



Republic of Botswana

FIA

FINANCIAL INTELLIGENCE
AGENCY

TRENDS REPORT

JANUARY-DECEMBER
2021

Table of Contents

1.0	PURPOSE	3
2.0	SUSPICIOUS TRANSACTION REPORTING	3
3.0	OBSERVED FINANCIAL TRANSACTION TRENDS	4
4.0	FRAUD – OBTAINING BY FALSE PRETENCES	5
5.0	USE OF PERSONAL ACCOUNTS FOR BUSINESS TRANSACTIONS	7
6.0	CHURCH AND ROMANCE SCAMS	7

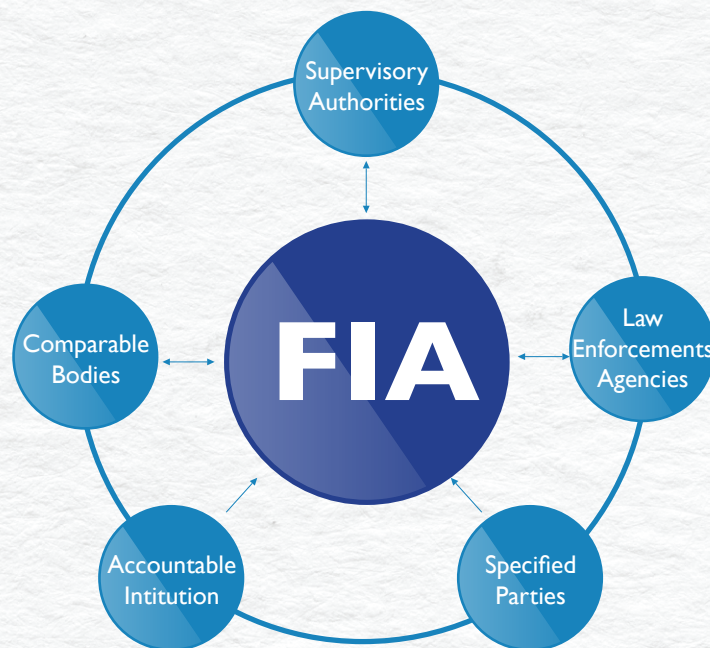


1.0 PURPOSE

1.1. This report highlights trends in financial crime observed by the Financial Intelligence Agency (FIA) during the period January to December 2021. The trends were developed from Suspicious Transactions Reports (STRs) filed with the FIA by reporting entities, financial intelligence received from domestic law enforcement agencies and other financial intelligence units. The purpose of the report is to provide a picture of the current, emerging and short term trends impacting the Anti-Money Laundering and Counter Financing of Terrorism and Proliferation (AML/CFT) environment.

1.2. FUNCTIONS OF THE FIA

The primary functions of the FIA is to receive, request, analyse and disseminate financial intelligence to an investigatory authority, supervisory authority or other financial intelligence units spontaneously or upon request. In addition, the FIA is responsible for overseeing supervision and compliance with the Financial Intelligence Act of specified parties without a designated supervisor for AML/CFT.



2.0 SUSPICIOUS TRANSACTION REPORTING

2.1 For the period January to December 2021, the FIA received a total of 167 Suspicious Transaction Reports (STRs) with a combined value of P394, 812, 895 as compared to 102 STRs valued at P76, 531,019 for the same period in the year 2020. The number of STRs increased significantly between the two years, at 63.72%. There is also a corresponding increase of over 400% in the value of reported STRs. Following submission, the STRs are put through a risk matrix to assign risk scores and prioritise those of higher impact, using a number of risk variables identified for the period. Of the 167 STRs filed in the period, 140 were prioritized for analysis whilst 35 were kept for intelligence purposes only.

