[BSP CIRCULAR NO. 436, June 18, 2004]

POLICY GUIDELINE REQUIRING BANKS TO ADOPT THE FOLLOWING MINIMUM PRESCRIBED GUIDELINES THAT CONTAIN THE SALIENT AND RELEVANT POLICIES AND PROCEDURES RELATED TO CORRESPONDENT BANKING TRANSACTIONS AND TO ELECTRONIC FUND TRANSFERS

The Monetary Board, in its Resolution No. 807 dated June 3, 2004, approved the issuance of a policy guideline requiring banks to adopt the following minimum prescribed guidelines that contain the salient and relevant policies and procedures related to correspondent banking transactions and to electronic fund transfers found in the attached annexes:

1. Minimum Guidelines for Fund Transfers (Annex "A")

2. Minimum Guidelines for Correspondent Banking Account Opening and Customer Identification (Annex "B")

These prescribed minimum guidelines should be incorporated as part of the standard operating procedures manual and wider anti-money laundering program which must be adhered to at all times. Enhancements may be introduced to these minimum guidelines to suit the particular institution's risk profile but taking into consideration the minimum requirements prescribed under existing anti-money laundering rules and regulations of the BSP, particularly in the area of "Know Your Customer/Customer Due Diligence".

This Circular shall take effect fifteen (15) days following its publication either in the Official Gazette or in a newspaper of general circulation.

Adopted: 18 June 2004

(SGD.) ARMANDO L. SURATOS
Officer-in-Charge

ANNEX "A"

Minimum Guidelines for Fund Transfers

1. **Nature of Fund Transfers**

Funds transfers are remittances of funds from one bank to another, either locally or

internationally, in local or foreign currencies. It is used for moving the proceeds of loans, reimbursing letters of credit, payment of collections, foreign exchange transactions, etc. This may also include the movement of money between customers or between accounts of the same customer, or from a customer to a third party who is not a customer of the Bank. Transfers can be effected by teletransmission, draft, manager's check, or certified check depending on the request of the applicant. The term also includes Automated Clearing House transfers, transfers made at automated teller machines, and point-of-sale terminals.

2. **Responsibility and Oversight**

a. The financial institutions should be governed by a Manually Initiated Funds Transfers (MIFT) Policies and Procedures for funds transfer requests that are manually initiated (via fax, telephone, messenger, electronic mail, file transfers, and other similar manual origination means) externally from clients or internally from within the banking group/entities.

b. The policies and procedures should specify personnel that will be responsible for ensuring compliance with the guidelines on funds transfers transactions.

c. The policies and procedures shall also provide for independent review by appropriate personnel to monitor and ensure continued compliance with the institution's policies, procedures and guidelines on funds transfers.

d. The financial institution shall allow wire transfer electronically (internet transfer) only upon its prior approval.

3. **Risk-Based Due Diligence**

a. The Bank should maintain a policies and procedures manual for funds transfers that are reasonably designed to prevent the financial institution from being used to facilitate money laundering and the financing of terrorist activities. At a minimum, the manual must incorporate policies, procedures and internal controls to:

- Verify customer information (KYC)
- Verify transactions that show indicators of suspicious transactions, particularly those instances stated under Rule 3.b.1 of the Revised Implementing Rules and Regulations (R.A No. 9160, as amended by R.A. No. 9194):
- File reports (including covered transactions/suspicious transactions reports);
- Respond to regulators/law enforcement requests;
- Provide education and/or training of personnel
- Provide security procedures.

b. The Bank should not accept funds transfer instruction from and/or pay-out transfers to non-customers, unless in cases where the initiating party is an authenticated primary customer of a sending group or unit of the Bank.

c. If the fund sender/remitter is not a bank or coming from non-FATF member or

non-compliant countries on AML, the receiving bank must do the due diligence on the beneficiary of the fund.

d. Whenever possible, manually initiated funds transfer instructions should not be the primary delivery method. Every effort should be made to provide the client with an electronic banking solution.

4. **Validation**

a. for written and faxed transaction initiations

The term "validation" applies to various methods used by both sending and receiving parties to verify the identity of the sender of a message. Some validation methods also verify elements in the message including but not limited to amount, value date and currency. Validation must be performed by all Bank units. Some specific validation methods are:

Test Key : An algorithmic computation method using a fixed set of factors known only to the sender and receiver, used to verify the sender and, in some cases, other elements of the message.

