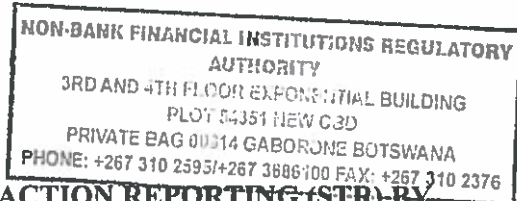


April 09, 2018

**NBFIRA 3/3/4-II (09)**

To: All Non-Bank Financial Institutions ("NBFIs")



**RE: GUIDANCE NOTES ON SUSPICIOUS TRANSACTION REPORTING (STR) BY NBFIs TO THE FINANCIAL INTELLIGENCE AGENCY (FIA)**

1. We refer to the above captioned subject matter.
2. Botswana has an obligation to support international efforts to combat money laundering, prevent, suppress and disrupt proliferation of weapons of mass destruction and the financing of terrorism.
3. The purpose of this communique is to disseminate and submit guidance notes to NBFIs to serve as guidance to comply with their STR obligations.
4. The guidance notes are issued by NBFIRA as a supervisory authority, in line with the Financial Intelligence Act, section 27 (1) (b) to issue instructions, guidelines or recommendations to help specified parties to comply with their obligations under the Act.
5. The guidance notes contain NBFIs STR obligation, what constitutes an STR, examples of sector specific suspicious transaction indicators, procedure for reporting with the FIA, as well as consequences of non-compliance.
9. For any further clarity on the above, kindly contact respective departments at NBFIRA (310 2595 or 368 6100.)

Yours faithfully

**Sriram Gade (Mr)**  
**ACTING CHIEF EXECUTIVE OFFICER**

**NBFIRA**

Non-Bank Financial  
Institutions Regulatory  
Authority



# RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

---

Guidance Note 01 of 2018 for Non-Bank  
Financial Institutions

**NON-BANK FINANCIAL INSTITUTIONS REGULATORY  
AUTHORITY**  
3RD AND 4TH FLOOR EXPONENTIAL BUILDING  
PLOT 54351 NEW CBD  
PRIVATE BAG 00214 GABORONE BOTSWANA  
PHONE: +267 310 2595/+267 3686100 FAX: +267 310 2376

GN 01  
00.00.18

A handwritten signature in black ink, appearing to be 'S. K.', is located in the bottom right corner of the page.

**Contents**

1. Interpretation.....3

2. Overview.....5

3. Purpose of the Guidance Note.....5

4. Responsibilities of an AML/CFT Compliance Officer.....5

5. Purpose of Filing STRs.....7

6. How to complete the STR form.....8

7. Indemnity and Protection of Identity of Persons and Information Relation to STRs.....9

8. Application.....10

PART ONE .....10

1.What is a Suspicious Transaction?.....10

2. Prohibition against Tipping Off .....11

PART TWO.....11

1. How To Identify A Suspicious Transaction .....11

General Indicators of ML/TF.....12

General Indicators of Suspicious Transactions.....13

a. Suspicious Transactions in Reporting or Record Keeping requirements.....15

b. Suspicious Transactions in Identity requirements.....15

c. Suspicious Transactions in Cash Transactions.....15

d. Suspicious Transactions involving accounts.....17

e. Suspicious Transactions involving Offshore Business Activity.....18

ii Industry Specific Indicators.....19

a. Suspicious Transactions in the Insurance sector.....19

b. Suspicious Transactions in the Retirement Funds sector.....20

c. Suspicious Transactions in the Capital Market and Investment Institutions sector.....21

d. Suspicious Transactions in the Lending and Pawn shop sector.....23

e. Suspicious Transactions in the Finance and Leasing sector.....24

**PART THREE.....24**

1 Reporting of a Suspicious Transaction the the Financial Intelligence Agency ..... 24

2 Financial Intelligence Agency contact details.....25

4 Failure to report a suspicious transaction.....25

5 Register or reported transactions.....25



## **Interpretation**

In this document, unless the context otherwise requires ;

“**CDD**” means Customer Due Diligence.

“**FIA**” means Financial Intelligence Agency.

“**FI Act**” means the Financial Intelligence Act.

“**FI Regulations**” means Financial Intelligence Regulations

“**Money Laundering**” is broadly referred to as the process of creating the appearance that large amounts of money obtained from serious crimes, such as drug trafficking or terrorist activity, originated from a legitimate source

“**Property**” means money or any other movable, immovable, corporeal, or incorporeal thing whether located in Botswana or elsewhere and includes any rights securities and any interest in privileges and claims over that thing as well as;

- (a) any currency, whether or not the currency is legal tender in Botswana, and any bill, security, bond, negotiable instrument or any instrument capable of being negotiated which is payable to bearer or endorsed payable to bearer, whether expressed in Botswana currency or otherwise;
- (b) any balance held in Botswana currency or in any other currency in accounts with any bank which carries on business in Botswana or elsewhere;
- (c) any balance held in Botswana currency or in any other currency in accounts with a bank which carries on business in Botswana;
- (d) any balance held in any currency with a bank outside Botswana;
- (e) motor vehicles, ships, aircraft, boats, works of art, jewellery, precious metals or any other item of value;
- (f) any right or interest in property; and
- (g) funds or other assets including all property and any interest, dividends or income on or value accruing or generated by such funds or assets.