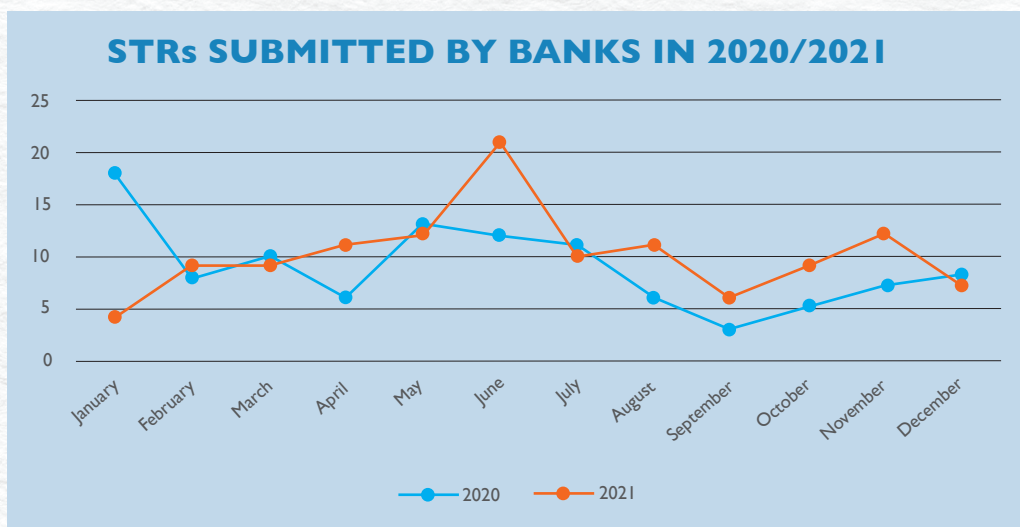
2.2 In both years a significant portion of the STRs were filed by the banking sector as was the case in previous years. However, a substantial increase in the number of STRs reported by the bureau de change sector was observed in 2021. The increase was attributed to a spike in reporting by one (1) entity.

2.3 There is no set international standard or threshold to determine the volume of STRs that entities should be filing, however entities are required to implement robust detection and monitoring systems to enable identification of suspicious transactions and activities as and when they occur.

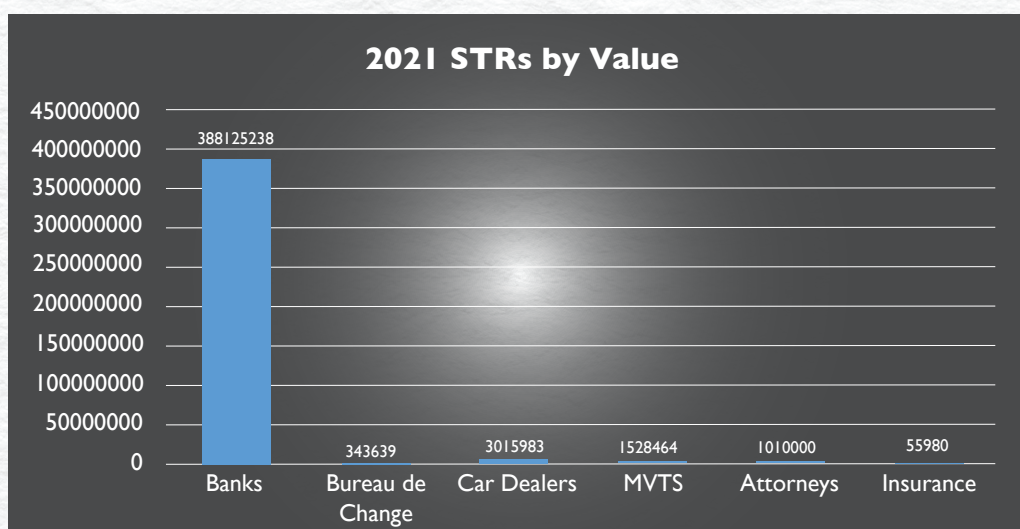
2.4 The table below provides STR statistics reported in the two (2) years:

	2020	2021
Banks	99	94
Bureau de Change	0	57
Car dealer	2	9
Micro Lender	0	4
Attorneys	0	2
Insurance	1	1
TOTAL	102	167

