

**BANK OF NAMIBIA**

**No. 121**

**2 June 1998**

**DETERMINATIONS UNDER THE BANKING INSTITUTIONS ACT, 1998  
(ACT NO 2 OF 1998)**

In my capacity as Governor of the Bank of Namibia (The Bank), and under the powers vested in the Bank by virtue of section 71(3) of the Banking Institutions Act, 1998 (Act No 2 of 1998), read in conjunction with section 50 of the aforementioned Act, I hereby issue the Determinations on Money Laundering and "Know your Customer Policy" (BID-3), which Determinations shall become effective on 1 July 1998.

**T K ALWEENDO  
GOVERNOR**

**WINDHOEK, 2 June 1998**

## **DETERMINATIONS ON MONEY LAUNDERING AND “KNOW YOUR CUSTOMER POLICY”**

### **Overview**

Money laundering covers all activities and procedures to change the identity of illegally obtained money so that it appears to have originated from a legitimate source.

The most common form of money laundering that banking institutions will encounter on a day-to-day basis takes the form of accumulated cash transactions which are deposited in the banking system or exchanged for value items. These simple transactions may be just one part of the sophisticated web of complex transactions set out on the next pages. Nevertheless, the basic fact remains that the key stage for the detection of money laundering operations is where the cash first enters the banking system.

### **1. Stages of Money Laundering**

There are three stages of money laundering. In each of them, there may be numerous transactions made by launderers through banking institutions, i.e.:

- 1.1 **placement** - the physical disposal of cash proceeds derived from illegal activity often by converting such cash into non-cash assets;
- 1.2 **layering** - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity; and
- 1.3 **integration**- the turning of criminally derived wealth into "legitimate" funds.

If the layering process succeeds, the integration phase places the laundered proceeds back into the economy in such a way that the funds re-enter the financial system as legitimate business funds.

## **2. The Basle Statement of Principles**

The adoption of a Statement of Principles by the Basle Committee on Banking Regulations and Supervisory Practices in December 1988 and by the banking community worldwide, is a step towards preventing the use of the financial system for criminal and money laundering purposes. The Statement is essentially of a general nature, containing ethical principles aimed at encouraging banking and other financial institutions to put in place within their institutions, certain effective procedures and basic policies to assist in the suppression of money-laundering through the banking system. To this end, the Statement recommends that financial institutions should implement specific procedures to ensure that:

- 2.1 all persons conducting business with them are properly identified;
- 2.2 all transactions that do not appear legitimate are discouraged; and
- 2.3 cooperation with law enforcement agencies is achieved.

The Bank is of the view that the adoption of the Statement of Principles on the Prevention of Criminal Use of the Banking System would be beneficial to the banking industry in Namibia. **Annexure A** provides details on the Basle Statement of Principles.

## **3. Implementation of "Know Your Customer Policy"**

### **3.1 Introduction**

The requirement for a banking institution to report cases of suspicious money transactions to the Bank of Namibia is governed by section 50 of the Banking Institutions Act, 1998 (Act 2 of 1998). The Bank of Namibia Act, 1997 (Act 15 of 1997) prohibits any person to directly or indirectly disclose to another person any information that he or she has acquired in the performance of his or her duties or functions for or on behalf of the Bank, except for the purpose of the performance of his or her duties or

functions in terms of that Act or when required to do so by a court of law or under any law or on authority of the Board of Directors of the Bank. The question of breaching customer confidentiality is thus well provided for.

In view of this, and the need for awareness, vigilance and a system for monitoring, investigating and reporting suspicious transactions, the minimum safeguards for banking institutions to detect and combat such activities shall include the development of a "Know Your Customer Policy" incorporating the following concepts, procedures and controls.

### **3.2 Opening of Accounts**

Banking institutions should ensure proper identification of their customers at the time a relationship is established, particularly when opening a deposit account or when offering a safe custody facility in order to prevent the creation of fictitious accounts. Apart from official identification documents, a good form of verification of identity is by way of personal introduction from a known and respected customer and/or a member of staff. The golden rule is that a business relationship with a banking institution should never be established until the identity of a potential customer is satisfactorily established.

If a potential customer refuses to produce any of the requested information, any relationship already begun should be terminated.

Banking institutions should not keep anonymous accounts or accounts in obviously fictitious names.

### **3.3 Record Keeping**

The principle that "traces must remain" is an important one, particularly in facilitating the needs of the investigating authorities in drug and other crime-related money laundering cases. Document retention may be by way of original documents, microfiche or in computerized form. Banking institutions should keep a copy or references of a customer's identification document, such as, a Namibian identity card or international

passport, as well as records of transactions such as account ledgers, credit/debit vouchers and cheques.

### 3.4 **Sufficient Knowledge of Customer's Activities**

Banking institutions should exercise "due diligence" by paying special attention to all complex, unusual large transactions, especially substantial cash deposits or withdrawals, and all unusual patterns of transactions which have no apparent economic or visibly lawful purpose. A suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of account. Therefore, the first key to recognition is knowing enough about the customer's business to recognize that a transaction, or series of transactions, is unusual. Examples of customer behaviour or activity which may warrant investigation are provided in **Annexure B**.

