

BANK OF ZAMBIA ANTI-MONEY LAUNDERING DIRECTIVES, 2004

ARRANGEMENT OF DIRECTIVES

**PART I
PRELIMINARY**

Directives

1. Short Title
2. Interpretation
3. Application of these Directives

**PART II
AUTHORITY OF BANK OF ZAMBIA**

4. Authority of the Bank of Zambia

**PART III
CUSTOMER DUE DILIGENCE AND OTHER OBLIGATIONS**

5. Anti-money laundering measures and practices
6. Customer identification
7. Verification of individual customers' names and addresses
8. Verification of corporate bodies' names and addresses
9. Trusts
10. Record keeping
11. Reporting of suspicious activities
12. Money laundering reporting officer
13. Obligations of employees
14. Obligations of regulated institutions

PART IV
COOPERATION WITH LAW ENFORCEMENT AGENCIES

- 15. Co-operation with law enforcement agencies

PART V
OBLIGATIONS OF THE BOARD AND PRINCIPAL OFFICERS

- 16. Obligations of board and principal officers of regulated institution
- 17. Annual compliance report

PART VI
STAFF TRAINING AND OTHER OBLIGATIONS

- 18. Staff training
- 19. Programme for staff training
- 20. Staff not to disclose investigations to customer
- 21. Staff to report money-laundering offence in which involved

PART VII
GENERAL

- 22. External auditors
- 23. Offence and penalty
- 24. Coming into force of the Directives

FIRST SCHEDULE

SECOND SCHEDULE

Bank of Zambia Anti-Money Laundering Directives, 2004

IN EXERCISE of the powers contained in section 12(4) of the Prohibition and Prevention of Money Laundering Act Number 14 of 2001, the following Directives are hereby made:

PART 1 PRELIMINARY

- | | |
|----------------|--|
| Short title | 1. These Directives may be cited as the Bank of Zambia Anti-Money Laundering Directives, 2004. |
| Interpretation | 2. In these Directives, unless the context otherwise requires, |
| No. 14 of 2001 | “Act” shall mean the Prohibition and Prevention of Money Laundering Act; |
| | “anti-money laundering measures and practices” includes policies, procedures and controls put in place by a regulated institution to prevent and detect money laundering as prescribed in these Directives and by the Bank of Zambia from time to time; |
| Cap. 388 | “corporate body” shall include companies incorporated under the Companies Act, and other legal entities; |
| | “customary authority” shall mean a body with whom a person has or had business dealings as a customer of that body; |
| | “Customer” in relation to a transaction or an account shall include an employee of a regulated institution, a signatory to a transaction or account, any person to whom a transaction has been assigned or transferred, any person who is authorised to conduct a transaction, an employee of a regulated institution, or such other person as may be prescribed by law. |

“establishing a business relationship” means entering into a business relationship, other than opening an account, with a regulated institution or any other obligation arising out of the contractual relationship between a regulated institution and a customer, and includes buying and selling of foreign currency to a customer by a regulated institution;

No. 14 of 2001

“money laundering” shall have the meaning assigned to it in section 2 of the Prohibition and Prevention of Money Laundering Act;

“opening an account” means entering into a relationship with a regulated institution to operate *inter alia* a current account, a deposit account, a savings account or a loan account and includes transmission of money and investment of funds;

Cap. 387

“Principal Officer” means a Chief Executive Officer or Chief Financial Officer as defined under the Banking and Financial Services Act.

“regulated institution” means a bank or a financial institution as licensed or supervised by the Bank of Zambia under the Banking and Financial Services Act;

“suspicious transaction” means a transaction which is inconsistent with a customer's known legitimate business or personal activities or with the normal business for the type of account which the customer holds, and includes, but is not limited to, the activities listed in the First Schedule hereto; and

No. 14 of 2001

“transaction” shall have the same meaning assigned to the term ‘business transaction’ in the Prohibition and Prevention of Money Laundering Act.