“**Suspicious transaction**” means a transaction which –

- (a) Gives rise to a reasonable suspicion that it may involve financial offence;

- (b) Gives rise to a reasonable suspicion that it may involve property connected to, or to be used to finance terrorism, whether or not the property represent the proceeds of an offence;
- (c) Is made in circumstances of unusual or unjustified complexity;
- (d) Appears to have no economic justification or lawful objective;
- (e) Is made by or on behalf of a person whose identity has not been established to the satisfaction of the person with whom the transaction is made; or
- (f) Gives rise to suspicion for any other reason;
- (g) Causes a feeling of apprehension or mistrust about its legality;
- (h) Is unusual activity in terms of customer profile with no reasonable explanation; and
- (i) Arouses suspicion that a transaction may be connected with activities prohibited by the law.

**“STR”** means Suspicious Transaction Report

**“Transaction”** includes —opening an account, renting a safe deposit box, entering into a fiduciary relationship or establishing any other business relationship, as well as a proposed transaction.

A handwritten signature or mark consisting of a large, stylized loop with several vertical lines extending upwards from the top of the loop.

## 1. OVERVIEW

- 1.1 Botswana has an obligation as a member of Eastern and Southern Africa Anti-Money Laundering Group (“ESAAMLG”) to put in measures to combat ML/TF. ESAAMLG is an associate member of the Financial Action Task Force (“FATF”) which is an inter-governmental body whose objectives are to set international standards for adoption and effective implementation of the standards by countries. In turn, Botswana is required to put in place legal, regulatory and operational measures for combating ML/ TF and other related threats to the integrity of the financial system of Botswana and the world-over, consistent with the set international standards. It is therefore vital that all financial institutions in Botswana exercise appropriate care and diligence to ensure that neither they nor any services offered by them are used by criminals or whose intentions are to launder the proceeds of crime or to engage in TF.
- 1.2 As part of the integrated global financial system Botswana’s ability to engage in cross-border trade and financial flows is heavily dependent on promoting and maintaining the integrity of its financial system and this requires the financial institutions to put in place adequate mitigating controls to detect and prevent occurrences of ML /TF.
- 1.3 The Financial Intelligence Act is the primary legal framework for combating ML/TF in Botswana. The Financial Intelligence Agency’s main focus is to provide for the reporting of suspicious transaction and other cash transactions and to facilitate mutual assistance with comparable bodies outside Botswana in relation to financial information and for matters connected therewith and incidental thereto. The Agency is the central unit responsible for requesting, receiving and analysing and disseminating to an investigatory authority, supervisory authority or comparable body, disclosures of financial information.

## 2. Purpose of the Recognition and Reporting of Suspicious Transactions Guidance Note

- 2.1 The purpose of the Guide notes is to give guidance to NBFIs to properly discharge the mandatory reporting obligations in relation to suspicious transactions involving ML/ TF and associated crimes. Therefore the purpose of the Guide notes is to assist specified parties/regulated NBFIs to comply with their AML/CFT obligations under the FI Act in the following manner;



- i. By providing NBFIs with comprehensive guidance on implementing internal policies and procedures to detect and report high quality suspicious transactions without tipping the customer off; and
- ii. By providing indications that may be taken into consideration when determining whether a transaction should give rise to a suspicion..

### **3. Responsibilities of the AML/CFT Compliance Officer**

- 3.1 Section 9 (1) of the FI Act provides that a specified party shall designate a compliance officer at management level who will be in charge of implementation of internal programs and procedures.
- 3.2 There is an obligation on all employees to report in writing to the AML/CFT Compliance Officer suspicions of money laundering and terrorist financing. All NBFIs have a clear obligation to ensure that each relevant employee knows to which person s/he should report suspicions and that there is a clear reporting chain under which those suspicions will be passed directly and without delay to the AML/CFT Compliance Officer. Sufficient guidance should therefore be given to employees to enable them to recognize suspicious transactions. Once the employee has reported their suspicions to the AML/CFT Compliance Officer, they will have fully satisfied and discharged their statutory obligation.
- 3.3 The AML/CFT Compliance Officer must be endowed with a significant degree of responsibility and independence. S/he is required to determine whether the information or other matters contained in the transaction report they have received give rise to knowledge or reasonable suspicion that a customer is engaged in money laundering or the financing of terrorism.
- 3.4 In making this judgment, they should consider all other relevant information available within the financial institution concerning the person or business to whom the initial report relates. This may include making a review of other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship and referral to identification records held. If, after completing this review, it is decided that there are no facts that would negate the suspicion, then they must report the suspicious transaction to the FIA. Nevertheless, care should be taken to guard against a report being submitted as a matter of routine without undertaking reasonable internal enquiries to determine that all available information has been taken into account. In addition, the AML/CFT officer should distinguish between the making of Suspicious Transaction Reports in respect of money laundering or the financing of terrorism and the lodging of a complaint or allegation of crime with the police for investigation.





- 3.5 In the event that the AML/CFT Compliance Officer makes a decision not to make a report to the FIA, the reasons for such a decision must be documented and retained with the NBFIs.

