

Lesotho

Money Laundering and Proceeds of Crime Act, 2008

Money Laundering and Proceeds of Crime Regulations, 2019

Legal Notice 29 of 2019

Legislation as at 29 March 2019

FRBR URI: /akn/ls/act/ln/2019/29/eng@2019-03-29

There may have been updates since this file was created.

PDF created on 21 February 2024 at 14:35.

[Check for updates](#)



About this collection

The legislation in this collection, with facilitation from the Office of Parliamentary Counsel of Lesotho, has been reproduced as it was originally printed in Lesotho's Government Gazettes by the Government Printer, with improved formatting and with minor typographical errors corrected. All amendments have been applied directly to the text and annotated. A scan of the original gazette of each piece of legislation (including amendments) is available for reference.

This is a free download from LesLII and is presented in collaboration with the Office of Parliamentary Counsel of Lesotho and the Laws.Africa Legislation Commons, a collection of African legislation that is digitised by Laws.Africa and made available for free.

www.lesotholii.org | info@lesotholii.org

www.laws.africa | info@laws.africa

There is no copyright on the legislative content of this document.

This PDF copy is licensed under a Creative Commons Attribution 4.0 License (CC BY 4.0). Share widely and freely.

Money Laundering and Proceeds of Crime Regulations, 2019

Contents

Part I – Preliminary	1
1. Citation and commencement	1
2. Interpretation	1
Part II – Financial institutions and financial service-providers	3
3. Identification of a client or customer	3
4. Purpose of the business relationship	3
5. Applying risk based approach	4
6. Verification of a client's or customer's identification	4
7. Establishment and termination of a business relationship	5
8. Dealing with a corresponding business relationship	5
9. Reliance on an intermediary or third party	6
10. Higher risk countries	6
11. Establishing and maintaining client's or customer's records	7
12. Internal controls	7
13. Recruitment of employees	7
14. Training of employees	8
15. Audit and supervision	8
16. Inspections	8
17. Sharing of information	8
18. Compliance	9
19. Reporting suspicious transactions	9
20. Wire transfers	11
21. Registration with the Unit	12
Part III – Designated non-financial business and profession (DNFBP) and designated business	13
22. Identification of a client or customer and record keeping	13
23. Measures applicable to DNFBP and designated business	14
Part IV – Non-profit organisation	14
24. Affairs of a non-profit organisation	14
Part V – Financial sanctions related to terrorist financing and financing proliferation	15
25. Financing and supporting terrorist activities	15
26. Establishment of the Anti Terrorism Committee	16
27. Designation and identification of persons and entities	16
28. Freezing order	18
29. Sanctions against terrorist financing	19

30. Prohibition of dealing with funds and other assets	19
31. Freezing of fund and other assets	19
32. Access to frozen assets and other assets	20
33. Delisting of persons and entities and unfreezing of funds and other assets	21
34. Immunity and confidentiality	21
Part V – Miscellaneous provisions	21
35. Demand of communication call data	21
36. International Cooperation	22
37. General penalty	22
Schedule 3 (Regulation 2)	24
Schedule 1 (Regulation 2)	23
Schedule 2 (Regulation 2)	23
Schedule 4 (Regulation 2)	25
Schedule 5 (Regulation 10)	25
Schedule 6 (Regulation 28 (1))	26
Schedule 7 (Regulation 27(4)(e))	26
Schedule 8 (Regulation 27(8))	28
Schedule 9 (Regulation 35 (7))	29

Lesotho

Money Laundering and Proceeds of Crime Act, 2008

Money Laundering and Proceeds of Crime Regulations, 2019

Legal Notice 29 of 2019

Published in Government Gazette 21 on 29 March 2019

Commenced on 29 March 2019

[This is the version of this document from 29 March 2019.]

In the exercise of the powers conferred upon me by the Money Laundering and Proceeds of Crime Act 2008,¹

I,

Dr. Moeketsi Majoro

Minister responsible for finance make the following regulations —

Part I – Preliminary

1. Citation and commencement

These regulations may be cited as the Money Laundering and Proceeds of Crime Regulations, 2019 and shall come into operation on the date of publication in the *Government Gazette*.

2. Interpretation

In these regulations, unless the context indicates otherwise —

"**Act**" means the Money Laundering and Proceeds of Crime Act, 2008;

"**attempted transaction**" means a transaction that a client or customer intended to conduct and took some form of action to do so, and includes entering into negotiations or discussions to conduct the transaction and also includes concrete measures to be taken by an accountable institution or the client or customer;

"**batch transfer**" means a transfer comprised of a number of individual wire transfers that are being sent to the same financial institution or financial service-provider, but may or may not be ultimately intended for different persons;

"**beneficial owner**" means a natural person who ultimately owns or controls a client or customer and the natural person on whose behalf a transaction is being conducted, and includes those persons who exercise ultimate effective control over a legal person or arrangement;

"**beneficiaries**" refer to natural persons, or group of natural persons who receive charitable, humanitarian or other types of assistance through the services of a non-profit organisation;

"**beneficiary**" means a natural or legal person or legal arrangement who —

- (1) is identified by the originator as the receiver of the requested wire transfer;
- (2) in the case of a trust, is entitled to the benefit of a trust arrangement; or
- (3) in the case of a life cover insurance, will be paid the proceeds covered by the policy or contract;

¹

Act [No. 4 of 2008](#)

"beneficiary financial institution or financial service-provider" means a financial institution or financial service-provider which receives the wire transfer from the ordering financial institution or financial service-provider directly or through an intermediary financial institution or financial service-provider and makes funds available to the beneficiary;

"cross-border wire transfer" means any wire transfer where the ordering financial institution and beneficial institution are located in different countries, and includes any chain of wire transfers in which at least one of the financial institutions involved is located in a different country;

"designated person or entity" means an individual, entity, group or undertakings listed in Schedule 1;

"DNFBP" means designated non-financial business and professions including a business and a profession listed in Schedule 2;

"domestic wire transfer" means any wire transfer where the ordering financial institution or financial service-provider and beneficiary financial institution or financial service-provider are located in the same country, and include any chain of wire transfer that takes place entirely within the borders of a single country, even though the system used to transfer the payment message may be located in another country;

