



BANK OF MAURITIUS

Guidelines for banks licensed to carry on private banking business

**February 2017
Revised July 2017**

TABLE OF CONTENTS

INTRODUCTION	1
PURPOSE	1
AUTHORITY	1
SCOPE OF APPLICATION	1
EFFECTIVE DATE	1
INTERPRETATION	1
1. CONDITIONS APPLICABLE TO PRIVATE BANKING ACTIVITIES.....	2
2. GENERAL MATTERS.....	2
3. BOARD AND SENIOR MANAGEMENT OVERSIGHT	3
3.1 <i>Role of the board of directors</i>	3
3.2 <i>AML / CFT compliance: Role of senior management</i>	3
4. POLICIES AND PROCEDURES.....	4
5. RISK MEASUREMENT, MONITORING AND MANAGEMENT REPORTING SYSTEM	4
6. RISK MITIGATION AND CUSTOMER RISK ASSESSMENT	5
7. INTERNAL CONTROLS	5
7.1 <i>Internal control environment</i>	5
7.2 <i>Conduct of staff</i>	5
7.3 <i>Account and transaction monitoring</i>	5
7.4 <i>Hold mail</i>	6
7.5 <i>Inactive and dormant accounts</i>	7
7.6 <i>Customer account statements</i>	7
7.7 <i>Voice logging</i>	7
7.8 <i>Whistleblowing/reporting of suspicious cases</i>	7
8. COMPLIANCE	8
9. INTERNAL AUDIT	8
10. SEGREGATION OF DUTIES, COMPLIANCE AND AUDIT	8

Introduction

Section 7(5) of the Banking Act 2004 provides that a bank may be permitted to carry on private banking business in Mauritius.

Private banking business is defined in the Banking Act 2004 as “the business of offering banking and financial services and products to high-net-worth customers including, but not limited to, an all-inclusive money-management relationship”.

Further, section 7(7D) of the Banking Act 2004 states that ‘A bank which has been granted a banking licence to carry on exclusively private banking business by the central bank may be exempted from such provisions of the Act as the central bank may determine and be subject to such terms and conditions and guidelines as the central bank may determine’.

Purpose

These guidelines give effect to the above-mentioned provisions of the Banking Act 2004 and set out the regulatory and supervisory framework that would be applicable to banks licensed to carry on private banking business.

Authority

These guidelines are issued under the authority of section 50 of the Bank of Mauritius Act 2004 and sections 7(7D) and 100 of the Banking Act 2004.

Scope of application

These guidelines shall apply to all banks licensed under section 7(5) of the Banking Act 2004 to carry on exclusively private banking business and also to other banks offering private banking services as part of their banking services.

Effective date

These guidelines shall come into effect on 21 July 2017.

Interpretation

“Act” means the Banking Act 2004.

“Bank” means the Bank of Mauritius established under the Bank of Mauritius Act 2004;

“discretionary wealth management” means an investment management service whereby the investment manager manages a specific portfolio for and on behalf of the client and the investment manager has full discretion over the investment decisions of the portfolio in accordance with the terms and conditions that may exist between the bank and the clients”

“non-discretionary wealth management” means investments for and on behalf of the client, duly approved by him.

“private banking business” has the same meaning as in the Banking Act 2004.

“related party” has the same meaning as in the Banking Act 2004.

“significant interest” has the same meaning as in the Banking Act 2004.

1. Conditions applicable to private banking activities

- (i) A bank carrying on private banking business shall, depending on the business model proposed and the extent to which it is engaged in banking activities, be exempted from such provisions of the Act and such guidelines, guidance notes, instructions issued by the Bank, as the Bank may determine.
- (ii) A person who intends to hold a significant interest in a private bank shall:
 - (a) seek the prior written approval of the Bank to hold such an interest in the bank; and
 - (b) undertake in writing to the central bank not to influence or impede the prudent management and functioning of the bank in accordance with sound banking practice.
- (iii) The central bank may proceed against a private bank in terms of section 11 of the Act for breach of the provisions mentioned under (ii) above.
- (iv) A bank carrying on private banking business shall, on a yearly basis, notify the Bank of the percentage of the share capital or voting rights of each shareholder.