2.5 The following graph shows STRs submitted by banks for the period 2020 and 2021.



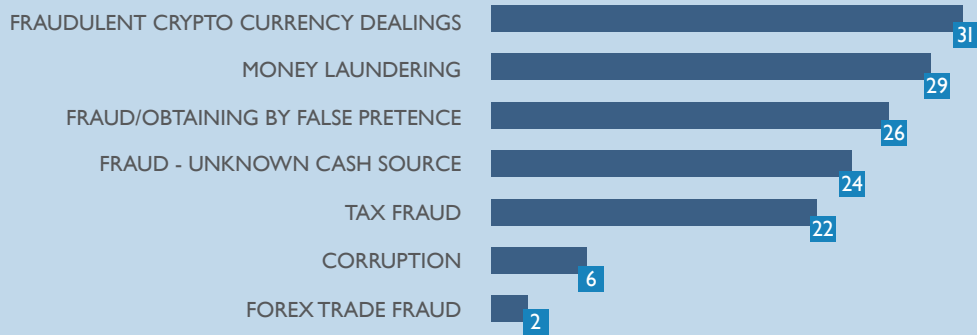
2.6 Suspicious Transaction Reports by Value (Pula) – 2021



3.0 OBSERVED FINANCIAL TRANSACTION TRENDS

3.1 The FIA assesses filed reports to determine current trends in financial crimes and the methods/modus used to carry out the crimes. The following statistics is observed in relation to predicate offences observed in the STRs filed for the period January to December 2021.

UNDERLYING PREDICATE OFFENCES IN STRs



3.2 During the period under review, the most reported underlying predicate offence was fraud, in particular, obtaining by false pretences from the public under the pretext of investing in virtual assets. According to the Financial Action Task Force (FATF), the term virtual asset refers to any digital representation of value that can be digitally traded, transferred or used for payment and investment purposes. However, virtual assets do not include digital representation of fiat currencies, securities and other financial assets.

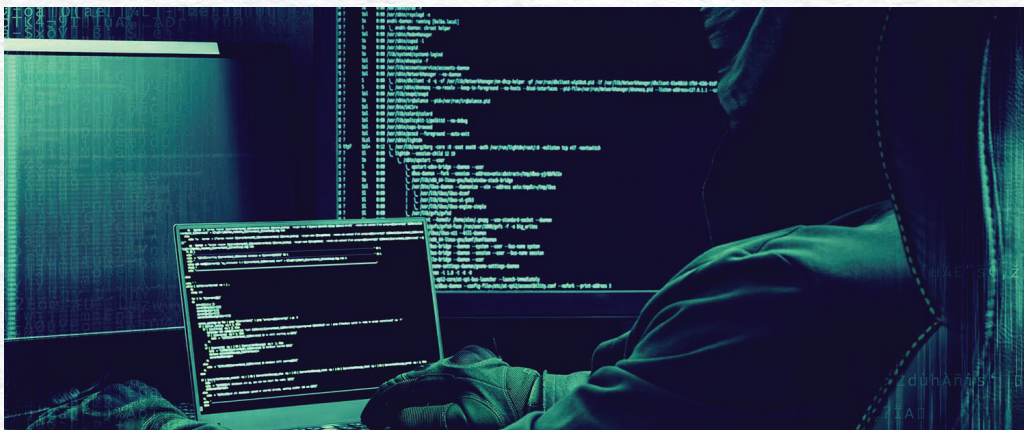
3.3 The section below outlines money laundering trends observed in the course of analysis of suspicious transaction reports.

4.0 FRAUD – OBTAINING BY FALSE PRETENCES

4.1 DEALINGS IN CRYPTO CURRENCIES



4.1.1 Cybercrime continues to escalate in scale and complexity with the increase in online usage. During the period January to December 2021 a total of 31 reports were received involving the defrauding of the public in the pretext of investing in cryptocurrencies.