Application

3. These Directives shall apply to all banks and financial institutions operating in Zambia.

PART II

AUTHORITY OF BANK OF ZAMBIA

- Authority of the Bank of Zambia
4. The Bank of Zambia shall be the supervisory authority for the purposes of giving effect to these Directives.

PART III

CUSTOMER DUE DILIGENCE AND OTHER OBLIGATIONS

- Anti-money laundering measures and practices
5. A regulated institution shall put in place such anti-money laundering measures and adopt such practices as are necessary for the detection and prevention of money laundering as set out in these Directives.

- Customer Identification
6. (1) A regulated institution shall require its individual customers, when opening an account, establishing business relations, or conducting business transactions, with it, to produce the following documents for identification purposes -
- (a) in the case of a Zambian national, a National Registration Card or valid Passport or Driver's Licence; or
 - (b) in the case of a foreign national, a National Registration Card and a valid Passport with, where applicable, a duly issued visa.
- (2) When a regulated institution has doubts as to the identity of a customer in the course of its business relationship with that customer, the regulated institution shall require that customer to renew that customer's identification or provide further identification documents.
- (3) A regulated institution shall identify the beneficial owner of an account opened with it and any person using remittance and safe custody facilities, and if the regulated institution fails to ascertain the identity of such owner or person, it shall make a report to the Anti Money Laundering Investigations Unit.

- (4) A regulated institution shall establish clear procedures on how to identify a customer who applies to open an account through the internet or other electronic means, and shall not permit a customer to establish a business relationship through this means unless the identity documents of the customer have been verified or confirmed.
- (5) Subsections (3) and (4) shall not apply to a bureau de change.

Verification of individual customers' names and addresses

- 7. **A.** Directives 7B, 8, and 9 shall not apply to a bureau de change.
- 7. **B.** A regulated institution shall verify the names and addresses of its individual customers by any or more of the following methods:-
 - (a) obtaining a reference from a professional, an employer of the individual customer, a known customer of the regulated institution, or a customary authority that knows the applicant all of whom should have known the applicant for not less than one year;
 - (b) in the case of non-residents, obtaining references from the individual customer's foreign banks, where possible;
 - (c) conducting a credit reference agency search;
 - (d) requesting an original or certified true copy of recent council or applicable rates or utility bill receipt;
 - (e) using one of the address validation or verification services on offer; or
 - (f) In addition to one or more of the above, doing all things that the regulated institution may deem necessary to verify the documentation submitted by the applicant.

Verification of Corporate Bodies' names and addresses

- 8. (1) Where a corporate body opens an account with a regulated institution, the regulated institution shall verify the legal existence of the corporate body and identify the directors, the beneficial owners and the management of that corporate body.
- 2) A regulated institution shall obtain the following information and

documentation from a corporate body before it allows the corporate body to open an account with it:

- (a) a certified copy of the certificate of incorporation or equivalent, details of the registered office and the place of business;
- (b) details of the nature of the corporate body's business, the reason for the account being opened, an indication of the expected turnover, the source of funds, and a copy of the last available accounts, where applicable;
- (c) where there is more than one signatory to the account, satisfactory evidence of the identity of all the signatories;
- (d) a certified copy of the resolution of the Board authorising the account signatories;
- (e) certified copy of power of attorney, or any other authority, affecting the operation of the account, given by the directors in relation to the corporate body; and
- (f) such other additional documents as the regulated institution may deem necessary for this purpose.

(3) Where a corporate body intends to establish a business relationship or conduct a specific business transaction with a regulated institution, the regulated institution shall obtain the following information and documentation from the corporate body prior to establishing the business relationship or conducting the business transaction

- (a) the certificate of incorporation or equivalent, details of the registered office and the place of business;
- (b) details of the nature of the corporate body's business, the source of funds, and a copy of the last available accounts, where applicable;
- (c) such other documents as the regulated institution may deem necessary for this purpose.

