TO ALL LICENSEES:

NOTICE

RE: INTERIM GUIDELINES FOR ANTI-MONEY LAUNDERING AND KNOW YOUR CUSTOMER PROCEDURES FOR LICENSEES

Please be advised that the following guidelines have been issued for Licensees' immediate adherence, effective today, April 1, 2004.

Any questions regarding these guidelines should be addressed to The Manager, Bank Supervision Department.

CENTRAL BANK OF THE BAHAMAS

SUPERVISORY AND REGULATORY GUIDELINES: 2004-03
AML-KYC
1st April, 2004

INTERIM GUIDELINES FOR ANTI-MONEY LAUNDERING AND KNOW YOUR CUSTOMER PROCEDURES FOR LICENSEES

I. INTRODUCTION

The Central Bank of The Bahamas *("the Central Bank")* is responsible for the licensing, regulation and supervision of banks and trust companies operating in and from within The Bahamas pursuant to The Banks and Trust Companies Regulation Act, 2000, and The Central Bank of The Bahamas Act, 2000. Additionally, The Central Bank has the duty, in collaboration with financial institutions, to promote and maintain high standards of conduct and management in the provision of banking and trust services.

All licensees are expected to adhere to the Central Bank's licensing and prudential requirements and ongoing supervisory programmes, including periodic onsite inspections, and required regulatory reporting. Licensees are also expected to conduct their affairs in conformity with all other Bahamian legal requirements.

II. PURPOSE

The Banks and Trust Companies Regulation Act, 2000 directs the Inspector of Banks and Trust companies to ensure that banks have in place strict Know-Your-Customer (KYC) rules that promote high ethical and professional standards, and so prevent the use of the bank for criminal purposes. The Inspector is required to ensure effective off-site supervision of licensees and is empowered to conduct on-site examinations for the purpose of satisfying himself that the provisions of inter alia the Financial Transactions Reporting Act, 2000 are being complied with.

The Central Bank will shortly issue for consultation, Guidelines for Anti-Money Laundering and Know Your Customer Procedures for Licensees. These Guidelines will replace the existing Guidelines on Anti-Money Laundering and Suspicious Transactions Reporting issued by the Financial Intelligence Unit in 2001, but only in relation to anti-money laundering and know your customer procedures. Licensees should continue to adhere to the FIU's Guidelines insofar as they relate to suspicious transactions reporting.

The Central Bank has prepared these Interim Guidelines to inform licensees of their obligations under the Financial Transactions Reporting (Amendment) Act, 2003 (the Amending Act) and the Financial Transactions Reporting (Amendment) Regulations, 2003 (the Amending Regulations). These amendments maintain the current high standards which exist in The Bahamas, while offering increased flexibility in the application of the AML-KYC requirements.

For Licensees to adequately apply the Amending Regulations, they will need to adopt a risk based approach to customer due diligence. These Interim Guidelines set out for licensees, the minimum criteria for developing a risk based approach to verifying customer identity.

III. APPLICABILITY

These Interim Guidelines apply to all licensees of the Central Bank of The Bahamas.

IV. APPLICABLE LEGISLATION

For the purposes of these Interim Guidelines licensees should have regard to the following legislation:

- Banks and Trust Companies Regulation Act, 2000 (Chapter 316 of the Statute Laws of The Bahamas, 2000)
- Financial Transactions Reporting Act, 2000 (Chapter 368 of the Statute Laws of The Bahamas, 2000)
- Financial Transactions Reporting Regulations, 2000 (Chapter 368 of the Subsidiary Legislation of The Bahamas, 2000)
- Financial Transactions Reporting (Amendment) Act, 2003 (Act No. 23 of 2003)
- Financial Transactions Reporting (Amendment) Regulations, 2003 (S.I. No. 103 of 2003)

V. FINANCIAL TRANSACTIONS REPORTING (AMENDMENT) ACT, 2003

The Financial Transactions Reporting Act, 2000 (FTRA) was amended by the Financial Transactions Reporting (Amendment) Act, 2003. The Amending Act which came into force on 1st January, 2004, effected the following changes to the FTRA:

Inclusion of Investment Fund Operators

- **Section 3(1)(i)** of the FTRA, as amended, previously included fund administrators and operators in the definition of "financial institution". The amendment removed this reference and replaced it with a reference to investment fund administrators and operators of investment funds (as defined by the Investment Funds Act, 2003).