"FATF" means the Financial Action Task Force;

"intermediary financial institution" means a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution;

"non-profit organisation" means a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such a charitable, religious, cultural, educational, social or fraternal purposes, or for carrying out of other types of good works;

"ordering financial institution or financial service-provider" means a financial institution or financial service-provider which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator;

"originator" means the holder who allows the wire transfer from his or her account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer;

"payable-through accounts" means correspondent accounts that are used directly by third parties to transact business on their own behalf;

"resolution" means United Nations Security Council resolution made under Chapter VII of the United Nations Charter;

"risk" means money laundering and terrorist financing risk;

"sanction list" means a list of designated persons or entities published in the *Gazette*;

"sector supervisory authority" means an institution established by law including institutions and accreditation institutions or ministries and departments listed in Schedule 3;

"serious offences" include offences listed in Schedule 4 which shall also be referred to as "predicate offences to money laundering";

"straight-through processing" means payment transactions that are conducted electronically without the need for manual intervention;

"third party" means an accountable institution which is supervised or monitored and is subject to the requirements of regulation 9;

"trustee" means a person under whose control assets have been placed by another person, the settlor, for the benefit of a beneficiary or for a specified purpose;

"unique transaction reference number" means a combination of letters, numbers or symbols, determined by the payment service provider, in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer;

"Unit" means the Financial Intelligence Unit established under the Act; and

"wire transfer" means any transaction carried out on behalf of an originator through a financial institution or a person who provides money remittance services by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

Part II – Financial institutions and financial service-providers

3. Identification of a client or customer

- (1) A financial institution or financial service-provider shall identify a client or customer when —
 - (a) establishing a business relationship;
 - (b) carrying out an occasional transaction above the prescribed threshold;
 - (c) carrying out an occasional transaction which is a cross-border or domestic wire transfer, including serial payments and cover payments;
 - (d) there is a suspicion of the commission of a serious offence; or
 - (e) the financial institution or financial service-provider has doubts about the veracity or adequacy of previously obtained client or customer identification data.
- (2) A financial institution or financial service-provider shall identify the client or customer using reliable, independent source documents, data or information.
- (3) A financial institution or financial service-provider shall identify the beneficial owner and ensure that the financial institution or financial service-provider knows who the beneficial owner is, or understands the ownership and control structure of the client or customer where the beneficial owner is a legal person or arrangement.
- (4) Where a client or customer is a legal person or arrangement, a financial institution or financial service-provider shall identify the client or customer and verify its identity through the following information —
 - (a) name, legal form and proof of existence;
 - (b) the powers that regulate and bind the legal person or arrangement, as well as the names of relevant persons having a senior management positions in the legal person or arrangement; and
 - (c) the address of the registered office, if different, a principal place of business.

4. Purpose of the business relationship

A financial institution or financial service-provider shall —

- (a) obtain information on the purpose and intended nature of the business relationship;
- (b) monitor the business relationship and scrutinize the transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's or service-provider's knowledge of the client or customer, their business and risk profile, including, where necessary, the source of funds.

5. Applying risk based approach

- (1) A financial institution or financial service-provider shall determine the need to undertake the requirements in regulations 3,4, and 6 using a risk based approach.
- (2) A financial institution or financial service-provider shall apply risk based approach in order to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.
- (3) In implementing risk based approach, a financial institution or financial service-provider shall have in place processes to identify, assess, monitor, manage and mitigate money laundering and terrorist financing risks.
- (4) Where higher risks are identified, a financial institution or financial service-provider shall apply enhanced measures to mitigate those risks. Equally, where the risks are lower, a financial institution or financial service-provider may apply simplified measures.
- (5) A financial institution or financial service-provider shall not apply simplified measures whenever there is a suspicion of money laundering or terrorist financing.

6. Verification of a client's or customer's identification

- (1) A financial institution or financial service-provider shall verify a client's or customer's identity using reliable and independent source documents, data or information.
- (2) A financial institution or financial service-provider shall take reasonable measures to verify the identity of the beneficial owner.
- (3) The requirements to verify the identity of the client or customer and beneficial owner shall apply when —
 - (a) establishing a business relationship; and
 - (b) conducting a transaction for an occasional client or customer.
- (4) Subject to subregulation (3) and in order not to disturb or interrupt the normal conduct or process of business, a financial institution or financial service-provider may complete verification of the identity of a client or customer and the beneficial owner as soon as practicable after establishing the business relationship.
- (5) Where a client or customer is a legal arrangement, a financial institution or financial service-provider shall take reasonable measures to verify the identity of a beneficial owner through the following information —
 - (a) for trusts, the identity of the settlor, the trustee or trustees, the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust, including through a chain of control or ownership;
 - (b) for beneficiaries of trusts designated by characteristics or class, the identity of the beneficiary at the time of payout or whenever the beneficiary intends to exercise vested rights; or
 - (c) for other types of legal arrangements, the identity of persons in similar or equivalent positions in paragraph (a) above.
- (6) Where a client or customer is a legal person, a financial institution or financial service-provider shall take reasonable measures to verify the identity of a beneficial owner through the following information —
 - (a) the identity of the natural person or persons who ultimately has a controlling ownership interest in a legal person;

- (b) to the extent that there is doubt under paragraph (a) above or where no natural person exerts control through ownership interest, the identity of the natural person or persons exercising control over the legal person or through other means; or
- (c) where no natural person is identified under paragraphs (a) or (b), the identity of relevant natural person or persons holding the position of senior management.

7. Establishment and termination of a business relationship

- (1) A financial institution or financial service-provider shall not open an account or establish a business relationship where the financial institution or financial service-provider —
 - (a) fails to identify a client or customer and beneficial owner;
 - (b) cannot independently verify a client or customer and beneficial owner;
 - (c) cannot establish the ownership or control structure of a client or customer in the case of a legal person; or
 - (d) fails to obtain information on the purpose and intended nature of the business relationship.
- (2) For an existing business relationship, a financial institution or financial service-provider shall terminate the business relationship where the —
 - (a) financial institution or financial service-provider —
 - (i) cannot obtain and verify the client's or customer's additional information on identification data;
 - (ii) fails to obtain additional information on the intended nature and purpose of the business relationship;
 - (iii) fails to obtain information on the source of funds or wealth of the client or customer; or
 - (b) client or customer is involved in money laundering or terrorist financing activities.