#### 4. Purpose of Filing STRs

- 4.1 The FI Act requires that International Finance Services Centre accredited entities, Insurance entities, Investment Institutions, Micro Lending entities and Retirement Funds detect and report transactions that are suspected of involving or relating to funds generated through unlawful means as they could be used by criminals for laundering or financing of terrorism purposes. Upon receipt of the STR, the FIA conducts an analysis of all information submitted to it by the regulated entity and where there is indication of a financial offence, disseminates the results of the analysis in the form of a financial intelligence report to law enforcement agencies. The FIA also disseminates intelligence products Botswana Revenue Services and to the Directorate of Intelligence and Security Services where it has reasonable grounds suspect that the information would be relevant to the national security. NBFIs therefore play an integral role in ensuring that the financial integrity of Botswana is safeguarded against criminality and as a result, gains global recognition for conducting a safe and sound financial sector in compliance with international best practice.

The failure to detect and report STRs severely damages the viability of an NBFIs (specifically) and the integrity of Botswana's financial system (in general) as it becomes associated with money laundering and the financing of terrorism.

- 4.2 It is a criminal offence for an NBFIs to fail to take measures as reasonably necessary to prevent its institution or the services its institution offers from being used to commit or to facilitate the commission of ML/TF as provided for in section 9 (3) of the FI Act. Section 25 of the FI Act prescribes penalties for failure to comply with the obligation to make STRs and other reports such as cash and electronic transfer threshold reports. The penalties are a fine, suspension or revocation of the NBFIs operating license or both. There is also provision of personal liability for the person in the NBFIs charged with making STRs and has failed to do so, the penalty is a fine and or imprisonment.
- 4.3 This guidance note is therefore a statement of the minimum standard expected of all NBFIs. Failure for NBFIs to comply and therefore allow themselves to become loop holes for ML/TF will greatly affect Botswana's reputation and lead to international blacklisting which will cut off Botswana from the global financial market due to it



being regarded as a ML/TF high risk area. This will limit NBFIs' ability to timeously carry out transaction and in some cases be unable to transact at all. In summary, failure to report a suspicious transaction can therefore lead to the following consequences;

- *Criminal Prosecution*

There are penalties, as stated above for breaches of the provisions of the money laundering and the terrorism prevention legislation, whether by firms, individuals or employees.

- *Commercial Loss*

The institution may incur non-productive costs to address issues arising out of investigations into alleged money laundering and/or terrorist financing, costs to defend prosecutions, and costs to repair the institution's public image.

- *Negative Publicity*

Institutions which, even inadvertently, become involved in money laundering and/or terrorist financing, risk loss of their good reputation in the market. This may occur as a result of media coverage of the circumstances.

**5. How to complete the Suspicious Transaction Report Form**

- 5.1 The report is to be made in the form set out in the Schedule to the FI Regulations (and attached hereto) and be sent to the FIA through the electronic portal provided by the FIA. For NBFIs that have no access to this portal, the report can be sent by facsimile, hand delivery or any other method determined by the FIA – maybe it should be moved to the next section.
- 5.2 The STR form should be fully completed in order to aid the FIA to investigate any suspicious activity. The FI Act also makes provision for the content of the STR report, which is embedded in the STR form fields that NBFIs will be completing when making an STR as provided for in section 22 of the Financial Intelligence Act;
- (a) the identification of the customer and other party to the transaction;
  - (b) the description of the nature of the transaction;
  - (c) the amount of the transaction;
  - (d) circumstances giving rise to the suspicion;



- (e) the business relationship of the customer to the person making the report;
- (f) where the customer is an insider, whether such customer is still affiliated with the NBFi;
- (g) any voluntary statement as to the origin, source or destination of the proceeds;
- (h) the impact of the suspicious transaction on the financial soundness of the NBFi; and
- (i) the names of all the officers, employees or agents dealing with the transaction.

NBFIs are strongly advised to contact the FIA should they have any problems completing the form or if they do not understand certain fields.

## **6. Indemnity and Protection of Identity of Persons and Information Relating to STRs**

- 6.1 The FI Act protects those reporting or receiving reports of suspicious transactions of ML/TF or additional information thereon from claims in respect of any alleged breach of client confidentiality or for disclosure of confidential information.
- 6.2 The FI Act also provides immunity from civil or criminal proceedings against any person who has, in good faith reported any suspicions they may have had whether or not the suspicion proves to be well founded upon investigation. Any person who has supplied the FIA with any information pursuant to a request made by FIA is also indemnified.
- 6.3 In addition to the above, no administrative or disciplinary proceedings for breach of professional secrecy or contract shall be taken against any person for submitting a completed STR form in good faith or in compliance with directions given by the legislation.
- 6.4 The identity of the person who files an STR with the FIA shall not be disclosed to any person. The FI Act prohibits the staff of the FIA or of the NBFi from doing so or providing any evidence concerning the identity of a person who has made, initiated or contributed to a report under the FI Act or who has furnished additional information concerning the report. The FI Act goes on to prohibit the identity of the person making the report or providing information to the FIA from being admissible as evidence in proceedings before a court unless the person testifies at the proceedings.



**7. Application**

- 7.1 The Guide notes apply to all NBFIs licensed, registered/exempted or intending to apply for recognition under the provisions of the licensing regulations of the respective NBFIRA departments. These NBFIs have been designated as Specified Parties in accordance with the First Schedule to the FI Act.
- 7.2 The relevance and usefulness of the Guide notes will be kept under review and it may be necessary to issue amendments from time to time.