Further Verification of Customer Identity in the Case of Suspicious Transactions

- **Section 10A** has been added to the FTRA and provides, in addition to the existing statutory requirements for verifying the identity of any customer, that financial institutions must also carry out such verification as soon as practicable after they know, suspect or have reasonable grounds to suspect that a customer is conducting or proposes to conduct a transaction which:
  - involves the proceeds of criminal conduct as defined in the Proceeds of Crime Act, 2000; or
  - is an attempt to avoid the enforcement of the Proceeds of Crime Act, 2000.

VI. FINANCIAL TRANSACTIONS REPORTING (AMENDMENT) REGULATIONS, 2003

The Financial Transactions Reporting Regulations 2000 (FTRR) were amended by the Financial Transactions Reporting (Amendment) Regulations, 2003. The Amending Regulations, which came into force on 1st January 2004, effected the following changes to the FTRR:

Prescribed Amount

- **Regulation 2,** as amended, has increased the prescribed amount from $10,000 to $15,000.

Individual Customers

- **Regulation 3(1)**, as amended, prescribes the minimum KYC information which financial institutions must obtain when they seek to verify the identities of individual customers. The required information is as follows:

  (a) full and correct name of the individual;
  (b) address;
  (c) date and place of birth; and
  (d) purpose of the account and the nature of the business relationship.

- **Regulation 3(2),** as amended, introduces a risk based approach to customer due diligence and provides financial institutions with guidance on the type of information and documentation they may rely upon (apart from the required information) when verifying an individual customer's identity.

  In any case where a licensee is required by the FTRA to verify the identity of an individual customer, no new accounts should be opened by the licensee without the minimum KYC information required by regulation 3(1).

Companies, Partnerships and Unincorporated Businesses

- **Regulations 4 and 5,** as amended, adopt a risk based approach to verifying the identities of corporate entities (see Regulation 4), partnerships and other unincorporated businesses (see Regulation 5).

Beneficial Owners

- **Regulation 7A,** has been added to the FTRR and requires licensees to verify the identities of the beneficial owners of all facilities.

  In the case of corporate entities, however, the requirement to verify beneficial owner identity is limited to those beneficial owners having a controlling interest in the corporate entity.

For the purposes of these Interim Guidelines, the Central Bank defines "controlling interest" as an interest of ten percent or more of a corporate entity's voting shares.

Exemption from Verification Procedures

- **Regulation 5(A)(i)** of the Amending Regulations provides that verification of identity is not normally required in the case of a customer with a Bahamian dollar (B$) facility of or below $15,000. Where an exempted customer is an individual, licensees should ensure that they have the minimum information detailed in regulation 3(1).

Ongoing Monitoring of the Business Relationship

The Central Bank expects all licensees to have in place a process for the ongoing monitoring of client account activity. The purpose of such monitoring is to enable licensees to compare actual account activity with the customers' stated account purposes and to identify irregular or suspicious transactions (where cost is justified, an automated transaction monitoring system is preferred). The monitoring process should be documented in licensees' policies and procedures and should clearly articulate the additional due diligence measures to be taken when suspicious or unusual transactions are identified.

- **Regulation 9(1)**, as amended, requires further verification of customer identity (after the establishment of the business relationship), if there is a material change in the way a customer's facility is operated. Although "material change" is not defined in the regulation, the Central Bank is of the view that a material change is a change which is inconsistent with a facility holder's account profile.

- **Regulation 9(2)**, as amended, requires financial institutions to monitor customer accounts throughout the business relationship.

Appropriate records should be maintained by licensees to evidence that the monitoring process is carried out on a consistent basis and oversight of the process is provided by management. Where unusual transactions are identified, licensees should document the factors they considered when reviewing an unusual transaction and any decision made regarding the transaction, whether or not a Suspicious Transaction Report is made to the Financial Intelligence Unit. The documentation for transactions should be kept in a file available for review by the licensee's auditors and the Central Bank.