Trusts

9. (1) A regulated institution shall, when a person opens an account for and on behalf of a trust, endeavour to know and understand the structure of the trust and identity of the trust owners sufficiently to determine the provider and source of funds and the controlling authority of the funds.

(2) Where account is opened or business transaction conducted on behalf of a trust, the regulated institution shall request:

(i) the same information as is required in Directive 8, with the necessary modifications;

(ii) details which prove to the satisfaction of the regulated institution, the identity of the beneficial owner or owners; and

(iii) such other information as may be required to demonstrate the provider and source of funds and the controlling authority of the funds in respect of the trust.

Record Keeping

10. (1) A regulated institution shall maintain

(a) a business transaction record for a period of 10 years after termination of the business transaction and

(b) copies of identification records for a period of 10 years after termination of the business transaction with the customer.

(2) A regulated institution shall keep records under this Directive by way of original documents in the form of hard copies or by using electronic storage devices.

(3) Where the records referred to in this Directive relate to an on-going investigation or business transaction, which has been the subject of a disclosure, a regulated institution shall retain those records, after the ten year period, until, in the case of an on-going investigation, the law enforcement agencies confirm that the investigation has been closed or completed, as the case may be, or, in the case of an on-going business transaction, the regulated institution confirms that the business

transaction has been completed.

(4) The records referred to in sub Directive (1) shall be sufficient to permit a reconstruction of individual business transactions, including the amounts and types of currency involved, if any, so as to provide, if necessary, evidence for prosecution of criminal conduct.

Reporting of
suspicious activities

11. (1) A regulated institution shall report to the Anti Money Laundering Investigations Unit in the Form set out in the Second Schedule hereto any suspicious transactions or suspicious activities by its customers and shall, on request, send to the Anti Money Laundering Investigations Unit copies of the relevant documents and retain the originals.

(2) A person making a suspicious transaction report shall not disclose to an unauthorised person that such a report is being, has been or is about to be made.

(3) A regulated institution shall ensure that all its employees swear an Oath of Secrecy to be administered by a Commissioner for Oaths.

Money Laundering
Reporting Officer

12. (1) A Money Laundering Reporting Officer as provided for in section 13(1)(f) of the Act shall be a person at management level in a regulated institution.

Obligations of Money
Laundering Reporting
Officer

(2) The Money Laundering Reporting Officer shall:

- (a) keep a register of all reports made by employees of the regulated institution and of all reports that the officer makes to the Anti Money Laundering Investigations Unit;
- (b) on written request by the law enforcement agencies,
 - i. give to them an acknowledgment receipt of the reports, from the Anti Money Laundering Investigations Unit ;
 - ii. make available to the law enforcement agencies copies of reports he/she makes to the Anti Money Laundering Investigations Unit and those made to the Money

Laundering Reporting Officer by employees of the regulated institution; and.

- (c) after receiving a report in terms of Directive (13), promptly evaluate whether or not there are reasonable grounds for believing that a customer has been engaging in illegal activities or crime, and if after such evaluation, the Money Laundering Reporting Officer finds that such grounds exist, the Money Laundering Reporting Officer shall immediately report the case to the Anti Money Laundering Investigations Unit in the prescribed format.

(3) If a Money Laundering Reporting Officer resigns from a regulated institution, the Money Laundering Reporting Officer shall prepare and deliver to the Bank of Zambia and the Unit, within ten days after delivery to the regulated institution of the Money Laundering Reporting Officer's resignation, a written statement of the reasons for the resignation.

(4) If a regulated institution terminates the appointment of its Money Laundering Reporting Officer, the regulated institution shall prepare and deliver to the Bank of Zambia and the Unit, within ten days of the decision to terminate the appointment, a written statement of the reasons for the termination.