**PART ONE**

**1. What is a Suspicious Transaction?**

Whenever a NBFi processes a transaction to which there is reasonable grounds to suspect that it may fit the definition of a suspicious transaction, it should take reasonable measures to ascertain the purpose of that transaction and submit a suspicious transaction report to the FIA without tipping the customer off.

“Reasonable grounds to suspect” is determined by what is reasonable in a NBFi’s circumstances, including normal business practices and systems within your industry. The context in which the transaction occurs or is attempted, is a significant factor in assessing suspicion. This will vary from business to business and from one customer to another. You should evaluate transactions in terms of what seems appropriate and is within normal practice in your particular line of business and based on your knowledge of your customers business, financial history, background and behavior.

Evidence of potential money laundering activity often occurs in the form of unusual or unexpected patterns of transactional activity. Adherence to satisfactory CDD measures provides the foundation for the recognition of such activity. In addition to helping Licensees to identify and manage the risks inherent in certain customer relationships, adequate CDD measures enable Licensees to know enough about customers, to be able to recognise unusual or unexpected activity, as or before it occurs.



## **2. Prohibition against Tipping Off**

The FI Act prohibits any person who is directly or indirectly involved in the reporting of a suspicious transaction from divulging to any person involved in the transaction or to any unauthorised third party, that the transaction has been reported.

Unauthorised disclosure in this case may comprise of;

- Where a person knows or suspects that a report has been made to the FIA and discloses this information to an unauthorized person
- Disclosure to an unauthorised person of an investigation which one knows or suspects that the the FIA is acting or proposing to act and is being conducted or about to be conducted in relation to the financing of terrorism
- Where one discloses information to an officer of the NBFIs other than the AML/CFT Compliance Officer even if in accordance with the policies and procedures of the institution, t that person is guilty of an offence if he/she discloses information or other matter relating to such a disclosure.

It is however not deemed an unauthorized disclosure if one discloses information or any other matter relating to a report, investigation or disclosure, for the purpose of facilitating the investigation or any proceedings which might be conducted following the report.

## **PART TWO**

### **1. How To Identify A Suspicious Transaction**

When conducting a business relationship or engaging in a once-off transaction a suspicious transaction will often be one which is inconsistent with the customer's known, legitimate or personal activities or with their normal business. Therefore, the first key to recognition is knowing enough about your customer and their business to recognize that a transaction or series of transactions are unusual.

Satisfactory CDD will enable the NBFIs to gain knowledge about the risk profile of its customers for ML/TF risks. It also assists NBFIs to know if their customers are conducting transactions that are inconsistent with the knowledge already formed of them by the NBFIs. This inconsistency may give rise to the filing of an STR with the FIA.



Reliance on what should be reported is largely on one's assessment, based on knowledge and experience, as well as the specific circumstances of the transaction. The assessment should therefore be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, their financial history, background and behavior. The person reporting does not need to know the activity underlying the money laundering and/or terrorist financing or that the funds themselves definitely arose from a criminal offence.

The paragraphs below provide a non-exhaustive list of general indicators of suspicious transactions which apply to all sectors. There is also a list of sector specific suspicious transaction indicators in the Capital Markets, Investment Institutions, Lending, Retirement Funds and the Insurance sectors.

These indicators are not intended to cover every possible scenario and are not to be viewed in isolation. As such, a single indicator is not necessarily indicative of reasonable grounds to suspect ML/TF. Taken together, the presence of one or more indicators as well as knowledge of your customer's business or financial affairs may help you to identify suspicious transactions.

**i. General Indicators on ML/TF**

In addition to the indicators, below are some questions that an NBFIs and/or its employees can consider when determining whether an established customers transactions might be suspicious;

1. Is the volume and /or size of the transactions and/or value of the property consistent with the normal pattern of activity for the customer?
2. Is the receipt of the property or transaction in the context of the customer's business or personal activities and their stated commercial objectives;
3. Has the pattern of transactions conducted by the customer changed?; and
4. Where the transaction is international by nature, does the customer have any obvious reason for conducting business with the other country involved

NBFIs are reminded that although not all unusual or unexpected activity is necessarily suspicious, employees are expected to be able to recognise unusual activity as a result of effective CDD checks conducted on an on-going basis. Suspicion need not only be based on transactions or activities within the business relationship, but also on information from other sources, including the media, intermediaries, or the customer him/herself. Employees must analyse the transaction/activity in more detail to ascertain whether it is suspicious.



**ii. General Indicators of Suspicious Transactions**

The FI Act defines a suspicious transaction in its interpretation section as a transaction. In addition to the above definition, other general indicators are;

1. You are aware that the customer is the subject of a money laundering or terrorist financing investigation;
2. You are aware or you become aware, from a reliable source (that can include media or other open sources), that a customer is suspected of being involved in illegal activity;
3. A new or prospective customer is known to you as having a questionable legal reputation or criminal background;
4. Customer admits to or makes statements about involvement in criminal activities;
5. A customer who is reluctant to provide identifying information when purchasing a product or who provides minimal or seemingly fictitious information;
6. Customer provides false information or information that you believe is unreliable;
7. Any apparent unnecessary use of an intermediary in the transaction;
8. Customer is quick to volunteer that funds are “clean” or “not being laundered”;
9. Customer shows uncommon curiosity and/or knowledge about internal systems, controls and policies;
10. Large sums being transferred from overseas for making payments;
11. Customer insists that a transaction be done quickly;
12. Stated occupation of the customer is not in keeping with the level or type of activity;
13. Unusual activity in accounts compared to past transactions;
14. Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers;
15. The transaction does not appear to make sense or is out of keeping with usual or expected activity for the customer;
16. Where the transaction being requested by the customer, without reasonable explanation is out of the ordinary range of services normally requested or is outside the experience of the financial services business in relation to the particular customer;
17. Where without justifiable explanation, the size of the pattern of transactions is out of line with any pattern that has previously emerged;