4.1.2 This is a continuing trend from previous years, however, we have observed an escalation in the number of incidents and amounts involved. Syndicates and individual fraudsters using business and personal bank accounts funnel funds from the public under the pretext of investing in virtual currency more specifically bitcoins.

4.1.3 The public is coerced using mostly social circles and media to avoid face-to-face contact. New payment methods such as electronic wallets and mobile money transfer service are the preferred avenues to solicit funds from victims. Typically, the first few ‘investors’ earn their funds back with interest whilst the rest loose out as their funds are used to settle earlier ‘investors’ and the rest is used to finance luxurious goods and lifestyle of the fraudsters. The luxury lifestyle and goods for some of the syndicate members include luxury hotel stays, purchasing of vehicles and financial gifts to loved ones and associates.

Case Study

4.1.4 In one case, a syndicate of seven (7) individuals with four (4) business entities defrauded the public money in millions. Using a total of 16 bank accounts to funnel the funds, the syndicate received funds in the five (5) months period of February to June 2021 as follows:

Transaction Mode	Amount Involved (Pula)
Cash deposits through Automated Teller Machines	11 203 800
Electronic wallet	2 930 496
TOTAL	14 134 296

4.1.5 Financial intelligence relating to the case was disseminated to the relevant competent authorities for appropriate action.

4.2. FAKE TENDERS



4.2.1 Fraudsters target individuals and established companies into believing they are engaged in business deals when in fact the tenders are fake.

Case study

4.2.2 The fraudsters impersonate senior officials in businesses or government agencies to establish contact with unsuspecting businesspersons/agents. The businessperson were then offered a tender worth millions to supply specialized equipment.

4.2.3 The fraudsters operated by emailing Invitation to Tender (ITT) document which resembled and in the format of the impersonated entity’s ITT thereby extremely convincing to the businessperson. The scammer then directed the businessperson to a fictitious website domain where the products to be procured were to be sourced. In all the cases reported, the products were to be sourced outside the country.

4.2.4 Fake foreign cellphone and landline numbers appearing as local phone numbers were provided to discuss the supply. Once invoices were produced and paid, the website and phone numbers were then discontinued. The cases are currently under investigation.

5.0 USE OF PERSONAL ACCOUNTS FOR BUSINESS TRANSACTIONS

5.1 This is a continuing trend from previous years where individuals use personal accounts for business purposes. In some cases there will be a business account, declared to Botswana Revenue Service (BURS) but hardly used for the business. The FIA profiles and disseminates such cases to the BURS for appropriate action. In addition, there is a standing arrangement between FIA and BURS to avoid dissipation of funds destined to other countries.

6.0 CHURCH AND ROMANCE SCAMS

6.1 The target group for online romance scammers are individuals who turn to online dating applications of social networking sites to find partners. Romance scammers create fake profiles on dating site, applications or popular social media sites like Facebook and Instagram. The scammers strike up a relationship with the victim to build trust by giving them love and attention.

6.2 Individuals are overtime made to believe there is a romantic relationship after which they ask for financial assistance or send pictures of expensive gifts that are purported to have been acquired for the victim. The trick is to make the victims believe such gifts exist and then coerce them to send funds to pay for transportation costs and tax clearance.

6.3 On the other hand worshippers are fooled into parting with their money by being made to contribute to some online church or a worthy cause. The church minister imposters have turned out to be fraudsters raising funds to support their personal lifestyle.

6.4 The FIA has observed that such transactions are mostly facilitated through money or value transfer service providers. In December 2021 alone, a total of 19 STRs were filed by one (1) money or value service provider regarding this type of scam.

****END****

GENERAL INFORMATION - FINANCIAL INTELLIGENCE AGENCY

Name	:	Financial Intelligence Agency
Postal Address	:	Private Bag 0190, Gaborone, Botswana
Telephone number	:	+267 3998400
Fax Number	:	+267 3931754
Website	:	https://www.finance.gov.bw