8. Dealing with a corresponding business relationship

- (1) A financial institution or financial service-provider shall not enter into or continue with a cross-border correspondent banking relationship or a similar institution or relationship with a shell bank.
- (2) A financial institution or financial service-provider shall satisfy itself that the cross-border correspondent banking relationship or a similar institution or relationship does not permit its accounts from being used by a shell bank.
- (3) A financial institution or financial service-provider shall, during the course of establishing and during the business relationship —
 - (a) gather sufficient information about the corresponding respondent institution or service-provider to understand fully the nature of the corresponding respondent institution's or service-provider's business and to determine from publicly available information the reputation of the corresponding respondent institution or service-provider and the quality of supervision, including whether the corresponding respondent institution or service-provider has been subject to a money laundering or terrorist financing investigation or regulatory action;
 - (b) assess the corresponding respondent institution's or service-provider's anti-money laundering and counter the financing of terrorism controls;
 - (c) obtain approval of senior management before establishing new correspondent business relationship;

- (d) clearly understand the responsibilities of the financial institution or financial service-provider and corresponding respondent institution or service-provider respectively; and
- (e) with respect to "payable-through accounts", be satisfied that the corresponding respondent institution or service-provider has conducted measures in regulations 3, 4, 5, and 6 on the clients or customers having direct access to accounts of the corresponding respondent institution or service provider, and that such information is readily available upon request.

9. Reliance on an intermediary or third party

- (1) A financial institution or financial service-provider may rely on an intermediary or a third party to perform requirements under regulations 3, 4, 5, and 6, except that reliance on an intermediary or a third party does not extend to outsourcing or agency relationships.
- (2) Notwithstanding subregulation (1), a financial institution or financial service-provider relying on an intermediary or a third party shall bear the ultimate responsibility over the requirements set out in regulations 3, 4, 5, and 6.
- (3) Where a financial institution or financial service-provider relies on an intermediary or a third party, a financial institution or financial service-provider shall —
 - (a) immediately obtain information set out by the requirements under regulations 3, 4, 5, and 6;
 - (b) take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the requirements under regulations 3, 4, 5, and 6 will be made available from the intermediary or third party upon request without delay;
 - (c) satisfy itself that an intermediary or a third party is regulated, supervised or monitored for complying with requirements of regulations 3, 4, 5, 6 and 11; and
 - (d) have regard to information available on the level of country risk from which the intermediary or third party operates, provided that where the intermediary or third party in a higher risk country is part of the same financial group adequately implementing anti-money laundering and counter terrorist financing measures, this requirement shall not apply to such financial institution or financial service-provider.

10. Higher risk countries

- (1) A sector supervisory authority and the Unit shall have the power to issue out directives, instructions, and make pronouncements to financial institutions or financial service-providers under their authority to apply enhanced measures under regulations 3, 4, 5, and 6 to their clients or customers from higher risk countries for which these enhanced measures are called for by the FATF or where the sector supervisory authority or the Unit deems appropriate.
- (2) Without derogating from the generality of subregulation (1), a sector supervisory authority or the Unit may issue out directives or instructions or make pronouncements for a financial institution or financial service-provider under their authority to apply enhanced measures set out in Schedule 5, which measures shall include any other measures that have a similar effect in mitigating risks.
- (3) A sector supervisory authority or the Unit may prohibit a financial institution or financial service-provider under its authority from —
 - (a) establishing branches or subsidiaries or representative offices of a financial institution or financial service-provider in a higher risk country which does not have adequate anti-money laundering and counter terrorist financing systems;
 - (b) relying on third parties located in the higher risk country to conduct measures in regulations 3, 4, 5, and 6.

11. Establishing and maintaining client's or customer's records

- (1) A financial institution or financial service-provider shall keep records of all domestic and international transactions.
- (2) Records kept shall be maintained to enable a financial institution or financial service-provider to comply swiftly with information requests from a competent authority, a sector supervisory authority or the Unit.
- (3) A financial institution or financial service-provider shall maintain records and information obtained through measures adopted in regulations 3 to 10, account files, business correspondence, and results of any analysis undertaken as well as pursuant to compliance with the requirements of these regulations.
- (4) Records and information obtained shall be kept for a period of at least 5 years beginning from the date a business relationship is terminated or after the date of the occasional transaction.
- (5) Where a competent authority, sector supervisory authority or the Unit so directs, a financial institution or financial service-provider shall keep records or information for a longer period more than the period specified in subregulation (4), which period, not exceeding 5 years, shall be specified in the directive.

12. Internal controls

- (1) A financial institution or financial service-provider shall have internal controls to fight money laundering and counter terrorist financing.
- (2) The internal controls to be put in place shall include policies, programmes and procedures for —
 - (a) identification of a client or customer;
 - (b) dealing with politically exposed persons;
 - (c) verification of the identity of a client or customer and beneficial ownership;
 - (d) conducting of risk assessment;
 - (e) dealing with risk inherent in using new and developing technologies and products;
 - (f) identification of suspicious transactions including reporting thereof and prescribed threshold transactions;
 - (g) record keeping; and
 - (h) information sharing within a financial institution's or financial service-provider's group arrangement for anti-money laundering and counter terrorist financing purposes.
- (3) A financial institution or financial service-provider shall have processes and systems that will enable the financial institution or financial service-provider to meet its obligations under the Act and these regulations.
- (4) A financial institution or financial service-provider shall put in place adequate safeguards on the confidentiality and exchange of information.

13. Recruitment of employees

- (1) A financial institution or financial service-provider shall screen employees upon recruitment to ensure high employment standards.
- (2) Amongst employees employed, a financial institution or financial service-provider shall designate an officer at a senior management level to undertake activities specified under section 19(1) and (2) of the Act.

- (3) A designated senior officer shall have the requisite knowledge and understanding of a financial institution's or financial service-provider's anti-money laundering and counter terrorist financing internal control programmes.