2. General matters

- (i) A bank carrying on private banking business shall:
 - (a) ensure that its staff act with professionalism, diligence and that its activities are guided by ethical values, prudence and integrity;
 - (b) adopt a Code of Ethics to be observed by all of its staff so as to promote fair and ethical actions that are fundamental to good business practices;
 - (c) in the event of a Discretionary Portfolio Management Mandate ensure that, prior to investment, its clients clearly authorize the bank to invest in entities related to the bank. The bank shall report to its clients all their investments made with related parties on a yearly basis or at such higher frequency as may be requested by the clients; and
 - (d) in the event of a Non-Discretionary Portfolio Management Mandate, seek the prior approval of its clients for all investments. A report shall be sent to its clients on all their investments on a yearly basis or at such higher frequency as may be requested by the clients.
- (ii) The purpose of all private banking relationships shall be clearly recorded. The bank shall perform its due diligence by adequately and reasonably ascertaining and documenting that the funds of its private banking customers have been derived from legitimate sources.

- (iii) The audit, risk management and compliance functions of the bank shall be independent from line management.

3. Board and senior management oversight

- (i) The board and senior management shall create an appropriate corporate culture based on sound risk management and appropriate control environment. Senior management shall exercise proper oversight for ensuring compliance with corporate policies and procedures.
- (ii) Policies and procedures shall be duly approved by the board to control business operation, with clear accountability established for the risk management and control functions.
- (iii) Regular meetings shall be held to oversee the operation/business as well as compliance with corporate policies and procedures.
- (iv) Complete, accurate and timely Management Information System (MIS) reports shall be made available to the board for review of business activities, customer services, compliance and exceptions.

3.1 *Role of the board of directors*

- (i) The board is responsible for approving policies and procedures for the anti-money laundering and combating the financing of terrorism (AML/CFT) program and for monitoring its effectiveness on an ongoing basis. Its oversight responsibilities shall be aligned with those in the *Guideline on Corporate Governance* and *Guidance Notes on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institutions* issued by the Bank. Also, it is important that the board's accountability in this area is properly documented.
- (ii) The board's principal responsibilities in this program will include:
 - (a) approval of the AML/CFT framework, including key policies;
 - (b) receiving regular reports on the effectiveness of the AML/CFT administration; and
 - (c) obliging external auditors to report on the effectiveness of AML/CFT program.

3.2 *AML/CFT compliance: Role of senior management*

In respect of compliance with AML/CFT, senior management shall have, among other aspects, responsibility and accountability for directing the day-to-day management of AML/CFT program, and ensure that it is effective in mitigating money laundering and terrorist financing risks. More specifically, senior management must ensure that:

- (i) the officer designated to monitor and ensure AML/CFT compliance is appropriately qualified and has a documented authority and accountability for the design and execution of the program;

- (ii) the officer so designated does not report to any revenue-generating business unit in order to avoid potential conflict of interest;
- (iii) the officer is given adequate data management systems to administer effectively the AML/CFT program and to provide objective opinions or advice to senior management and the board;
- (iv) the officer is made responsible for analysing and identifying inherent risks in the bank's operations and how to protect against such risks; and
- (v) recommendations of the responsible officer are acted upon in a timely manner.

4. Policies and procedures

Banks carrying on private banking business shall have in place proper "Know Your Customer" policies and procedures, consistent with the *Guidance Notes on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institutions* issued by the Bank. They shall obtain identification and basic information on their customers that describe their source of wealth and lines of business. They shall request references, handle referrals, and identify suspicious transactions. They shall have in place adequate written policies and procedures that address, amongst others, money laundering-related issues.