Obligations
employees of

13. An employee of a regulated institution shall promptly report to a Money Laundering Reporting Officer all cases where:

- (a) the employee becomes aware, has knowledge or suspects or has reasonable grounds to believe, that a customer has been or is involved in an illegal activity or crime; or
- (b) a customer in respect of whom the employee becomes aware, has knowledge or suspects or has reasonable grounds to believe, that another customer has been engaging in illegal activities or crime, deposits, transfers or seeks to invest funds or obtain credit against the security of funds obtained from such illegal activities or crime.

Obligations of regulated institutions

14. A regulated institution shall ensure that all employees concerned with the holding, receipt, transaction and or investment of funds, whether in cash or otherwise, obtained or suspected to have been obtained from illegal activities or crime, or the making of loans against the security of such funds are aware of the procedures set out in these Directives.

PART IV

COOPERATION WITH LAW ENFORCEMENT AGENCIES

Cooperation with Law Enforcement Agencies

15. (1) A regulated institution shall:
 - (a) cooperate with the law enforcement agencies to facilitate the exchange of information relating to money laundering; and
 - (b) with any law which requires the provision of information to the law enforcement agencies to assist in an investigation.
- (2) No act, matter or thing done by a director, principal officer or employee of a regulated institution or by any other person in the exercise or performance or purported exercise or performance, in good faith, of any power, duty or function under these Directives shall give rise to any action, claim, liability suit or demand against the person concerned.

PART V

OBLIGATIONS OF THE BOARD AND PRINCIPAL OFFICERS

Obligations of the board and principal officers of a regulated institution

16. (1) The board and principal officers of a regulated institution shall put in place an anti-money laundering programme consisting of anti money laundering measures to be taken and practices to be adopted in order to detect and prevent the commission of the offence of money laundering, and shall ensure that the employees of the regulated

institution are familiar and comply with the programme.

(2) The measures and practices referred to in sub Directive (1) shall include:

- (a) the development of internal policies, procedures and controls with due regard to the risks posed by money laundering;
- (b) the establishment of "know your customer" procedures, which shall include knowing the customer's business, establishing systems that would recognise suspicious activities and having in place internal reporting procedures of suspicious transactions;
- (c) the appointment of Money Laundering Reporting Officers;
- (d) the establishment of a sound anti-money laundering compliance policy which shall be reviewed by the regulated institution annually and approved by the Bank of Zambia;
- (e) procedures to be followed by directors, principal officers, officers and employees of a regulated institution in the conduct of the business of the regulated institution;
- (f) instructions given to directors, principal officers, officers and employees of a regulated institution on the prevention of the use of the regulated institution for the purpose of engaging in activities of money laundering; and
- (g) training of directors, principal officers, officers and employees of a regulated institution for the purpose of enabling them to identify business transactions which may relate to the commission of the offence of money laundering.

Annual compliance
report

17. The Money Laundering Reporting Officer shall prepare, for the board of the regulated institution, an annual compliance report, relating to but not limited to:

- (a) changes in legislation or industry rules on money laundering issues;
- (b) compliance deficiencies in relation to money laundering; and

- (c) number of internal reports received on money laundering and the percentage of reports that have been submitted to law enforcement agencies.

PART VI

STAFF TRAINING AND OTHER OBLIGATIONS

Staff training

- 18. A regulated institution shall, with the assistance of the Unit, train its employees, irrespective of the level of seniority, on what money laundering is and the importance of reporting any suspicious transactions to its Money Laundering Reporting Officer, and shall draw up a programme for the training of its employees.

Programme for staff training

- 19. (1) The programme referred to in Directive (18) shall include:
 - (a) indicators that may give rise to suspicion and the procedures to be adopted when a business transaction is considered to be suspicious;
 - (b) a component to train the staff of a regulated institution on how to make a report on suspicious activities;
 - (c) the identification and prevention of money laundering for employees of the regulated institution who have contact with clients and compliance personnel;
 - (d) instruction, covering all aspects of money laundering procedures, to those with the responsibility for supervising or managing staff; and
 - (e) an in-depth training for the money laundering reporting officer on all legislation relating to money laundering and the regulated institution's internal policies on money laundering.

