LESOTHO
Government Gazette

Vol. 60 Friday – 31st July, 2015 No. 50

CONTENTS

Published by the Authority of His Majesty the King
Price: M13.00

LEGAL NOTICE NO. 77 OF 2015

Financial Institutions (Anti-Money Laundering and Combating of Financing of Terrorism) Regulations, 2015

PART I - PRELIMINARY

PART II - ANTI MONEY LAUNDERING AND COMBATING OF FINANCING OF TERRORISM MEASURES

LEGAL NOTICE NO. 77 OF 2015

Financial Institutions (Anti-Money Laundering and Combating of Financing of Terrorism) Regulations, 2015

In exercise of the powers conferred upon the Commissioner of Financial Institutions by section 71 of the Financial Institutions Act, 2012, the Commissioner makes the following regulations:

PART I - PRELIMINARY

Citation and commencement

1. These regulations may be cited as the Financial Institutions (Anti-Money Laundering and Combating of Financing of Terrorism) Regulations, 2015 and shall come into operation on the date of publication in the Gazette.

Interpretation

2. (1) In these regulations, unless the context otherwise requires -

"Board of Directors" means the Board of Directors of a bank;

"bank" has the same meaning as in the Financial Institutions Act, 2012

"Commissioner" has the same meaning as in the Financial Institutions Act, 2012;

"correspondent banking" means provision of banking services by one bank called 'the correspondent bank', to another bank referred to as 'the respondent bank';

"money laundering" has the same meaning as assigned to it under the Money Laundering and Proceeds of Crime Act, 2008;

"politically exposed person" has the same meaning as assigned to it under Money Laundering and Proceeds of Crime Act, 2008;

"staff" means an employee of a bank;

"shell bank" means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision;

"Unit" means the Financial Intelligence Unit established under the Money Laundering and Proceeds of Crime Act, 2008.

(2) Other words used have the same meaning assigned to them in the Financial Institutions Act, 2012 or the Money Laundering and Proceeds of Crime Act, 2008.

Objective

3. The objective of these regulations is to prescribe safeguards against the abuse of the financial services in the banking sector.

Application

4. These regulations apply to a bank licensed in Lesotho.

PART II - ANTI MONEY LAUNDERING AND COMBATING OF FINANCING OF TERRORISM MEASURES

Anti money laundering and combating of financing of terrorism measures

5. (1) A bank shall have and implement, at the minimum, the following policies together with the necessary processes:

(a) internal control policies to guard against criminal activities;

(b) operational risk management policies;

(c) a policy on:

(i) ethical and professional conduct of staff;

(ii) reporting of incidents of fraud and suspicious activities;

(iii) customer due diligence;

(iv) correspondent banking;

(v) internal and external auditors; and

(vi) record keeping.

Internal controls relating to anti-money laundering and combating of financing of terrorism

6. (1) In addition to the existing regulatory framework on internal controls, a bank shall adhere to the internal control requirements specified in this regulation.

(2) The Board of Directors shall ensure that a system of internal controls for anti-money laundering and combating of financial terrorism purposes is established and maintained.

(3) A bank's internal control framework shall provide and set up an organizational structure, which shall provide accounting policies and processes, checks and balances, and framework intended to safeguard assets and investments to ensure that the bank is not used for money laundering and terrorist financing.

(4) In relation to organizational structure, the bank's framework should have clear definitions of duties and responsibilities, including clear delegation of authority, decision making powers, policies and processes, separation of critical functions such as business origination, payments, reconciliation, accounting, risk management, audit and compliance.

(5) A bank's accounting policies and processes shall include but not be limited to reconciliation of accounts, control lists and management information systems.

(6) A bank shall have -

(a) a policy that encourages checks and balances to ensure cross checking of major decisions by more than one person to ensure that the bank is not used for criminal

activities.

(b) processes for safe guarding assets and investments including physical and electronic infrastructure control to ensure that assets are not used for criminal activities.