Policies and procedures governing the private banking business shall, inter-alia, cover the following areas:

- 1) Background, integrity, fitness and propriety checks on Relationship Managers (RMs);
- 2) Account and transaction monitoring;
- 3) Responsibilities of RMs;
- 4) Staff code of conduct;
- 5) Compliance;
- 6) Customer transaction processing and order processing;
- 7) Hold mail service;
- 8) Inactive and dormant account handling;
- 9) Complaints handling; and
- 10) Fraud/suspicious transaction detection and reporting.

These policies and procedures shall be reviewed and updated annually. There shall also be established processes and procedures for ensuring staff's awareness of and compliance with these policies and procedures.

5. Risk measurement, monitoring and management reporting system

There shall be procedures in place for reporting of frauds to senior management. Complete, accurate and timely MIS reports (e.g. performance by individual RMs, exceptions on operational losses and transaction irregularities, customer complaints, inactive and dormant accounts) shall be prepared for review by authorised officers or line managers.

Banks carrying on private banking business shall obtain and keep records of all due diligence documents for all their clients. Proper follow-up shall be carried out to

corroborate information provided by a customer, with retention of information on the ultimate beneficial owner.

6. Risk Mitigation and Customer Risk Assessment

Banks carrying on private banking business shall assess the risks posed by their private banking activities on the basis of the scope of operations and the complexity of the banks' customer relationships. A risk profile for each customer shall be established for ongoing monitoring of account activities.

The following factors shall, inter-alia, be considered when identifying risk characteristics of private banking customers:

- (i) The source of the customer's wealth and the nature of his business activities;
- (ii) The size, purpose, types of accounts, products and services involved in the private banking relationship with the customer;
- (iii) The nature and duration of the bank's relationship with the customer;
- (iv) The corporate structure of the customer;
- (v) The geographic location and jurisdiction of the customer's domicile and business; and
- (vi) Any public information known or available on the customer.

7. Internal controls

7.1 *Internal control environment*

Responsibilities shall be well-defined with duties properly segregated among the front, middle and back office staff. In particular, there shall be dual control on the approval of new relationships, and new account documentation processing and account activation shall be performed by departments independent from the sales team. RMs shall not single-handedly be responsible for the execution of customer instructions without involvement of other control units for checks and controls. Customer complaints, account statements, hold mail services and inactive and dormant accounts shall not be handled by RMs only.

7.2 *Conduct of staff*

- (i) Staff account dealing policies shall be implemented and enforced to prevent violation of conduct and conflict of interest that could arise therefrom. There shall be rules governing staff dealing activities and these activities shall be subject to management approval and regular monitoring. In-house accounts of staff relatives shall also be subject to regular monitoring.
- (ii) Mandatory consecutive leave policy for staff shall be enforced.

7.3 *Account and transaction monitoring*

- (i) The bank's Customer Due Diligence (CDD) procedures shall allow for the collection of sufficient information to develop a profile for each customer to be used for analysing client transactions. An effective CDD and customer onboarding policy shall cater for high risk accounts, including politically-exposed persons (PEPs), for which there shall be more extensive due diligence and closer

and more proactive monitoring. Internal systems shall be developed for monitoring and identifying transactions that are inconsistent with the profile for a customer, which may thus constitute suspicious activity. All internal suspicious transaction reports shall be promptly made to the Money Laundering Reporting Officer.

- (ii) For high-risk/high-value transactions, banks shall have procedures to confirm these transactions with the customers such as phone call-back by an independent person of the back office and by SMS to the customers.
- (iii) Consideration shall be given to periodic rotation of RMs in the domestic private banking business.
- (iv) Audit trails of communication with clients (e.g. call reports) shall be maintained.
- (v) Banks carrying on private banking business shall have full knowledge of originator details for incoming wire transfers, and ensure that similar information is provided for all outgoing wire transfers.
- (vi) Formal review of customer relationships shall be conducted on a regular basis depending on the risk profile of the customers to ensure that customer information remains up to date.