- (2) A regulated institution shall hold courses at regular intervals of at least annually for principal officers of a regulated institution, to remind such officers of their responsibilities in relation to money laundering and to raise awareness of any changes in the anti-money

laundering measures and internal procedures.

(3) Notwithstanding the provisions of sub Directives (1) and (2), a regulated institution shall tailor its training programme to suit the needs of the regulated institution depending on the size, the resources available and the type of business it undertakes.

Staff not to disclose investigations to customers

20. An employee of a regulated institution shall not disclose to a customer that the customer is being, has been or is about to be investigated for money laundering activities.

Staff to report money laundering offence in which involved

21. An employee of a regulated institution may report to a principal officer of the regulated institution or the Anti Money Laundering Investigations Unit any money laundering offence in which the employee is involved.

PART VII

GENERAL

External Auditors

22. (1) The Bank of Zambia may require a regulated institution, at the expense of the regulated institution, to be audited by independent external auditors who shall conduct a special audit on the adequacy of anti-money laundering measures, practices and enforcement thereof.

(2) The external auditors referred to in sub Directive (1) shall report in writing to the Bank of Zambia any finding resulting from any audit, or contact by a person with the regulated institution which suggests the commission of the crime of money laundering by that person in that regulated institution, and the Bank of Zambia shall, where such a crime has been or is suspected to have been committed, take all necessary action to prosecute the crime.

Offence and Penalty

No. 14 of 2001

23. A person who contravenes the provisions of these Directives shall be guilty of an offence under section 13 of the Prohibition and Prevention of Money Laundering Act.

Directives to come into force

24. These Directives shall come into force on such day as the Bank of Zambia shall prescribe.

FIRST SCHEDULE

Examples of suspicious activities (Directive 11)

Suspicious Customer Behaviour

- (a) Customer has an unusual or excessively nervous demeanour during the business transaction;
- (b) Customer discusses the regulated institution's record keeping or reporting duties with the apparent intention of avoiding them;
- (c) Customer threatens an employee of a regulated institution attempting to deter a record keeping or reporting duty;
- (d) Customer is reluctant to proceed with a business transaction after being told it must be reported;
- (e) Customer suggests payment of a gratuity to an employee of the regulated institution;
- (f) Customer appears to have a hidden agenda or behaves abnormally, such as passing the opportunity to obtain a higher interest rate on a large account balance; or
- (g) Customer opens an account in the name of a family member who begins making large deposits not consistent with the known legitimate sources of income of the family.

Suspicious Customer Identification Circumstances

- (a) Customer claims to be a law enforcement agent conducting an undercover operation when there are no valid indications to support that;
- (b) Customer furnishes unusual or suspicious identification documents and is unwilling to provide personal background information;
- (c) Customer is unwilling to provide personal background information when opening an account;

- (d) Customer opens or attempts to open an account without identification, references or a local address;
- (e) Customer's permanent address is outside the bank's service area or outside Zambia;
- (f) Customer's home or business telephone is disconnected;
- (g) Business customer is reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity;
or
- (h) Customer provides no record of past or present employment on a loan application.

Suspicious Cash Transactions

- (a) Customers who together, and simultaneously, use separate tellers to conduct large Kwacha cash transactions or foreign exchange transactions;
- (b) Customer opens several accounts in one or more names, and then makes several cash deposits;
- (c) Customer conducts unusual cash transactions through night deposit boxes, especially large sums that are not consistent with the customer's business;
- (d) Customer makes frequent deposits or withdrawals of large amounts of currency for no apparent business reason, or for a business that generally does not generate large amounts of cash;
- (e) Customer conducts several large cash transactions at different branches on the same day, or orchestrates persons to do so on his/her behalf;
- (f) Customer deposits cash into several accounts and then consolidates the funds into one account and wire transfers them outside of Zambia;
- (g) Customer attempts to take back a portion of a cash deposit after learning that a currency transaction report will be filed on the transaction;
- (h) Customer conducts several cash deposits at automated teller machines;
- (i) Corporate account has deposits or withdrawals primarily in cash rather than cheques;
- (j) Customer's cash deposits often contain counterfeit or musty or suspicious

dirty notes;

- (k) Customer frequently deposits large sums of cash wrapped in currency straps stamped by other banks;
- (l) Customer makes frequent purchases of monetary instruments for cash; or
- (m) Customer conducts an unusual number of foreign currency conversion transactions.