14. Training of employees

- (1) A financial institution or financial service-provider shall establish a training programme designated to ensure that employees are aware of money laundering and terrorist financing activities.
- (2) A financial institution or financial service-provider shall develop manuals and training programmes to ensure that employees are aware of –
 - (a) know your client or customer and verification requirements;
 - (b) reporting of suspicious transactions and transactions above the designated threshold;
 - (c) record keeping requirements;
 - (d) internal control programmes; and
 - (e) obligations under the Act, these regulations, and guidelines issued in terms of the Act.

15. Audit and supervision

A financial institution or financial service-provider shall –

- (1) have an independent audit function to test the veracity and adequacy of the internal control procedures, processes, supervision and systems to fight money laundering and counter terrorist financing; and
- (2) exercise adequate supervision on all its branches, subsidiaries and representative offices to ensure compliance with the Act, these regulations and guidelines issued in terms of the Act.

16. Inspections

- (1) A sector supervisory authority and the Unit shall have the power to conduct anti-money laundering and counter terrorist financing inspections and assessments on a financial institution or financial service-provider.
- (2) When conducting inspections or assessments, a sector supervisory authority or the Unit may compel the production of any document, record or material which may be necessary to give a glimpse of whether a financial institution or financial service-provider complies or does not comply with the Act, these regulations or guidelines issued out under the Act.
- (3) Inspections and assessments may be conducted jointly by a sector supervisory authority and the Unit.
- (4) A sector supervisory authority shall be obliged to produce inspection and assessment reports and share them with the Unit.

17. Sharing of information

- (1) A financial institution or financial service-provider with branches, subsidiaries, or representative offices shall share information on anti--money laundering and counter terrorist financing measures employed by the financial institution or financial service-provider.
- (2) Shared information shall be subject to confidentiality protocols and safeguards applicable within a financial institution or financial service-provider.

- (3) A financial institution or financial service-provider shall ensure that information —
 - (a) shared does not in any way compromise any inquiry or investigation conducted by a competent authority pursuant to reporting of a suspicious report submitted by a financial institution or financial service-provider; and
 - (b) communicated to the financial institution or financial service-provider in terms of regulation 10 is shared with all the financial institution's or financial serviceprovider's branches, subsidiaries or representative offices.
- (4) When sharing information, a financial institution or financial service-provider shall satisfy itself that same information is shared.

18. Compliance

- (1) A sector supervisory authority and the Unit shall have the power to take such regulatory measures as prescribed under respective regulatory laws to ensure that a financial institution or financial service-provider under the sector supervisory authority's or Unit's supervision complies with the Act, these regulations and guidelines issued in terms of the Act.
- (2) Where a financial institution or service-provider fails to comply with the Act, these regulations and guidelines issued in terms of the Act, a sector supervisory authority or the Unit may impose any or some of these administrative sanctions —
 - (a) suspension of a license for a specified period which shall not be for a period of more than 12 months;
 - (b) revocation of a license or permit as the case may be;
 - (c) additional conditions on the license or permit;
 - (d) a public statement to the effect that a relevant financial institution or financial service-provider is not complaint with the Act, these Regulations, and guidelines issued in terms of the Act;
 - (e) directive obliging a relevant financial institution or financial service-provider to perform a specific act or refrain from a certain act mentioned in the directive; or
 - (f) forfeiture of certain rights and privileges.
- (3) Where the Unit has no power to impose administrative sanctions, the Unit shall recommend to a sector supervisory authority to impose administrative sanctions.
- (4) A sector supervisory authority or the Unit shall have the power to impose a financial penalty prescribed under any regulatory law or prescribed under the Act against a financial institution or financial service-provider for failure to comply with the Act, these regulations or guidelines issued under the Act.
- (5) Without derogating from the generality of this regulation, a sector supervisory authority or the Unit may impose any or some of the administrative sanctions in subregulation (2) against a person, including a financial institution or financial service-provider, convicted of an offence under the Act.

19. Reporting suspicious transactions

- (1) A financial institution or financial service-provider shall—
 - (a) if it suspects or has reasonable grounds to suspect that a transaction with a client or customer involves funds which are the proceeds of a serious offence listed in Schedule 4, report its suspicion to the Unit; and
 - (b) report a suspicious transaction by filling completely, sufficiently and timely a suspicious transaction reporting form prescribed pursuant to section 18 of the Act.

- (2) Reporting of a suspicious transaction shall be done immediately upon forming the suspicion and in any case, not later than 7 days.
- (3) Where a financial institution or financial service-provider fails to report as required under subregulation (2), a financial institution or financial service-provider shall submit, together with the suspicious transaction report, a written reasonable explanation the cause of the delay.
- (4) A financial institution or financial service-provider shall report not only suspicious transactions but also attempted transactions.
- (5) Reporting of suspicious and attempted transactions shall be reported irrespective of the amount of the transaction.
- (6) Where a suspicious or attempted transaction is in relation to financing of terrorism, a financial institution or financial service-provider shall specify in the report whether the suspicious or attempted transaction was for the financing of —
 - (a) terrorist acts;
 - (b) terrorist groups or organisations; or
 - (c) individual terrorists.
- (7) Reporting of a transaction in relation to subregulation (6) shall be done irrespective of whether there is any link to specific terrorist act or acts.
- (8) Where a transaction is known, rather than suspected, to be related to property owned or controlled by or on behalf of a terrorist or terrorist group or organisation, a financial institution or financial service-provider shall not complete the transaction.
- (9) A financial institution or financial service-provider shall adequately, clearly, concisely, and thoroughly describe the factors that made or rendered a transaction or activity suspicious.
- (10) Where the Unit has requested additional information other than information submitted in the suspicious transaction report, a financial institution or financial service-provider shall submit such additional information within a reasonable time and in any event not later than 14 days of the request for additional information.
- (11) A financial institution or financial service-provider shall keep a record of a copy of a suspicious or attempted transaction report as well as a copy of additional information submitted.
- (12) A financial institution or financial service-provider shall not —
 - (a) disclose to anyone, including the client or customer, the contents of the suspicious transaction report or that the financial institution or financial service-provider has made such a report and neither shall the officials of the Unit disclose the contents of the suspicious transaction reports or that the suspicious or attempted transaction have been reported to the Unit; and
 - (b) request any information from the person making or attempting to make a transaction that would not normally be requested when conducting a transaction to avoid tipping off.
- (13) There shall be immunity from criminal or civil proceedings for a financial institution or financial service-provider including its directors, employees, or officers, which submits a suspicious or attempted transaction report in good faith and the immunity shall extend to situations where a financial institution or financial service-provider voluntarily provide information to the Unit because of suspicion of a serious offence activity.
- (14) Where a financial institution or financial service-provider decides to terminate a business relationship with the client or customer upon filing a suspicious transaction report, the financial institution or financial service-provider shall include that decision as part of the information in the suspicious transaction report.