Authentication: A cryptographic process used to verify the sender and, in some cases, the full text of a message.

Signature Verification: A matching of signature or other representation from a source document request to a document presigned by a Bank customer and held on file by the Bank, or other documents held by the customer (e.g. Bank approved acceptable identification), used to verify the sender.

Telephone Callback: A procedure used to verify the authenticity of a message received by telephone. The Bank places a return phone call to the customer using a pre-determined telephone number on file within the Bank.

- Validation Procedures

i. Prior to the Bank accepting from a customer a manually initiated funds transfer request, the customer must execute and sign an agreement which preferably is part of the account opening documentation, wherein are outlined the manual instruction procedures with related security procedures including customer agreement to accept responsibility for fraudulent or erroneous instructions provided the Bank has complied with the stated security procedures.

ii. It is mandatory that written MIFT instructions are signature verified. In addition, one of the following primary security procedures must be applied: a recorded callback to the customer to confirm the transaction instructions, or testword arrangement/verification. The callback or testword requirement may be substituted by any of the following validity checks: use of a controlled PIN or other pre-established code; sequential

numbering control of messages; pre-established verifiable forms; same as prior transmissions; standing/pre-defined instructions; or value for value transactions.

iii. It is mandatory that faxed MIFT instructions are signature verified and the Fax machine be located in a secured environment with limited and controlled staff access which permits visual monitoring. If monitoring is not possible, the equipment must be secured or programmed to receive messages into a password protected memory.

Faxed MIFT transactions below a certain threshold (approved by the President/Country Manager (for branches of foreign banks) or Business Risk Manager) may be processed with the mandatory procedure described above and an enhanced security procedure such as (a) a recorded callback to the customer to confirm the transaction instructions and/or (b) testword arrangement/verification, and/or (c) utilization of secured forms that incorporate verifiable security procedures such as watermarks or codes, and/or (d) transmission encryption.

iv. Telephone callback numbers and contacts must be securely controlled. The confirmation callback is to be recorded and made to the signatory/(ies) of the customer's individual account(s). For commercial and company accounts the callback will be made to the signatory(ies) of the account or, if so authorized, another person designated by the customer in the MIFT agreement. The party called is to be documented on the instructions. The callback must be made by someone other than a) the person receiving the original instructions and b) effecting the signature verification.

b. Over-the-counter initiated transactions

Over-the-counter initiated funds transfers by the customers themselves require positive identification of the customer and verification of his/her signature. For transactions over a threshold set by the President/Country Manager (for branches of foreign banks) or Business Risk Manager these transactions shall also require a recorded telephone callback confirmation or another appropriate additional security procedure.

5. **Exception Processing**

On rare occasions, exceptions processing may be necessary. When an established control standard temporarily cannot be met, a senior officer preferably Vice President or above, designated in writing by the President/Country Manager (for branches of foreign banks) may approve an exception processing standard because of unique business circumstances. The reason for creating the exception must be clearly documented including the identification of the applied compensating controls.

6. **Control and Administration Policies for Incoming fund/wire transfers**

This section deals with teletransmission payment orders received from Head office, branches and banks requesting payment or credit to be made to a specified

beneficiary.

a. Cash payments to beneficiaries should only be made against proper receipt and identification.

b. Payment orders with incomplete or insufficient details should be referred immediately to the remitter Bank for clarification. If no response is received within a reasonable time, the matter should be referred to the Compliance or Operations Officer or his/her designated officer for appropriate action as to whether to further investigate or return funds.

7. Integration with Anti-Money Laundering Program

These guidelines shall form part of the institution's wider anti-money laundering program.

Annex "B"

Minimum Guidelines for Correspondent Banking
Account Opening and Customer Identification

1. *Nature of Correspondent Banking Activities*

Correspondent Banking refers to activities of a bank having direct connection or friendly service relations with another bank.

2. *Responsibility and Oversight*

Financial institutions should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures:

a. Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to money laundering or terrorist financing investigation or regulatory action.

b. Assess the respondent institution's anti-money laundering and terrorist financing controls.

c. Obtain approval from senior management before establishing new correspondent relationships.

d. Document the respective responsibilities of each institution.

e. With respect to "payable-through accounts" be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access accounts of the correspondent and that it is able to