VII. RISK RATING CUSTOMERS

International Standards

In its paper issued in October, 2001 on Customer Due Diligence for Banks, The Basel Committee on Banking Supervision recognises that adequate KYC policies and procedures have particular relevance to the safety and soundness of banks, in that such policies:

- prevent reputation risk and preserve the integrity of the banking system by preventing the use of the bank for criminal purposes;
- complement the risk management strategy of banks (by enabling them to identify, limit and control risk exposure in assets and liabilities).

Similarly, the Financial Action Task Force (FATF), in its revised 40 Recommendations on Anti-money Laundering and Combating the Financing of Terrorism, issued in June 2003, also recommends that financial institutions adopt a risk based approach to customer due diligence.

The FTRA and FTRR, as amended, adopt the risk based approach recommended by the Basel Committee and the FATF. The FTRR, as amended, gives financial institutions the discretion to determine the appropriate level of information and documentation required to verify customer identity based on the nature and degree of risk inherent in the customer relationship. This approach is in keeping with international best practices.

Developing a Risk Rating Framework

Every licensee is required to develop and implement a risk rating framework which is approved by its Board of Directors as being appropriate for the type of products offered by the licensee, and capable of assessing the level of potential risk each client relationship poses to the licensee. As part of the on-going on-site examination program, Central Bank on-site examiners will assess the adequacy of licensees' risk rating policies, processes and procedures, in light of the type of business conducted by licensees, as well as the extent to which licensees have adhered to legislative requirements.

As a minimum the risk rating framework should include:

1. Differentiation of client relationships by risk categories (such as high, moderate or low);
2. Differentiation of client relationships by risk factors (such as products, client type/profession, country of domicile, complexity of ownership and legal structure, source of business, type of assets, size and volume of transactions, type of transactions, cash transactions, adherence to client activity profile);
3. The KYC documentation and information requirements appropriate for each Risk Category and Risk Factor; and,
4. A process for the approval of the downgrading/upgrading of risk ratings.

The risk rating framework should provide for the periodic review of the customer relationship to allow the licensee to determine whether any adjustment should be made to the risk rating. The review of the risk rating for high risk customers may be undertaken more frequently than for other customers and a determination made by senior management as to whether the relationship should be continued. All decisions regarding high risk relationships and the basis for these decisions should be documented.

The risk rating framework should include customer acceptance and on-going monitoring policies and procedures that assist the licensee in identifying the types of customer that are likely to pose

a higher than average risk of money laundering. A more extensive customer due diligence process should be adopted for higher risk customers. There should also be clear internal guidelines on which level of management is able to approve a business relationship with such customers.

The risk rating framework should provide for documentation of any changes in a customer's risk rating and the reason(s) for such change.

In determining the risk profile of any customer, licensees should take into account factors such as the following risk criteria (which are not set out in any particular order of importance nor should they be considered exhaustive):

(a) geographical origin of the customer

(b) geographical sphere of customer's business activities including the location of the counterparties with which the customer conducts transactions and does business, and whether the customer is otherwise connected with certain high risk jurisdictions, or those known to the licensee to lack proper standards in the prevention of money laundering or customer due diligence process;

(c) nature of the customer's business, which may be particularly susceptible to money laundering risk, such as pawn shops or casinos that handle large amounts of cash;

(d) nature of activity;

(e) frequency of activity;

(f) customer type, e.g. potentates/politically exposed persons;

(g) type, value and complexity of the facility;

(h) unwillingness of the customer to cooperate with the licensee's customer due diligence process for no apparent reason;

(i) unreasonable pattern of account activity given the licensee's information on the customer;

(j) for a corporate customer, unduly complex structure of ownership for no apparent reason;

(k) whether there is any form of delegated authority in place (e.g.: power of attorney);

(l) whether hold mail arrangements are in place;

(m) whether an account/business relationship is dormant; and

(n) any other information that raises suspicion of the customer being connected to money laundering.