18. Where a customer who has entered a business relationship uses the relationship for a single transaction or for only a short period of time without a reasonable explanation;
19. The extensive use of trusts or offshore structures in circumstances where the customers needs are inconsistent with the use of such services;
20. Transfers to and from high risk jurisdictions without reasonable explanation which are inconsistent with the customers declared business dealings or interests;
21. Unnecessary routing of funds or other property from/to third parties or through third party accounts;
22. The customer does not want correspondence sent to their home address;
23. The customer conducts transactions at different physical locations in an apparent attempt to avoid detection;
24. The customer repeatedly uses an address but frequently changes the names involved;
25. The customer is accompanied and watched at all relevant times;
26. The customer presents confusing details about the transaction or knows few details about its purpose;
27. The customer over justifies or explains the transaction;
28. The customer is secretive and reluctant to meet in person;
29. The customer is nervous, not in touch with the transaction and/or has only vague knowledge of the amount of a transaction;
30. The customer's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact customer shortly after opening account;
31. Normal attempts to verify the background of a new or prospective customer are difficult;
32. The customer appears to be acting on behalf of a third party, but does not tell you;
33. Inconsistencies appear in the customer's presentation of the transaction;
34. The customer attempts to develop close rapport with staff;
35. The customer uses aliases and a variety of similar but different addresses;
36. The customer presents different identification documents each time a transaction is conducted;
37. The customer offers you money, gratuities or unusual favours for the provision of services that may appear unusual or suspicious;
38. The transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist).





**a. General Indicators of Suspicious Transactions in Reporting or Record Keeping requirements**

1. Customer makes inquiries that would indicate a desire to avoid reporting;
2. Customer attempts to convince an employee not to complete any documentation required for the transaction;
3. Customer has unusual knowledge of the law in relation to suspicious transaction reporting;
4. Customer appears to be structuring amounts to avoid record keeping, customer identification or reporting thresholds; and
5. Customer appears to be collaborating with others to avoid record keeping, customer identification or reporting thresholds.

**b. General Indicators of Suspicious Transactions in Identity requirements**

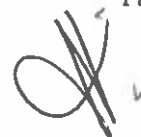
1. Customer provides doubtful or vague information;
2. Customer produces seemingly false identification or identification that appears to
3. be counterfeited, altered or inaccurate;
4. Customer refuses to produce personal or corporate identification documents or
5. refuses to cooperate with the CDD and/or ongoing monitoring process;
6. Customer presents different identification document each time a transaction is
7. conducted;
8. Customer only submits copies of personal identification documents;
9. Customer wants to establish identity using something other than his or her personal
10. identification documents;
11. Customer's supporting documentation lacks important details such as a phone number;
12. Customer inordinately delays presenting personal or corporate documents;
13. Customer refuses to have foreign documents notarised for purposes of certification; and
14. All identification documents presented appear new or have recent issue dates.

**c. Indicators of Suspicious Transactions in Cash Transactions**

1. Customer starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the customer in the past;
2. Customer frequently exchanges small notes for large ones;



3. Customer uses notes in denominations that are unusual for the customer, when the norm in that business is different;
4. Customer presents notes that are packed or wrapped in a way that is uncommon for the customer;
5. Customer deposits musty or extremely dirty bills;
6. Customer consistently makes cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold;
7. Customer conducts a transaction for an amount that is unusual compared to amounts of past transactions;
8. Customer asks you to hold or transmit large sums of money or other assets when this type of activity is unusual for the customer;
9. Stated occupation of the customer is not in keeping with the level or type of activity (for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area);
10. Cash is transported by a cash courier where this is not in keeping with customers normal transaction habits, stated income or occupation;
11. Customer carries out large transactions using a variety of denominations;
12. Customer insists on using cash for a large transaction;
13. A shared address for individuals involved in cash transactions, particularly when the address is also for a business location or does not seem to correspond to the stated occupation (for example, student, unemployed, self-employed, etc.); and
14. Unusual payment methods such as cash and cash equivalents (when such a usage of cash or cash equivalents is, in fact, unusual).
15. Company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than the forms of debit and credit normally associated with commercial operations (e.g., cheques, Letters of Credit, Bills of Exchange, etc.)
16. Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.
17. Customers who constantly pay in or deposit cash to cover requests for money transfers, bankers' drafts or other negotiable and readily marketable money instruments.
18. Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.
19. Frequent exchange of cash into other currencies
20. Branches that have a great deal more cash transactions than usual
21. Customers whose deposits contain counterfeit notes or forged instruments
22. Customers transferring large sums of money to or from overseas locations with instruments for payment in cash