20. Wire transfers

- (1) A financial institution or financial service provider shall ensure that all cross-border wire transfers are always accompanied by the following information —
 - (a) accurate originator's information which include —
 - (i) name of the originator;
 - (ii) account number of the originator where such an account is used to process the transaction or, in the absence of the account, a unique transaction reference number which permits traceability of the transaction; and
 - (iii) address, national identity number, or date and place of birth of the originator.
 - (b) beneficiary information which include —
 - (i) name of the beneficiary; and
 - (ii) account number of the beneficiary where such an account is used to process the transaction or, in the absence of the account, a unique transaction reference number which permits traceability of the transaction.
- (2) Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, a financial institution or financial service-provider shall —
 - (a) ensure that the batch file contains accurate originator's information as well as full beneficiaries' information which is fully traceable within the beneficiaries' countries; and
 - (b) include the originator's account number or unique reference number of the transaction in the batch file.
- (3) Whenever a cross-border wire transfer takes place and there is a suspicion of a money laundering or terrorist financing activity, a financial institution or financial service-provider shall verify information required under subregulation (1) above.
- (4) An intermediary financial institution or financial service--provider shall —
 - (a) ensure that all the information of the originator and beneficiary that accompanies a cross-border wire transfer is retained with it;
 - (b) keep a record, for at least 5 years, of all the information received from the ordering financial institution or financial service-provider or another intermediary financial institution or financial service-provider where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer;
 - (c) take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers which lack the required information for the originator or beneficiary; and
 - (d) put in place risk-based policies and procedures for determining —
 - (i) when to execute, reject, or suspend a cross-border wire transfer lacking the required originator or beneficiary information; and
 - (ii) the appropriate follow-up action.
- (5) A beneficiary financial institution or financial service-provider shall —
 - (a) take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack the required originator or beneficiary information;

- (b) verify the identity of the beneficiary if the identity has not been previously verified and maintain this information in accordance with regulation 11; and
- (c) have risk-based policies and procedures for determining —
 - (i) when to execute, reject, or suspend a wire transfer lacking the required originator or beneficiary information; and
 - (ii) the appropriate follow-up action.
- (6) A money or value transfer service provider, whether operating directly or through agents, shall comply with the requirements of subregulations 1, 2, and 3 above subject to necessary modifications.
- (7) Where a money or value transfer service provider controls both the ordering and beneficiary sides in a wire transfer, the money or value transfer service provider shall —
 - (a) take into account all the information from both the ordering and beneficiary sides in order to determine whether a suspicious transaction report has to be filed; and
 - (b) file the suspicious transaction report indicating the country affected by the suspicious wire transfer, and make relevant transaction information available to the Unit.
- (8) An ordering, intermediary, or beneficiary financial institution or financial service-provider, including a money or value transfer service provider shall —
 - (a) identify and report all suspicious wire transfers; and
 - (b) implement the requirements to take freezing action and comply with obligations set out in Part V of these regulations.

21. Registration with the Unit

- (1) A financial institution or financial service-provider shall register with the Unit in a form to be prescribed by the Unit.
- (2) An existing financial institution or financial service-provider shall register with the Unit within 90 days of publication of the prescribed form by the Unit.
- (3) Where a financial institution or financial service-provider is established after the publication of the prescribed form, the financial institution or financial service-provider shall register with the Unit within 30 days of its establishment.
- (4) The registration of a financial institution or financial service-provider shall be accompanied by such particulars as are required under the registration form prescribed by the Unit.
- (5) The Unit shall keep and maintain a register of every financial institution or financial service-provider registered.
- (6) A financial institution or financial service-provider registered shall notify the Unit, in writing, of any changes to the particulars furnished in terms of this regulation within 60 days of such changes.
- (7) A financial institution or financial service-provider which fails to register with the Unit as required under the Act and this regulation may be subjected to financial penalty of a fine not exceeding M50,000.00.

Part III – Designated non-financial business and profession (DNFBP) and designated business

22. Identification of a client or customer and record keeping

A designated non-financial business and profession or designated business shall undertake and observe the requirements of regulations 3, 4, 5, 6 and 11 subject to the following —

- (1) a casino - when clients or customers engage in financial transactions equal to or above the threshold of M25, 000.00;
- (2) a real estate agent - when involved in transactions for clients or customers concerning the buying and selling of real estate provided that a real estate agent shall comply with the requirements of regulations 3, 4, 5, and 6 in respect of both the clients or customers and the vendors of the property;
- (3) a dealer in precious metals and dealer in precious stones - when they engage in any cash transaction with a client or customer equal to or above the applicable threshold of M100, 000.00;
- (4) a lawyer, notary, other independent legal professional and accountant - when they prepare for or carry out transactions for their clients or customers concerning the following activities —
 - (a) buying and selling of real estate;
 - (b) managing of client's or customer's money, securities or other assets;
 - (c) management of bank, savings or securities accounts, or books of accounts;
 - (d) organisation of contributions for the creation, operation or management of companies;
 - (e) buying and selling of business entities; or
 - (f) creation, operation or management of legal persons or arrangements.
- (5) a trust and company service provider - when preparing for or carrying out transactions for clients or customers concerning the following activities —
 - (a) acting as a formation agent of legal persons;
 - (b) acting as, or arranging for another person to act as, a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
 - (c) providing a registered office, business address or accommodation, correspondence or administrative address of a company, a partnership or any other legal person or arrangement;
 - (d) acting as, or arranging for another person to act as, a trustee of an express trust or performing the equivalent function for another firm of legal arrangement; or
 - (e) acting as or arranging for another person to act as a nominee shareholder for another person; and
- (6) a dealer in motor spare parts, hardware store, motor vehicle dealership, manufacture and wholesaler - when clients or customers engage in cash transactions equal to or above the threshold of M25, 000.00.