### 3.5 **Reporting of Suspicious Transactions**

Banking institutions are required to report immediately to the Bank all cases of suspicious transactions involving an amount of N\$50 000 or more.

The obligation to report is on the individual who becomes suspicious. Some banking institutions, however, may choose to require such unusual or suspicious transactions to be drawn to the attention of supervisory management (branch or departmental manager). The circumstances of each case can then be reviewed at that level to determine whether the suspicion is justified. In the absence of factual information to negate the suspicion, the decision should be taken to report without delay. In any case, banking institutions may wish to assign one of its officers, the additional responsibility of being a focal point or contact person for such reporting.

3.6 **Annexure C** contains a standard format which shall be used for reporting suspicious transactions. In the event that urgent disclosure is required in a "live" situation, particularly when the account concerned is part of an

on-going investigation, an initial notification should be made to the Bank Supervision Department of the Bank by telephone.

### **3.7 Adequate Internal Control Procedures**

Banking institutions should establish adequate procedures of internal control and communication in order to forestall and prevent operations related to money laundering. Such procedures may include, as appropriate, the designation of a compliance officer at management level as well as an audit function to test all procedures relating to the prevention of money laundering.

### **3.8 Staff Awareness**

The effectiveness of the procedures and recommendations contained in these Determinations depends on the extent to which staff in banking institutions appreciate the seriousness and potential implications of the issue. They must be encouraged to co-operate fully with the law enforcement agencies and to provide prompt reporting of suspicious transactions.

Timing and content of training packages for staff will be dictated by the institution's specific needs.

The following shall be adopted as a minimum: -

#### **3.8.1 New Employees**

A general appreciation of the background to money laundering and the subsequent need for reporting of any suspicious transactions to the appropriate designated focal point should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority.

### 3.8.2 **Cashiers/Foreign Exchange staff**

Members of staff who are dealing directly with the public are the first point of contact with potential money-launderers and they must be made aware of their responsibilities and of the organisation's reporting system for such transactions. It is vital that "these front line" staff are made aware of the institution's policy for dealing with non-regular customers, particularly where large cash transactions are involved.

### 3.8.3 **Account Opening/New Client Personnel**

Staff who deal with account opening or new clients should receive similar training as those front line staff. In addition, the need to verify the identity of the customer must be understood, and training should be given in the area of account opening and customer/client verification procedures.

3.8.4 It is also necessary to make arrangements for refresher training at regular intervals to ensure that staff are reminded of their responsibilities.

## 3.9 **Funds Transfers**

It should be noted that funds transfers, particularly international funds transfers can be used for layering or to dissimulate the identity of the original ordering customer or the beneficiary. In this regard, banking institutions are required, when effecting funds transfers, to ensure that the names, addresses and account numbers of both the ordering customer and the beneficiary are identified. The name of the banking institution acting for the ordering customer should also be identified. The above information is considered necessary for purposes of maintaining a credible audit trail.

## **Basle Statement of Principles**

### **I. Purpose**

Banking and other financial institutions may unwittingly be used as intermediaries for the transfer or deposit of money derived from criminal activity. The intention behind such transactions is often to hide the beneficial ownership of funds.

The use of the financial system in this way is of direct concern to police and other law enforcement agencies; it is also a matter of concern to banking supervisors and banking institutions' management, since public confidence in banking institutions may be undermined through their association with criminals.

This Statement of Principles is intended to outline some basic policies and procedures that banking institutions' management should ensure are in place within their institutions with a view to assisting in the suppression of money laundering through the banking system, national and international. The Statement thus sets out to reinforce existing best practices among banking institutions and specifically, to encourage vigilance against criminal use of the payments system, implementation by banking institutions of effective preventive safeguards, and cooperation with law enforcement agencies.

### **II. Customer Identification**

With a view to ensuring that the financial system is not used as a channel for criminal funds, banking institutions should make reasonable efforts to determine the true identity of all customers requesting the institution's services. Particular care should be taken to identify the ownership of all accounts and those using safe custody facilities. All banking institutions should institute effective procedures for obtaining identification from new customers. It should be an explicit policy that significant business transactions will not be conducted with customers who fail to provide evidence of their identity.

### **III. Compliance with Laws**

Banking institutions' management should ensure that business is conducted in conformity with high ethical standards and that laws and regulations pertaining to financial transactions are adhered to. As regards transactions executed on behalf of customers, it is accepted that banking institutions may have no means of knowing whether the transaction stems from or forms part of criminal activity.

Similarly, in an international context it may be difficult to ensure that cross-border transactions on behalf of customers are in compliance with the regulations of another country. Nevertheless, banking institutions should not set out to offer services or provide active assistance in transactions which they have good reason to suppose are associated with money laundering activities.