23. Large cash deposits using night safe facilities, thereby avoiding direct contact with bank staff.

**d. Indicators of Suspicious Transactions involving Accounts**

1. Opening accounts when the customer's address is outside the local service area;
2. Where the customer appears to have accounts with several financial institutions in one area for no apparent reason;
3. Opening accounts in other people's names;
4. Opening accounts with names very close to other established businesses;
5. Attempting to open or operate accounts under a false name;
6. Account with a large number of small cash deposits and a small number of large cash withdrawals;
7. Funds are being deposited into several accounts, consolidated into one and transferred outside the country;
8. Customer frequently uses many deposit locations outside of the home branch location;
9. Multiple transactions are carried out on the same day at the same branch but with apparent attempt to use different tellers;
10. Account activity far exceeds activity projected at the time of opening of the account;
11. Establishment of multiple accounts, some of which appear to remain dormant for extended periods;
12. An account that was reactivated from inactive or dormant status suddenly sees significant activity;
13. Reactivated dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum(s) has been removed;
14. Unexplained transfers between the customer's products and accounts;
15. Large transfers from one account to other accounts that appear to be pooling money from different sources;
16. Multiple deposits are made to a customer's account by third parties;
17. Deposits or withdrawals of multiple monetary instruments, particularly if the instruments are sequentially numbered;
18. Frequent deposits of bearer instruments (for example, cheques, money orders) in amounts just below a determined threshold;
19. Unusually large cash deposits by a customer with personal or business links to high risk areas;



20. Correspondent accounts being used as “pass-through” points from foreign jurisdictions with subsequent outgoing funds to another foreign jurisdiction; and
21. Multiple personal and business accounts are used to collect and then funnel funds to a small number of foreign beneficiaries, particularly when they are in high risk areas.

**e. Indicators of Suspicious Transactions involving Offshore Business Activity**

1. Accumulation of large balances inconsistent with the known turnover of the customer’s business and subsequent transfers to overseas account(s);
2. Loans secured by obligations from offshore banks;
3. Loans to or from offshore companies;
4. Large amounts of deposits from a confidential source being sent from an offshore bank or somehow guaranteed by an offshore bank;
5. Transactions involving a shell bank whose name may be very similar to the name of a major legitimate institution;
6. The transaction crosses many international lines;
7. Transactions involving high-volume international transfers to third party accounts in countries that are not usual remittance corridors;
8. A transaction that involves a country known for highly secretive banking and corporate law;
9. Transactions involving countries deemed by the Financial Action Task Force as requiring enhanced surveillance;
10. A transaction that involves a country where illicit drug production or exporting may be prevalent or where there is no effective anti-money-laundering system;
11. A transaction involving a country known or suspected to facilitate money laundering activities;
12. Deposits are followed within a short time by wire/electronic transfer of funds to or through locations of concern, such as countries known or suspected to facilitate money laundering activities;
13. Unexplained electronic funds transfers by customer on an in and out basis;
  14. Use of letter-of-credit and other methods of trade financing to move money between between countries when such trade is inconsistent with the customer’s business;
  15. Use of a credit card issued by an offshore bank;
  16. Frequent requests for traveller’s cheques or foreign currency drafts or other negotiable instruments to be issued;
  17. Frequent paying in of traveller’s cheques or foreign currency drafts particularly if originating from overseas;



18. Changes in employee or agent performance, (e.g. the salesman selling products for cash has remarkable or unexpected increase in performance);
19. Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

iii. **Industry Specific Indicators**

a. **Indicators of Suspicious Transactions in the Insurance Sector**

The following are examples of common indicators that may point to suspicious or unusual transactions within the Insurance sector. Kindly note that these indicators are not exhaustive and thus should not be viewed in isolation.

1. The purchase of an insurance product inconsistent with the customer's needs;
2. Customer proposes to purchase an insurance product using a cheque drawn on an account other than his or her personal account;
3. Customer requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment;
4. Customer who has other small policies or transactions based on a regular payment structure makes a sudden request to purchase a substantial policy with a lump sum payment;
5. Customer conducts a transaction that results in a conspicuous increase in premium contributions;
6. Customer makes payments with small denomination notes, uncommonly wrapped, with postal money orders or with similar means of payment;
7. Transaction involves use and payment of a performance bond resulting in a cross border payment;
8. Customer who has other small policies or transactions based on a regular payment structure makes a sudden request to purchase a substantial policy with a lump sum payment;
9. Scale of investment in insurance products is inconsistent with the customers economic profile;
10. Unanticipated and inconsistent modification of customers contractual conditions, including significant or regular premium top-ups;
11. Unforeseen deposit of funds or abrupt withdrawal of funds;
12. Involvement of one or more third parties in paying the premiums or in any other matters involving the policy;



13. Overpayment of a policy premium with a subsequent request to refund the surplus to a third party;
14. Funds used to pay policy premiums or deposits originate from different sources;
15. Use of life insurance product in a way that resembles use of a bank account, namely making additional premium payments and frequent partial redemptions;
16. Customer cancels insurance soon after purchase;
17. Early redemption takes place in the absence of a reasonable explanation or in a significantly uneconomic manner;
18. Insistence on depositing securities or other assets in an investment portfolio that would not normally be allowed by the scheme rules;
19. Customer shows more interest in the cancellation or surrender of an insurance contract than in the long-term results of investments or the costs associated with termination of the contract;
20. The first (or single) premium is paid from a bank account outside the country;
21. The transfer of the benefit of a product to an apparently unrelated third party;
22. Customer accepts very unfavourable conditions unrelated to his or her health or age;
23. Repeated and unexplained changes in beneficiary;
24. Relationship between the policy holder and the beneficiary is not clearly established;
25. A customer who shows little concern for the investment performance of a product/service but a great deal of concern about the early termination features of the product; and
26. Customer who borrows the maximum amount available soon after purchasing the product.
27. Introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where organized criminal activities (e.g. drug trafficking or terrorist activity) are prevalent.
28. Requests for a large purchase of a lump sum contract where the policyholder's usually transacts in is small, regular payments;
29. Applicant for insurance business requests to make a lump sum payment by a wire payment/wire transfer or with foreign currency.