7.4 *Hold mail*

- (i) Customers shall receive regular bank statements on their cash and investment transactions. Some institutions provide hold mail service to their customers because, for instance, the customers require a confidential relationship. This may be open to abuse such as concealment of unauthorised transactions as customers may not be able to verify the accuracy of their cash and investment transactions in a timely manner. In general, banks carrying on private banking business shall not allow hold mail service. If the customer insists, and hold mail service is provided, there shall be control measures in place to mitigate the risks, e.g. tighten the control on such applications, separate custody of the customer's mail from the RM, reconfirming with customers who have requested for this service and keeping a copy of the customer's written confirmation in file. In any case, there shall be a limit on the period (not more than 6 months) within which the customer must collect mails held by the bank from a person independent of the RM, such as the back office.
- (ii) Procedures shall be established to verify customer authorisation for releasing hold mail. If RMs were allowed to release mail on hold to customers directly, there shall be control measures, e.g. customers' signatures shall be obtained to acknowledge receipt of the mail and the signatures shall be verified by an independent unit.

7.5 *Inactive and dormant accounts*

There shall be a clear policy to classify accounts as inactive/dormant. These accounts shall be subject to monitoring by units independent of RMs. Sufficient control procedures shall be formulated for reactivating such accounts and the customer shall be informed of such procedures.

7.6 *Customer account statements*

There shall be proper segregation of duties in generating and delivering account statements, handling customer request for change of correspondence address and collecting and following up with returned mail/advice/statements.

7.7 *Voice logging*

All the telephone lines of RMs/assistants shall be tape-recorded. Procedures shall be established to control the tape-recording system and safe-keeping of tapes, as well as periodic tape listening on a sample basis.

7.8 *Whistleblowing/reporting of suspicious cases*

- (i) Banks carrying on private banking business shall have policies and procedures in place for the reporting and escalation of suspicious cases (which may arise from customer complaints, MIS reports, whistleblowing by another staff, etc.) which may have serious implications and/or entail possible criminal elements.

These policies and procedures shall, at a minimum, cover the following:

- (a) the opportunity to raise concerns to an independent unit which is outside the line management structure, such as compliance or internal audit;
- (b) respect for the confidentiality of employees who raise concerns about irregular activities, unacceptable/unethical practices or misconduct at any level;
- (c) an assurance that, where a disclosure has been made, the institution will take all reasonable steps to protect informers and ensure that no person under its control engages in victimisation/retaliation or harassment;
- (d) procedures for escalation of suspicious cases to senior management for appropriate action/investigation;
- (e) recommendation for appropriate disciplinary action for making false and malicious allegations;
- (f) procedures for reporting to the board of directors; and
- (g) making whistleblowing procedures accessible to staff.

- (ii) Whenever there is a suspected case involving possible criminal elements, banks are expected to report the incident to the Police in a timely manner. The Bank shall be notified of the fraud within a period of seven working days as from the date the fraud gets detected.

8. Compliance

Regular review shall be performed on compliance with the established operational control policies and procedures. Vulnerable customers, e.g. the old-aged, customers residing abroad, users of hold mail service, etc. shall be subject to more frequent checking of account activities to ward off risks of frauds.

9. Internal audit

Regular internal audit shall be conducted, with the implementation of the audit recommendations properly followed-up.

10. Segregation of duties, compliance and audit

Banks carrying on private banking business shall have in place an effective oversight system by board committees to ensure that:

- (i) proper segregation of duties is maintained at all times;
- (ii) there is no unauthorised waiver of documentation requirement;
- (iii) suspicious transactions are properly identified and reported; and
- (iv) compliance and audit programs are in place for ensuring the integrity of the risk management and control environment.

Bank of Mauritius
21 July 2017