Suspicious Wire Transfer Transactions

- (a) Non-account holder sends wire transfer with funds that include numerous monetary instruments;
- (b) An incoming wire transfer has instructions to convert the funds to cashier's cheques and mail them to a non-account holder;
- (c) A wire transfer that moves large sums to secrecy havens such as the Cayman Islands, Hong Kong, Luxembourg, Panama or Switzerland;
- (d) An incoming wire transfer followed by an immediate purchase by the beneficiary of monetary instruments for payment to another party;
- (e) An increase in international wire transfer activity in an account with no history of such activity or where the stated business of the customer does not warrant it;
- (f) Customer frequently shifts purported international profits by wire transfer to another country;
- (g) Customer receives many small incoming wire transfers and then orders a large outgoing wire transfer to another country; or
- (h) Account in the name of a currency exchange house receives wire transfers or cash deposits of a substantial amount.

Suspicious Safe Deposit Box Activity

- (a) Customer's activity increases in the safe deposit box area, possibly indicating the safekeeping of large amounts of cash; or
- (b) Customer rents multiple safe deposit boxes.

Suspicious Activity in Credit Transactions

- (a) Customer's financial statement makes representations that do not conform to generally accepted accounting principles;
- (b) Transaction is made to appear more complicated than it needs to be by use of impressive but unnecessary terms such as "emission rate," "prime bank notes," "standby commitment," "arbitrage" or "hedge contracts," etc;
- (c) Customer requests loans to offshore companies or loans secured by obligations of offshore banks;
- (d) Customer suddenly pays off a large problem loan with no plausible explanation for the source of funds;
- (e) Customer collateralizes a loan with cash deposits;
- (f) Customer uses cash collateral located offshore to obtain a loan; or
- (g) Customer's loan proceeds are unexpectedly transferred offshore.

Suspicious Commercial Account Activity

- (a) Business customer presents financial statements noticeably different from those of similar businesses;
- (b) Large business presents financial statements that are not prepared by an accountant;
- (c) Retail business that provides cheque cashing service does not make large withdrawals of cash against cheque deposits, possibly indicating that it has another source of cash;
- (d) Customer maintains an inordinately large number of accounts for the type of business purportedly being conducted;
- (e) Corporate account shows little or no regular or periodic activity; or
- (f) Transaction includes circumstances that would cause a banker to reject a loan application because of doubts about the collateral's validity.

Suspicious Trade Financing Transactions

- (a) Customer seeks trade financing on the export or import of commodities whose stated prices are substantially more or less than those in a similar market situation;
- (b) Customer makes changes to a letter of credit beneficiary just before payment is to be made;
- (c) Customer changes the place of payment in a letter of credit to an accountant in a country other than the beneficiary's stated location; or
- (d) Customer's standby letter of credit is used as a bid or performance bond without the normal reference to an underlying project or contract, or in favour of unusual beneficiaries.

Suspicious Investment Activity

- (a) Customer uses an investment account as a pass-through vehicle to wire funds particularly to off-shore locations;
- (b) Investor seems unconcerned about the usual decisions to be made about an investment account such as fees or suitable investment vehicles;
- (c) Customer wants to liquidate a large position through a series of small transactions; or
- (d) Customer deposits cash, money order, traveller's cheques or counter cheques to fund an investment account.