**b. Indicators of Suspicious Transactions in the Retirement Funds Sector**

The following are examples of common indicators that may point to suspicious or unusual transactions within the Retirement Fund sector. Kindly note that these indicators are not exhaustive and thus should not be viewed in isolation.

1. Customer conducts a transaction that results in a conspicuous increase in investment contributions;



2. Unforeseen deposit of funds;
3. Involvement of one or more third parties in paying retirement fund contributions or in any other matters involving the policy;
4. Overpayment of a contribution with a subsequent request to refund the surplus to a third party;
5. Funds used to pay contributions or deposits originate from different sources;
6. The first (or single) contribution is paid from a bank account outside the country;
7. The transfer of the benefit of a product to an apparently unrelated third party;
8. Customer accepts very unfavourable conditions unrelated to his or her health or age;
9. Repeated and unexplained changes in beneficiary;
10. Relationship between the policy holder and the beneficiary(s) is not clearly established;
11. Unusual payment methods, such as cash or cash equivalents (when such a usage of cash or cash equivalents is, in fact, unusual);
12. A customer who shows little concern for the investment performance of a product/service but a great deal of concern about the early termination features of the product;
13. Large cash sums deposited in pension schemes by members of the scheme;
14. Unrelated third party paying contributions cash on behalf of a member of a pension scheme; and
15. Unemployed persons paying contributions into an employee pension scheme.

**c. Indicators of Suspicious Transactions in the Capital Markets and Investment Institutions Sectors**

The following are examples of common indicators that may point to suspicious or unusual transactions within the Capital Markets and Investment Institutions sectors. Kindly note that these indicators are not exhaustive and thus should not be viewed in isolation.

1. Customer conducts a transaction that results in a conspicuous increase in investment contributions;
2. Acquiring of bonds and settlement of the bonds using large cash amounts;
3. Foreign and national PEPs investing in securities;
4. Foreign nationals using locals to acquire securities;
5. The use of unregistered or unlicensed securities businesses;
6. The transaction involves use and payment of a performance bond resulting in a cross-border payment;
7. Changing share ownership in order to transfer wealth across borders;
8. Redeeming a long-term investment within a short period;
9. Opening multiple accounts or nominee accounts;
10. Using brokerage accounts as long term depository accounts for funds;



11. Effecting transactions involving nominees or third parties;
12. Engaging in market manipulation, e.g. "pump & dump"<sup>1</sup> schemes;
13. Engaging in 'boiler room'<sup>2</sup> operations;
14. Transfer of assets from unrelated third party into an investment portfolio;
15. Customer attempts to purchase investments with cash;
16. Customer uses securities or futures brokerage firm as a place to hold funds that are not being used in trading of securities or futures for an extended period of time and such activity is inconsistent with the normal investment practice of the customer or their financial ability;
17. Customer frequently makes large investments in stocks, bonds, investment trusts or other securities in cash or by cheque within a short time period;
18. Transfers of funds or securities between accounts not known to be related to the customer;
19. Several customers open accounts within a short period of time to trade the same stock;
20. Customer is an institutional trader that trades large blocks of junior or penny stock on behalf of an unidentified party;
21. Customer attempts to purchase investments with instruments in the name of a third party;
22. Customer maintains bank accounts and custodian or brokerage accounts at high risk jurisdictions with no explanation by customer as to the purpose for such relationships;
23. Proposed transactions are to be funded by international wire/electronic payments, particularly if from countries where there is no effective anti-money-laundering system.;
24. Accounts that have been inactive suddenly experience large investments that are inconsistent with the normal investment practice of the customer or their financial ability;
25. Any dealing with a third party when the identity of the beneficiary or counter-party is undisclosed;
26. Customer wishes monies received through the sale of shares to be deposited into a bank account rather than a trading or brokerage account which is inconsistent with the normal practice of the customer;
27. Customer makes large or unusual settlements of securities in cash;
28. The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading;
29. Unrelated customers redirect funds toward the same account;

---

<sup>1</sup> a scheme that attempts to boost the price of a stock through recommendations based on false, misleading or greatly exaggerated statements

<sup>2</sup> Refers to the use of high pressure sales tactics to sell stocks to customers who are "cold called", or called randomly





30. Trades conducted by NBFIs that you know have been named or sanctioned by regulators in the past for irregular or inappropriate trading activity;
31. Customer is willing to deposit or invest at rates that are not advantageous or competitive;
32. All principals of customer are located outside of the country;
33. Payments made by way of third party cheques are payable to or endorsed over to the customer;
34. Transactions are carried out made by the NBFIs employees or that are made by a relative of an employee to benefit unknown parties;
35. Third-party purchases of shares in other names (i.e., nominee accounts);
36. Transactions in which customers make settlements with cheques drawn by, or remittances; and
37. Unusually large amounts of securities or stock certificates in the names of individuals other than the customer.
38. Purchasing of securities to be held by the institution in safe custody, where this does not appear appropriate given the customer's apparent standing.
39. Request by customers for investment management or administration services (either foreign currency securities) where the source of the funds is unclear or not consistent with the customer's apparent standing.