(7) A bank shall ensure that investments are not made in entities or territories that are not regulated against anti-money laundering and combating of financial terrorism and that the entity communication systems are not used for money laundering and terrorist financing.

Operational risk management to curb money laundering and financing terrorism

7. (1) A bank shall have appropriate operational risk management strategies, policies and processes that identify, assess, evaluate, monitor, report and control or mitigate operational risk that may give rise to money laundering and financing of terrorism.

(2) A bank's operational risk management strategies, policies and processes against money laundering and terrorist financing shall -

(a) be consistent with the bank's risk profile, systemic importance, risk appetite and capital strength;

(b) take into account market macro-economic conditions and address major aspects of operational risk prevalent in the business of the bank on a bank-wide basis, including periods when operational risk may increase;

(c) be approved and annually reviewed by the Board of Directors.

(3) The Board of Directors shall ensure that the operational risk management strategies, policies and processes against money laundering and terrorist financing are implemented effectively and are fully integrated into the bank's overall risk management process.

(4) A bank shall have a comprehensive disaster recovery and business continuity plan that shall enable the bank to resume operation in the event

of severe business disruptions.

Management Information System

8. (1) A bank shall put in place -

(a) management information systems policies and processes to identify assess, monitor and manage technology risks to prevent money laundering and terrorist financing;

(b) management information systems infrastructure to meet its current and projected business requirements under normal circumstances and periods of stress, which ensures data and system integrity, security and availability and supports integrated and comprehensive risk management including management of risk related to money laundering and terrorist financing.

(2) A bank shall ensure that it has appropriate and effective management information systems that:

(a) monitor operational risk including money laundering and terrorist financing risk;

(b) compile and analyse operational risk data referred to in paragraph (a); and

(c) facilitate appropriate reporting at the Board of Directors, senior management and business line levels that support proactive management of operational risk.

(3) A bank shall have policies and processes that assess, manage and monitor outsourced management information systems and other activities.

(4) At the minimum, the outsourcing risk management programme shall cover:

(a) conducting of due diligence in selecting potential service providers;

(b) structuring the outsourcing arrangement;

(c) managing and monitoring the risks associated with the outsourcing arrangement;

(d) ensuring regulatory control environment; and

(e) establishing viable contingency planning.

(5) A financial institution's outsourcing of information technology and other functions policies and processes shall require the bank to have comprehensive contracts or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank.

Ethical and professional standards for staff

9. (1) A bank shall have in place -

(a) policies and processes that promote high ethical and professional standards, specific to the organization and in line with those set by professional bodies, to prevent the bank from being used, intentionally, for criminal activities;

(b) screening policies and processes to ensure high ethical and professional standards.

Reporting of suspicious activities, incidents of fraud and large transactions

10. (1) A bank shall report -

(a) incident of fraud to the Commissioner;

(b) suspicious transactions and large transactions to the Unit in the format prescribed in the Money Laundering (Accountable Institutions) Guidelines, 2013 developed pursuant to section 15(2)(e) of the Money Laundering and Proceeds of Crime Act, 2008.

(2) If a bank considers that a suspicious activity is material to the

safey, soundness or reputation of the bank, the bank shall, in addition to reporting to the Financial Intelligence Unit, report the suspicious activity to the Commissioner.

(3) A staff member of a bank who reports a suspicious transaction or incident of fraud in good faith, either internally or directly to the Unit, the Commissioner, the law enforcement agency or another relevant authority shall not be held liable.

(4) A bank shall have and follow clear policies and processes for staff to report any suspected incident related to money laundering and terrorist financing to either local management or the relevant dedicated officer or to both.

(5) A bank shall have and utilize adequate management information systems to provide the Board of Directors, management, compliance and dedicated officers with timely and appropriate information to abuse of the bank's financial services of the bank.

Customer Due Diligence

11. (1) In addition to the Financial Institutions (Know Your Customer) Guidelines, 2007 a bank shall comply with the Money Laundering (Accountable Institutions) Guidelines, 2013 with regard to customer due diligence.

