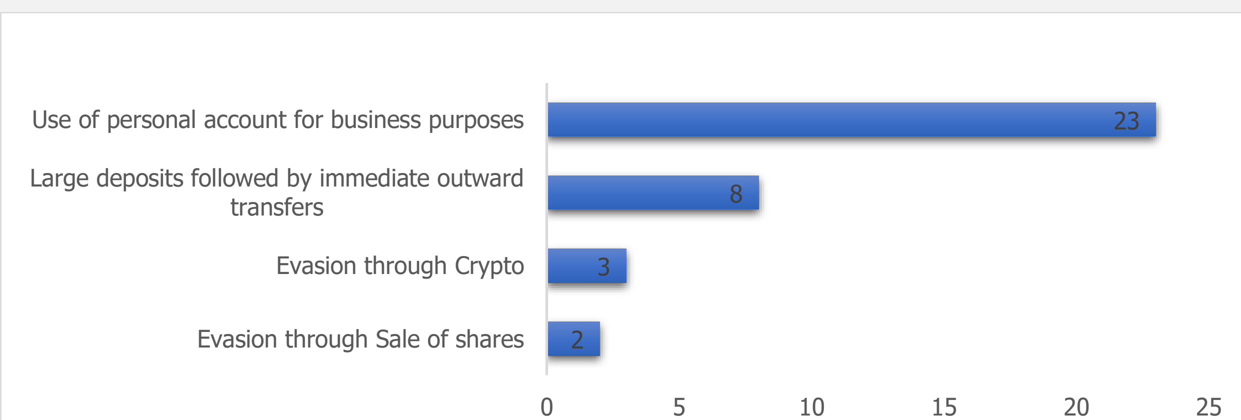
**International Receipts through mobile money accounts**: The FIA received several STRs from a mobile network operator indicating that a customer would receive a transfer into their mobile money account. This deposit will then be followed by a phone call from an unknown number indicating that the money was sent by mistake and instructed to send it back to a stipulated international number. In some cases, the fraudsters recruit recipients of the funds to work for them by continuing to send the funds outside the country as they come in.

**Use of Casinos for money laundering**: The FIA received reports from Casinos relating to suspected money laundering through their platform. Of the cases reported, the following methods were observed:

**Casino Dealings: Cash in, Cash out** – A trend was observed where casino chips were purchased and cashed out without playing. This behaviour is typical of classic money laundering cases.

## iv) Tax Crimes

Chart 6: Number of STRs received relating to Taxation



a) **Use of Personal Accounts for business transactions:** A trend was observed where businesses, mostly sole trader businesses, used personal accounts for business transactions. In most cases, only the business account is disclosed to Botswana Unified Revenue Service and not the personal account. We therefore conclude that the risk of using personal accounts for business transactions to evade taxes is high in such situations.

b) **Large cash deposits followed by immediate outward transfers**: There was a continuing trend where large cash deposits were made which are then followed by immediate transfers outside the country. The deposits were said to be for purchasing of stock from Asian countries. However, comparison with customs declaration records has revealed very little to no imports. Most of the companies reported for this behavior have registered for tax but appear to pay very little taxes relative to the volume of funds transferred outside the country.

## 4.0 CONCLUSION

During the period under review, banks accounted for 81% of the Suspicious Transaction Reports (STRs) received. The prevalent suspected predicate offenses primarily centered around fraud and scams. Mostly, the STRs involved fraudulent activities, wherein funds were unlawfully obtained from the public. Notably, the banking sector bore the burden of these fraudulent activities, with a significant portion of the reported cases being linked to bank transactions. This calls for robust AML/CFT measures within the banking sector, to safeguard against financial crimes.

## 5.0 RECOMMENDATIONS

Reporting entities and FIA should improve their public education framework to facilitate timely issuance of alerts to customers and the general public regarding prevailing risks and trends in financial crime. In that regard, it is recommended for FIA to issue a Media Advisory to that effect.