**d. Indicators of Suspicious Transactions in the Lending and Pawn shop Sector**

The following are examples of common indicators that may point to suspicious or unusual transactions within the Lending sector Kindly note that these indicators are not exhaustive and thus should not be viewed in isolation.

1. Customer repays problem loans unexpectedly;
2. Customer makes a large, unexpected loan payment with unknown source of funds or a source of funds that does not match what you know about the customer;
3. Customer repays a long term loan within a relatively short time period;
4. Source of down payment is inconsistent with borrower's background and income;
5. Down payment appears to be from an unrelated third party;
6. Down payment uses a series of money orders or bank drafts from different financial institutions;
7. Customer shows income from "foreign sources" on loan application without providing further details;
8. Customer's employment documentation lacks important details that would make it difficult for you to contact or locate the employer;
9. Customer offers you large deposits or some other form of incentive in return for favourable treatment of loan request;



10. Customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction; and
11. Down payment or other loan payments are made by a party who is not a relative of the customer.

**e. Indicators of Suspicious Transactions in the Finance and Leasing Sector**

1. Customer asks to borrow against assets held by another financial institution or a third party when the origin of the assets are not known;
2. The loan transaction does not make economic sense( i.e where the customer has significant assets and there does not appear to be a sound business reason for the transaction); and
3. Customer applies for loans on the strength of a financial statement reflecting major investments in or income from businesses incorporated in countries known for highly secretive banking and corporate law and the application is outside the ordinary course of business for the customer.

**PART THREE**

**1. Reporting of a Suspicious Transaction to the FIA**

Suspicious transactions are to be IMMEDIATELY reported to the FIA as soon as possible but no later than 15 working days after the suspicion arose concerning the transaction that gave rise to the need to report. Reports can either be sent to the FIA electronically or physically (facsimile, physical delivery or any another method determined by the Agency) using the form set out in the schedule to the FI Regulations. The said form has been attached to these guide notes for your convenience. NBFIs that have difficulty accessing the form from this document are required to contact the FIA using the contact details below to have a copy sent to them.

Once a transaction has been reported as suspicious, the NBFi should continue with or carry out the transaction unless the FIA directs otherwise. In so doing, there will be less of a chance of indirectly tipping off the customer or the customer suspecting that they may have been reported. The FIA is required to ensure that feedback has been given to the person making the report within 14 working days from the date of receipt of the report.

It is important to note that after a reporting institution makes an initial report in respect of a specific suspicious transaction, that initial report does not relieve the institution of the need to report further



suspicious in respect of the same customer or account and the institution should report any further suspicious transactions involving the customer.

## **2. Financial Intelligence Agency Contact Details**

Below are the contact details of the Financial Intelligence Agency. All completed forms can be delivered electronically as stated above, by facsimile or hand delivered to the FIA offices located at the addresses stated below.

**The Director  
Financial Intelligence Agency  
Private Bag 0190  
Gaborone**

**Plot 50762  
Block 2  
Attorney Generals Chambers, 3<sup>rd</sup> Floor  
Tel: 3998402  
Fax: 3931754**

## **3. Failure to report a suspicious transactions**

Failure to make a Suspicious Transaction Report is a criminal offence punishable by a fine of up to P 50 000 and/or the suspension or revocation of the NBFIs license or registration. A person who fails to make the report will, in their personal capacity, be liable to a fine of up to P10 000 and/or imprisonment for up to six months as provided for by section 25 of the Financial Intelligence Act.

## **4. Register of reported transactions**

Once a suspicious transaction has been reported and delivered to the FIA, NBFIs are required to ensure that records are kept of every report made. These registers are highly confidential and the designated AML/CFT Compliance Officer is required to ensure that they are satisfactorily secured and inaccessible to any unauthorized third parties. The register should contain the following;

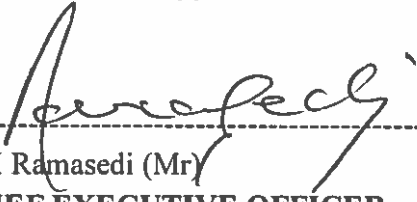
- a) Date that the STR was made;
- b) The person who made the report;



- c) The signature of the person who made the report;
- d) All employees involved in the reported transaction;
- e) The nature of the report (why it was deemed suspicious); and
- f) Date the report was submitted to FIA;
- g) Date that FIA acknowledged and/or provided their feedback.

The designated AML/CFT Compliance officer is responsible for creating and updating this register. In their temporary absence the NBFi must ensure that there is someone else in the organization who can act on their behalf with regards to reporting suspicious transaction and updating the reporting register. Record of the register should be kept for at least seven years and must be available to NBFIRA, and auditors upon request.

**AUTHORISATION**

A handwritten signature in black ink, appearing to read 'O.M. Ramasedi', is written over a horizontal dashed line.

O.M Ramasedi (Mr)  
**CHIEF EXECUTIVE OFFICER**