(2) A bankshall establish well documented customer due diligence policies and processes that are communicated to all relevant staff and integrated in the bank's overall risk management system.

(3) A bank's customer due diligence policies and processes shall comprise appropriate steps to identify, assess, monitor, manage and mitigate risks of money laundering and the financing of terrorism with respect to customers, countries and regions, as well as to products, services, transactions and delivery channels on an ongoing basis.

(4) A bank's customer due diligence program shall have the following essential elements:

(a) customer acceptance policy that identifies business relationships that the bank shall not accept based on identified risks;

(b) a customer identification, verification and due diligence programme on an ongoing basis which encompasses verification of beneficial ownership, understanding the purposes and nature of the business relationship, and risk-based reviews to ensure that records are updated and relevant;

(c) policies and processes to monitor and recognize unusual or potentially suspicious transactions;

(d) enhanced due diligence on high-risk accounts including escalation to the bank's senior management level decisions on entering into business relationships with high risk accounts or maintaining such relationships when an existing relationship becomes high risk;

(e) enhanced due diligence on politically exposed persons, including escalation to the bank's senior management level of decisions on entering into business relationships with politically exposed persons; and

(f) rules on records to be kept on customer due diligence and individual transactions and their retention period which shall not be less than 10 years.

Correspondent banking

12. (1) A bank shall have and implement customer due diligence policies and processes that are specific to its correspondent banking and the policies and processes shall include:

(a) gathering sufficient information about their respondent banks to appreciate the nature of their business and customer base, and how they are supervised;

(b) prohibit or discontinue correspondent relationships with a bank that does not have adequate controls against criminal activities or is not effectively supervised by the relevant authorities;

(c) a requirement by a bank to satisfy itself that respondent financial institutions in a foreign jurisdiction do not permit their account to be used by shell banks;

(d) prohibition of banks to enter into or continue correspondent banking relationships with shell banks;

(e) a requirement for the bank to provide evidence that their accounts with respondent banks are not used by shell banks.

(2) A bank shall also adhere to the Financial Institutions (Know Your Customer) Guidelines, 2007 regarding correspondent banking.

Internal and External Audit

13. (1) A bank shall -

(a) have a policy, approved by the Board of Directors, on the appointment of internal and external auditors;

(b) appoint internal and external auditors, to whose reports the Commissioner shall have unrestricted access, to independently evaluate the relavant risk management policies, processes and controls.

Compliance officers

14. (1) A bank shall -

(a) establish policies and processes to designate compliance officers or money laundering officers;

(b) appoint compliance or money laundering officers to whom potential abuses of the bank's financial services, including suspicious transactions, are reported.

Staff training

15. A bank shall undertake an ongoing training programme for its staff on -

(a) anti-money laudering;

(b) combating of financial terrorism;

(c) customer due diligence; and

(d) methods to monitor and detect criminal and suspicious activities.

Record keeping

16. (1) A bank shall -

(a) maintain customer records as prescribed by the Financial Institutions (Know Your Customer) Guidelines, 2007;

(b) maintain customer records for a minimum of 10 years.

On site examination

17. (1) The Commissioner may, from time to time, carry out an examination of a bank without prior notice to assess its compliance with anti-money laudering and financing of terrorism legislation.

(2) A bank shall provide information related to anti-money laudering and financing terrorism to examiners both on site and off site when required to do so.

(3) In carrying out an examination of a bank, the Commissioner may use its own staff or external experts.

(4) A bank shall provide working space for examiners to carry out their examination work.

Supervisory action

18. Where a person contravenes these regulations the Commissioner may pursue remedial measures set out in the Financial Institutions Act, 2012, including:

(a) revocation of a licence;

(b) imposition of penalty on the financial institution or any of its directors, managers, officers or staff.

DR. RETŠELISITSOE MATLANYANE
GOVERNOR OF THE CENTRAL BANK OF LESOTHO

Printed by the Government Printer, P.O. Box 268, Maseru 100 Lesotho