Suspicious Deposits

- (a) Customer deposits a large number of traveller's cheques often in the same denomination and in sequence without a reasonable explanation; or
- (b) Customer deposits money orders bearing unusual markings.

Miscellaneous Suspicious Customer Activity

- (a) Customer who is a student uncharacteristically transfers or exchanges large sums of money;
- (b) Account shows high velocity in the movement of funds, but maintains low beginning and ending daily balances;
- (c) Transaction includes correspondence received that is a copy rather than original letterhead;
- (d) Transaction involves offshore institutions whose names resemble those of well known legitimate banks;
- (e) Transaction involves unfamiliar countries or islands that cannot be found on a world atlas or map; or
- (f) Agent, attorney or financial advisor acts for another person without proper documentation such as a power of attorney.

Suspicious Employee Activity

- (a) Employee exaggerates the credentials, background or financial ability and resources of a customer in written reports the bank requires;
- (b) Employee is frequently involved in unresolved exceptions or recurring exceptions on exception reports;
- (c) Employee lives a lavish lifestyle that can not be supported by his or her salary;
- (d) Employee frequently overrides internal controls or established approval authority or circumvents policy;
- (e) Employee uses company resources to further private interests;
- (f) Employee assists transactions where the identity of the ultimate beneficiary or counter party is undisclosed; or
- (g) Employee deliberately avoids taking vacations.

SECOND SCHEDULE
Suspicious activity report to the Anti Money Laundering Investigations Unit
(Directive 11)

Purpose of this Form

This form provides an effective means for a regulated institution to notify the appropriate authorities of known or suspected criminal conduct or suspicious activities, that may be associated with violations of the law, that come to their notice.

Authority for making the Report

In addition to Directive 15 of these Directives, this Report is made under the authority of the Prohibition and Prevention of Money Laundering Act. The Act provides for criminal liability for any regulated institution, its directors and its employees arising as a result of any of the suspected violations of the law made by way of this Report.

Part I: Reporting Regulated Institution

Details of Regulated Institution	
<i>Name:</i>	
<i>Postal Address:</i>	
<i>Address of branch where activity occurred:</i>	
<i>Postal Address:</i>	
<i>Nature of Business (Whether Banking Business or Financial Service Business)</i>	
<i>Supervisory Authority</i>	

Part II: Suspicious Activity Information

Date of suspicious activity:	Amount involved in known or suspected activity: K..... US\$.....															
<p>Summary characterization of suspicious activity (Tick accordingly):</p> <table border="0"> <tr> <td>Bribery</td> <td>Counterfeit cheque</td> <td>Counterfeit credit or debit card</td> </tr> <tr> <td>Money laundering</td> <td>False statement</td> <td>Counterfeit instrument (other)</td> </tr> <tr> <td>Cheque fraud</td> <td>Mortgage loan fraud</td> <td>Misuse of position or self dealing</td> </tr> <tr> <td>Cheque kiting</td> <td>Credit or debit card fraud</td> <td>Commercial fraud</td> </tr> <tr> <td>Electronic transfer fraud</td> <td>Defalcation or embezzlement</td> <td>Other (specify)</td> </tr> </table>		Bribery	Counterfeit cheque	Counterfeit credit or debit card	Money laundering	False statement	Counterfeit instrument (other)	Cheque fraud	Mortgage loan fraud	Misuse of position or self dealing	Cheque kiting	Credit or debit card fraud	Commercial fraud	Electronic transfer fraud	Defalcation or embezzlement	Other (specify)
Bribery	Counterfeit cheque	Counterfeit credit or debit card														
Money laundering	False statement	Counterfeit instrument (other)														
Cheque fraud	Mortgage loan fraud	Misuse of position or self dealing														
Cheque kiting	Credit or debit card fraud	Commercial fraud														
Electronic transfer fraud	Defalcation or embezzlement	Other (specify)														
Amount of loss prior to recovery (if applicable) K..... \$.....	Amount of recovery (if applicable) K..... \$.....															