23. Measures applicable to DNFBP and designated business

Regulations 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, and 21 shall apply, with necessary modifications, to all designated non-financial businesses and professions and designated businesses subject to the following —

- (1) lawyers, notaries, other independent legal professionals, and accountants shall report suspicious transactions on behalf of or for clients or customers when they are engaged in financial transactions in relation to the activities described in regulation 22(4);
- (2) dealers in precious metals and dealers in precious stones shall report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable threshold of M100, 000.00;
- (3) trust and company service providers shall report suspicious transactions on behalf of or for clients or customers when they engage in a transaction in relation to activities described in regulation 22(5); and
- (4) designated businesses shall report suspicious transactions on behalf of or for clients or customers when they engage in cash transactions equal to or above the threshold of M25, 000.00.

Part IV – Non-profit organisation

24. Affairs of a non-profit organisation

- (1) A non-profit organisation shall conduct its affairs in a transparent manner in order to engender greater confidence in the sector, donor community, and the general public.
- (2) A non-profit organisation shall ensure that the funds or services it acquires or receives are not —
 - (a) proceeds of a serious offence;
 - (b) intended to finance a terrorist, terrorist group or organisation; or
 - (c) intended for the use by terrorist groups or organisations posing as legitimate non-profit organisations.
- (3) A non-profit organisation shall keep and maintain information on the —
 - (a) purpose and objectives of its stated activities; and
 - (b) identity of the person or persons who own, control or direct its activities, including senior officers, board members and trustees.
- (4) A non-profit organisation shall prepare and file with the sector supervisory authority annual financial statements that provide detailed breakdowns of incomes and expenditures.
- (5) A non-profit organisation shall put in place appropriate controls to —
 - (a) ensure that all funds are fully accounted for and are spend in a manner that is consistent with the purpose and objectives of the non-profit making organisation's stated activities;
 - (b) undertake outreach programmes to raise awareness for employees, trustees, and beneficiaries about the vulnerabilities of money laundering and terrorist financing risks; and
 - (c) conduct its transactions through, where feasible, regulated financial channels.
- (6) A non-profit organisation shall —
 - (a) establish the identity, credentials and good standing of its beneficiaries;
 - (b) verify or confirm the identity, credentials and good standing of its beneficiaries;

- (c) keep records and information of the identity of significant donors subject to respecting donors confidentiality where applicable;
 - (d) keep and maintain, for a period of at least 5 years, records of transactions made under these regulations;
 - (e) make available all records and information, without delay, kept and maintained to a competent authority, sector supervisory authority/accrediting institution or the Unit upon appropriate request;
 - (f) have clear policies that promote transparency, integrity and public confidence in the administration and management of the non-profit organisation; and
 - (g) comply with rules and regulations, including rules and standards applied by a sector supervisory authority or self-regulatory organisation.
- (7) A non-profit organisation, including persons who own, control or direct its activities, senior officers, board members and trustees, which is —
- (a) a front for raising funds for a terrorist, terrorist group or organisation;
 - (b) being exploited as a conduit or channel for terrorist financing, including for the purpose of escaping asset freezing measures; or
 - (c) concealing, obscuring, or disguising the diversion of funds intended for legitimate purposes, but redirected for the benefit of a terrorist, terrorist group or organisation,
- commits an offence, and shall be liable on conviction to imprisonment for a period not exceeding 25 years or a fine not exceeding M25, 000, 000.00 or both.
- (8) A sector supervisory authority or self-regulatory organisation may impose an administrative sanction or financial penalty not exceeding M50, 000.00 against a non-profit organisation that fails to comply with subregulation (6).
- (9) Regulations 10, 12, 13, 14, 15, 16, 17, 18, 19, and 21 shall apply, with necessary modifications, to a non-profit organisation provided that measures under regulations 3, 4, 5 and 6 shall be in respect of a non-profit organisation's beneficiaries, donors, or a person or persons who own, control or direct its activities, including senior officers, board members and trustees.

Part V – Financial sanctions related to terrorist financing and financing proliferation

25. Financing and supporting terrorist activities

- (1) Where a person contributes to the commission of an offence within the meaning of section 65(1) of the Act it shall be sufficient to show that such contribution was intentional in that it was made —
 - (a) with the aim of furthering the criminal activity or criminal purpose of the group or organisation; or
 - (b) in the knowledge of the intention of the group or organisation to commit a terrorist financing offence.
- (2) Where a person is charged with terrorist financing, it shall be irrelevant whether the person alleged to have committed the offence is in Lesotho or in another country different from where the —
 - (a) terrorist, terrorist group or organisation is located;
 - (b) terrorist act occurred; or
 - (c) terrorist act will occur.

26. Establishment of the Anti Terrorism Committee

- (1) There is established a committee to be known as the Anti Terrorist Committee, in these regulations to be called "the Committee" comprising the following officers or their representatives —
 - (a) the Principal Secretary Ministry of Finance;
 - (b) the Principal Secretary Ministry of Home Affairs;
 - (c) the Principal Secretary Ministry of Foreign Affairs and International Relations;
 - (d) the Commissioner of Police;
 - (e) the Governor of the Central Bank; and
 - (f) the Director of the Financial Intelligence Unit.
- (2) The Committee shall —
 - (a) advise the Minister on the implementation of the Resolutions;
 - (b) coordinate the implementation of the Resolutions;
 - (c) recommend to the Minister proposals for designating or listing a person or entity in accordance with these regulations;
 - (d) develop procedures to communicate sanctions list; and
 - (e) collaborate with law enforcement, national intelligence service and sector supervisory authorities to ensure compliance and monitoring of measures to implement the Resolutions.