New Customers

Licensees should assess the potential risk inherent in each new client relationship prior to establishing a business relationship. This assessment should take account of whether and to what extent a customer may expose the licensee to risk, and of the product or facility to be used by the customer. Based on this assessment, the licensee should decide whether or not to establish a facility for the customer concerned or to continue with it.

Existing Customers

Licensees are required to risk rate all client relationships including those in existence prior to 29th December 2000 ("existing customers"). Licensees should review the KYC documentation in relation to their existing customers to ensure compliance with the FTRA, as amended, the FTRR, as amended, and the licensee's internal KYC requirements. All risk ratings should be documented.

VIII. VERIFICATION REQUIREMENTS

In February 2003, the Basel Committee on Banking Supervision issued a general guide to good practice for account opening and customer identification. The Basel Committee's guidance is based on the principles of the Basel Committee's paper on Customer Due Diligence for Banks. The general guidance focuses on some of the mechanisms that banks can use in developing effective customer identification policies and procedures. Licensees may access the Basel Committee's General Guidance on Account Opening and Customer Identification on the website of the Bank for International Settlements as follows: www.bis.org.

When should customer identity be verified?

The FTRA, as amended, provides that:

(a) financial institutions are required to verify the identity of customers having facilities established prior to 29th December 2000;

(b) financial institutions should verify the identity of new customers before permitting such customers to become facility holders;

(c) financial institutions must verify customer identity whenever the amount of cash involved in an occasional transaction exceeds $15,000. The identity of the person who conducts the transaction should be verified before the transaction is conducted;

(d) financial institutions must verify customer identity whenever the amount of cash involved in an occasional transaction exceeds $15,000 and it appears to a licensee that the person conducting the transaction is doing so on behalf of any other person or persons. In these circumstances the identities of the third parties must be verified before the transaction is conducted; and

(e) financial institutions must verify customer identity whenever it appears that two or more (occasional) transactions are or have been deliberately structured to avoid lawful verification procedures in respect of the person(s) conducting the transaction(s) and the aggregate amount of cash involved in the transaction(s) exceed $15,000. Verification should be conducted as soon as practicable after the licensee becomes aware of the foregoing circumstances.

The identity of third parties should be verified before transactions are conducted, or as soon as practicable after licensees become aware of any of the relevant circumstances referred to above.

In determining what documentation is necessary to verify the identity of any customer, whether individual, corporate or otherwise, licensees should have regard to the risk category of the particular customer whose identity is to be verified, and to the requirements of these Interim Guidelines.

When is further verification of identity necessary?

Where a customer's identity has been verified, no further verification is required unless-

(a) during the course of the business relationship the financial institution has reason to doubt the identity of the customer;

(b) a licensee knows, suspects or has reasonable grounds to suspect that a customer is conducting or proposes to conduct a transaction which

- involves the proceeds of criminal conduct as defined in the Proceeds of Crime Act, 2000; or
- is an attempt to avoid the enforcement of the Proceeds of Crime Act, 2000.

Verification should take place as soon as practicable after the licensee has the relevant knowledge or suspicion.

(c) there is a material change in the way a facility is operated.

Where licensees are required to verify a client's identity in any of the circumstances set out at (a), (b) or (c) above, the licensee should as part of the re-verification process, check its records on the client concerned to ensure that the documentation on file is current and that it adequately verifies the client's identity.

Licensees may wish, as part of their own internal anti-money laundering and know your customer policies, to re-verify a customer's identity on the occurrence of any of the following "trigger events":

(a) a significant transaction (relative to a relationship);

(b) a material change in the operation of a business relationship;

(c) a transaction which is out of keeping with previous activity;

(d) a new product or account being established within an existing relationship;

(e) a change in an existing relationship which increases a risk profile (as above);

(f) the early redemption of a fixed term product;

(g) the assignment or transfer of ownership of any product;

(h) a non-regular “top-up” of an existing insurance product;

(i) the addition of or a change to a principal in any relationship; and

(j) the roll-over of any fixed term product (taking into account the length of the roll-over period).

The above list should not be considered exhaustive.

****