### **IV. Co-operation with Law Enforcement Authorities**

Banking institutions should cooperate fully with national law enforcement authorities to the extent permitted by specific local regulations relating to customer confidentiality. Care should be taken to avoid providing support or assistance to customers seeking to deceive law enforcement agencies through the provision of altered, incomplete or misleading information.

Where banking institutions become aware of facts which lead to the reasonable presumption that money held on deposit derives from criminal activity or that transactions entered into are themselves criminal in purpose, appropriate measures consistent with the law, should be taken, for example, to deny assistance, sever relations with the customer and close or freeze accounts.

### **V. Adherence to the Statement**

All banking institutions should formally adopt policies consistent with the principles set out in this Statement and should ensure that all members of their staff concerned, wherever located, are informed of the institution's policy in this regard. Attention should be given to staff training in matters covered by the Statement. To promote adherence to these principles, banking institutions should implement specific procedures for customer identification and for retaining internal records of transactions. Arrangements for internal audit may

need to be extended in order to establish an effective means of testing for general compliance with the Statement.

## **ANNEXURE B**

### **Examples of Suspicious Transactions**

#### **1. Money Laundering Using Cash Transactions**

- (a) Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.
- (b) Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.
- (c) 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.
- (d) Company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than in the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit and Bills of Exchange).
- (e) Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments.
- (f) Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.
- (g) Frequent exchange of cash into other currencies.

- (h) Branches that have a great deal more of cash transactions than usual. (Head Office statistics should detect aberrations in cash transactions).
- (i) Customers whose deposits contain counterfeit notes or forged instruments.
- (j) Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.
- (k) Large cash deposits using night safe facilities, thereby avoiding direct contact with banking institution's staff.

## **2. Money Laundering Using Bank Accounts**

- (a) Customers who wish to maintain a number of trustee or clients' accounts which do not appear consistent with the type of business, including transactions which involve nominee names.
- (b) Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.
- (c) Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).
- (d) Reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the banking institution to verify.
- (e) Customers who appear to have accounts with several banking institutions within the same locality, especially when the banking institution is aware of a regular consolidation process from such accounts prior to a request

for onward transmission of the funds.

- (f) Matching of payments out with credits paid in by cash on the same or previous day.
- (g) Paying in large third party cheques endorsed in favour of the customer.
- (h) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.
- (i) Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.
- (j) Companies' representatives avoiding contact with the branch.
- (k) Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.
- (l) Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.
- (m) Insufficient use of normal banking facilities e.g. avoidance of high interest rate facilities for large balances.
- (n) Large number of individuals making payments into the same account without an adequate explanation.

### **3. Money Laundering Using Investment Related Transactions**

- (a) Purchasing of securities to be held by the banking institution in safe custody, where this does not appear appropriate given the customer's apparent standing.

- (b) Back to back deposit/loan transactions with subsidiaries of, or affiliates of, overseas banking institutions in known drug trafficking areas.
- (c) Requests by customers for investment management services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customer's apparent standing.
- (d) Larger or unusual settlements of securities in cash or bearer form.
- (e) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.
- (f) A number of transactions by the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, the proceeds being credited to an account different from the original account.
- (g) Investor introduced by an overseas banking institution, affiliate or other investors both of which are based in countries where production of drugs or drug trafficking may be prevalent.

#### **4. Money Laundering Involving Offshore/International Activity**

- (a) Customer introduced by an overseas branch, affiliate or other banking institution based in countries where production of drugs or drug trafficking may be prevalent.
- (b) Use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.
- (c) Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from, countries which are commonly associated with the production, processing, marketing of drugs or terrorist organizations.

- (d) Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.
- (e) Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account.
- (f) Frequent requests for travellers cheques, foreign currency drafts or other negotiable instruments to be issued.
- (g) Frequent paying in of travellers cheques or foreign currency drafts particularly if originating from overseas.

#### **5. Money Laundering Involving Financial Institution Employees and Agents**

- (a) Changes in employee characteristics, e.g. lavish life styles or avoiding taking holidays.
- (b) Any dealing with an agent where the identity of the ultimate beneficiary or counter party is undisclosed, contrary to normal procedure for the type of business concerned.

#### **6. Money Laundering by Secured and Unsecured Lending**

- (a) Customers who repay problem loans unexpectedly.
- (b) Request to borrow against assets held by the banking institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.
- (c) Request by a customer for a banking institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.

**7. Use of Dummy Companies or Trusts**

- (a) Clients forming companies or trusts with no apparent commercial purposes.
- (b) Long delays by clients producing company and trust financial statements.

**ANNEXURE C**

**Money Laundering: Reporting of suspicious transactions**

Report No.		
Name of Institution		
Branch Address and Tel. No.		
Account Name(s) (in full)		
Date of opening		
Occupation & Employer		
Nationality		Passport No.
Identification and/or references		
Address of subject		
Details of sums arousing suspicion indicating debit or credit, source & currency used (including the source, amount and date of suspicious transactions.)		
Other relevant information including reason for suspicion.		

Date: .....

Signature: .....

Name in full: .....

Designation: .....