Has the suspicious activity had a material impact on the financial soundness of the institution?	(Tick) Yes No
If any law enforcement agency has already been advised, please list the agency, address and contact details: Agency: Physical Address: Postal Address: Contact Person: Telephone/Fax: Email:	

Part III: Contact details - Money Laundering Reporting Officer

Last Name:	First Name:	Other Names:
Title:.....	Office Phone Number:	Date:

PART IV: Contact for Assistance (if different from person named in Part III)

Last Name:	First Name:	Other Names:
Title:..... NRC No.....	Phone No. Work:..... Home:..... Cell:.....	Date:

Part V: Description of Suspicious Activity

This section of the report is critical. The care with which it is written may make the difference in whether or not the described conduct and its possible criminal nature are clearly understood. Please provide on the next page an account of the possible violation of law, including what is unusual, irregular or suspicious about the transaction. Use the following check list as a guide:

- (1) Explain who benefited from the transaction, how, and by how much. Indicate whether currency or monetary instruments were involved;

- (2) Indicate where the possible violation took place;
- (3) Indicate whether the transaction is an isolated incident or involves other transactions;
- (4) Is there any related litigation? If so, explain the nature of the litigation;
- (5) Describe any supporting documentation, including any explanation of the transaction given by the suspect (or anybody else) and indicate to whom and when it was given. Retain any supporting documentation;
- (6) Retain any evidence of a cover-up or attempt to deceive auditors or investigators; and
- (7) Recommend any further investigation that might assist law enforcement authorities.

This report was made this day of, 20.....

.....
Money Laundering Reporting Officer

INSTRUCTIONS

WHO SHOULD COMPLETE THE FORMS

All regulated institutions operating in Zambia are required to make these reports (Schedule two) following discovery of suspicious activity that is suspected of being associated with violations of the law in the categories listed below -

(a) Inside abuse

The reports should be made whenever the regulated institution detects any known or suspected criminal violation, committed against that regulated institution or involving a transaction conducted through that regulated institution, where the regulated institution has a substantial basis for identifying one of its directors, officers, employees, or agents as having committed, or aided in the commission of a criminal act.

(b) Transactions involving potential money laundering

The reports should be made whenever the regulated institution becomes aware of a suspicious transaction, or series of transactions that it knows or suspects may be in the categories listed below –

- (1) the transaction involves funds derived from illegal activities or is intended to hide or disguise funds or assets derived from illegal activities (including the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate any law or Directive; or
- (2) the transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the regulated institution knows of no reasonable explanation of the transaction after examining the available facts, including the background and possible purpose of the transaction.

(c) Other suspect transactions

The reports should be made whenever the regulated institution becomes aware of any other transaction (or series of transactions) that it knows or suspects may be associated with any actual or potential violation of any law or Directive. A report should be made regardless of whether a suspect can be identified and regardless of whether the regulated institution has suffered actual or potential loss.

SUBMISSION OF REPORTS

Send each completed **second schedule** suspicious activity report to:

The Commissioner
Anti Money Laundering Investigations Unit
Drug Enforcement Commission
Ridgeway
Lusaka, Zambia

Do not include supporting documentation with the suspicious activity reports. Retain a copy of the reports and all supporting documentation for 10 years after termination of the business relationship with the customer or, in some cases, upon notification of the closure of a case by a law enforcement agency. All supporting documentation must be made available to appropriate authorities upon request.

In cases requiring immediate attention, such as when a violation is in progress, the regulated institution should notify the Anti Money Laundering Investigations Unit or any other competent authority immediately.

These Directives have been duly approved by the Anti Money Laundering Investigations Unit pursuant to Section 12 of the Prohibition and Prevention of Money Laundering Act, No. 14 of 2001.

Issued by the Bank of Zambia this 19th day of August 2004.



.....
Denny H. Kalyalya (Dr)
DEPUTY GOVERNOR - OPERATIONS

Cc: Governor