27. Designation and identification of persons and entities

- (1) Where a relevant United Nations Security Council Sanctions Committee has made a decision designating a person or entity and communicated or published such a decision in accordance with its established modes of communication, the communication shall be transmitted through the Minister responsible for foreign affairs and international relations in Lesotho.
- (2) Upon receipt of the communication, the Minister responsible for foreign affairs and international relations shall, without delay, submit designation to the Minister and the Minister shall by notice and without delay, communicate such decision to all accountable institutions, competent authorities, the Unit and sector supervisory authorities. For purposes of this subregulation, notice shall refer to any form of notification by letter, email, telephone, fax, or any form of written medium.
- (3) An accountable institution, a competent authority, the Unit, or a supervisory authority shall regularly consult a relevant United Nations Security Council Sanctions Committee's website to obtain a fully updated version of the list of already designated persons and entities subject to the sanctions measures.
- (4) The communication in respect of a person or entity shall be for a designated person or entity if such person or entity is, for purposes of —
 - (a) United Nations Security Council Resolutions 1267 (1999), 1989 (2011) and their Successor Resolutions listed in Schedule 6 and future successor resolutions to Resolution 1267 (1999) —
 - (i) a person or entity participating in the financing, planning, facilitating, preparing, or perpetrating acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; selling or transferring arms and related material to; recruiting for; or supporting acts or activities of Al-Qaida, or any cell, affiliate, splinter group or derivative thereof; or

- (ii) an undertaking owned or controlled, directly or indirectly, by any person or entity designated pursuant to subparagraph (i), or by persons acting on their behalf or at their direction;
- (b) United Nations Security Council Resolution 1267 (1999), 1988 (2011), and their successor resolutions —
 - (i) a person or entity participating in the financing, planning, facilitating, preparing, or perpetrating acts or activities by, in conjunction with, under the name of, on behalf of, or in support of; supplying, selling or transferring arms and related materials to; recruiting for; or otherwise supporting acts or activities of those designated and other individuals, groups, undertakings and entities associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan; or
 - (ii) an undertaking owned or controlled, directly or indirectly, by any person or entity designated pursuant to subparagraph (i), or by persons acting on their behalf or at their direction;
- (c) United Nations Security Council Resolutions 1373 (2001)—
 - (i) a person or entity who commits or attempts to commit terrorist acts, or who participates in or facilitates the commission of terrorist acts;
 - (ii) an entity owned or controlled, directly or indirectly, by any person or entity designated pursuant to subparagraph (i); or
 - (iii) a person or entity acting on behalf of, or at the direction of, any person or entity designated pursuant to subparagraph (i);
- (d) United Nations Security Council Resolution 1450 (2004) —
 - (i) a person or entity who acquires, develops, manufactures, possesses, transports, transfers, or uses biological, chemical and nuclear weapons and their means of delivery and related materials for terrorist purposes; or
 - (ii) a person or entity who engages or attempts to engage in the activities listed in subparagraph (d) (i) above by assisting, financing, or participating in such activities as an accomplice; or
- (e) Designation in accordance with Resolutions 1718 (2006), 1737 (2006), 1747 (2007), 1803 (2008) or 1829 (2010) or their successor resolutions as set out in Schedule 7.
- (5) The Committee shall, on reasonable grounds, determine whether a person or entity has been identified as a person or entity engaged in activities specified in subregulation (4)(a), (b), (d), or (e) and recommend to the Minister to propose designation or listing of such person or entity to the relevant United Nations Security Council Sanctions Committee.
- (6) The recommendation referred to in subregulation (5) shall detail the material facts or supporting evidence of activities associated with the identified person or entity, which may include —
 - (a) information on the residence and nationality of the person or entity;
 - (b) specific findings demonstrating the association or alleged activities;
 - (c) supporting evidence or documents that can be supplied;
 - (d) details of any connection with a currently listed person where applicable; or
 - (e) name of the person or person responsible for the decisions of a designated group, undertaking or entity.
- (7) The Minister shall submit the proposal for designation or listing using the Form in Schedule 8.

- (8) The Committee shall on reasonable grounds determine whether a person or entity has been identified as a person or entity engaged in activities specified in subregulation (4)(c) and recommend to the Minister to designate and publish a Sanction List in the *Gazette* the name of such person or entity.
- (9) When submitting a recommendation to designate under subregulation (8), the Committee shall detail the material facts or supporting evidence of activities associated with the identified person or entity, which may include information specified in subregulation (6).
- (10) A sector supervisory authority, the Unit, or relevant competent authority shall require any person or entity, including an accountable institution under its authority to identify within its business dealings and relationships whether a beneficiary, client, customer, a person or persons who own, control or direct its activities, including senior officers, board members and trustees, as the case may be, is a designated person or entity.
- (11) A criminal charge or conviction of a person or entity shall not be a prerequisite for a submission of a proposal for designation or listing.
- (12) Where —
 - (a) a designation or request for designation is made by a country pursuant to regulation 27(4)(c), it shall be transmitted to the Minister responsible for foreign affairs and international relations in Lesotho who shall, without delay, submit the request to the Minister for his consideration and the Minister shall, without delay, on the advice of the Committee, make a determination whether to designate the person or entity; or
 - (b) a freezing order has been issued in accordance with regulation 28(1) the Minister shall, through the Minister responsible for foreign affairs and international relations, request another country to freeze funds or other assets in accordance with its domestic laws.

28. Freezing order

- (1) Where a person or entity has been designated and listed in accordance with regulation 27, the Minister shall issue out a freezing order directing a person or entity, including an accountable institution, to freeze without delay and without prior notice funds or other assets of the designated person or entity.
- (2) The freezing order specified in subregulation (1) shall empower a sector supervisory authority, the Unit, or the Committee to issue out to a person or entity, including an accountable institution a directive, instruction, or request to observe and comply with the freezing order and to freeze, without delay and without prior notice, the funds or other assets, and to ensure that no funds and other assets are made available to or for the benefit of a person or entity —
 - (a) designated under the United Nations Security Council Resolution 1267 (1999) and its Successor Resolutions in Schedule 6 and future successor resolutions as a person or entity engaged in activities listed in regulation 27(4)(a);
 - (b) designated under the United Nations Security Council Resolution 1267 (1999), 1988 (2011), and their successor resolutions as a person or entity engaged in activities listed in regulation 27(4)(b);
 - (c) proposed for designation by the Minister or designated by another state pursuant to Security Council Resolution 1373 (2001) as a person or entity engaged in activities listed in regulation 27(4)(c);
 - (d) designated pursuant to the United Nations Security Council Resolution 1450 (2004) as a person or entity engaged in activities listed in regulation 27(4)(d); or
 - (e) designated in accordance with Resolutions 1718 (2006), 1737 (2006), 1747 (2007), 1803 (2008) or 1829 (2010) or their successor resolutions as set out in Schedule 7.

- (3) When undertaking obligations under subregulation (2), a person or an entity, including an accountable institution shall—
 - (a) respect the rights of affected parties;
 - (b) respect the rule of law; and
 - (c) recognise the rights of innocent third parties.

29. Sanctions against terrorist financing

- (1) Where there are funds or other assets in their custody or control, a person or entity, including an accountable institution shall stop —
 - (a) the flow of funds or other assets to a terrorist, terrorist groups or organisations;
 - (b) use of funds or other assets by a terrorist, terrorist groups or organisations.
- (2) When undertaking obligations under subregulation (1), any person or entity, including an accountable institution shall -
 - (a) respect the rights of affected parties;
 - (b) respect the rule of law; and
 - (c) recognise the rights of innocent third parties.

30. Prohibition of dealing with funds and other assets

- (1) No person or entity, including an accountable institution shall make any funds or other assets, economic resources, or financial or other related services available, directly or indirectly, wholly or jointly, for the benefit of designated persons and entities identified under regulation 27 and any person and entity acting on behalf of, or at the direction of such persons or entities unless authorised or notified in writing by a sector supervisory authority, the Unit, or any competent authority, exercising its powers under these regulations or any law in Lesotho.
- (2) Nothing in this regulation shall be construed as derogation from the obligation to protect the rights of *bona fide* third parties acting in good faith when implementing this regulation.
- (3) A person who contravenes this regulation commits an offence, and shall on conviction be liable to imprisonment for a period not exceeding 10 years or a fine of not exceeding M1, 000, 000.00.
- (4) Notwithstanding subregulation (3), a supervisory authority, the Unit, or any competent authority may impose against a person or entity, including an accountable institution, a financial penalty not exceeding M50,000.00 for non-compliance with subregulation (1).

31. Freezing of fund and other assets

- (1) Where there are funds or assets in their custody or control, any person or entity, including an accountable institution shall, act upon a freezing order and freeze, without delay and without prior notice, funds or assets of persons or entities identified pursuant to regulation 27 to the extent that —
 - (a) the funds or assets are wholly or jointly owned or controlled, directly or indirectly, by those persons or entities;
 - (b) it is not necessary that the funds or other assets are linked or tied to a particular terrorist act, plot or threat;
 - (c) the funds or other assets derive or are generated from funds or other assets owned or controlled, directly or indirectly, by those persons or entities; or

- (d) the funds or other assets are the funds or other assets of persons or entities acting on behalf of, or at the direction of those persons or entities.
- (2) Any person or entity, including an accountable institution shall, immediately upon freezing of the funds and other assets pursuant to subregulation (1), report to a sector supervisory authority, the Unit, or Committee as the case may be that funds or assets have been duly frozen.
- (3) Where a report is received in accordance with subregulation (2), a sector supervisory authority, the Unit, or Committee as the case may be shall immediately conduct an inspection to verify the correctness or otherwise of the report and where relevant, a sector supervisory authority shall share the inspection report with the Unit for ultimate advice to the Minister or relevant bodies.
- (4) Nothing in this regulation shall be construed as derogation from the obligation to protect the rights of *bona fide* third parties acting in good faith when implementing this regulation.
- (5) The Minister may impose against a person or entity, including an accountable institution, a financial penalty not exceeding M50,000.00 for non-compliance with subregulations (1) and (2).

32. Access to frozen assets and other assets

- (1) Where funds or others assets have been dealt with pursuant to Part V of these regulations, the ommittee shall recommend to the Minister to allow a person or entity identified pursuant to regulation 27 —
 - (a) to have access to the funds or other assets if they are —
 - (i) necessary for basic expenses, including payment for foodstuffs, rent or mortgage, medicines and medical treatment, taxes, insurance premiums, or public utility charges;
 - (ii) payment for reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services; or
 - (iii) fees or service charges for routine holding or maintenance of frozen funds or other financial assets or economic resources.
 - (b) to gain from the accounts dealt with pursuant to Part V —
 - (i) interest or other earnings due on those accounts; and
 - (ii) payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to Part V.
- (2) Access to frozen funds or other assets pursuant to subregulation (1) shall be authorised after the Minister has notified the relevant United Nations Security Council Sanctions Committee and upon receipt of approval thereof.
- (3) When making a notification under subsection (2), the Minister shall provide information on —
 - (a) recipient's name and addresses;
 - (b) recipient's reference number on the Sanctions List;
 - (c) purpose of payment and justification of the determination of expenses falling under subregulation (1); and
 - (d) where the recipient's frozen assets or other assets are kept.

33. Delisting of persons and entities and unfreezing of funds and other assets

- (1) Where the Minister —
 - (a) through the Minister responsible for foreign affairs, receives information from relevant United Nations Security Council Sanctions Committee that a person or an entity previously subject to sanctions measures is no longer subject to regulation 27(4)(a), (b), (d), or (e), the Minister shall communicate such information to all accountable institutions, sector supervisory authorities, competent authorities, and the Unit and in doing so, the Minister shall also revoke the freezing order in respect of that person or entity;
 - (b) upon reasonable grounds believes that a person or an entity in the Sanctions List is no longer subject to regulation 27(4)(c) the Minister shall remove the person or entity from the Sanction List and in doing so the Minister shall also revoke the freezing order in respect of that person or entity.
- (2) Request or recommendation to remove a person or entity from the Sanctions List shall —
 - (a) state why the person or entity is no longer associated or connected with activities under regulation 27;
 - (b) state the person's or entity's current activities, including occupation where relevant and information of possession, control, or ownership of assets; and
 - (c) submit any documentation supporting the request for delisting with an explanation of its relevance.
- (3) Where a person or entity has been dealt with in accordance with subregulation (1), the person or entity, including an accountable institution shall unfreeze funds or other assets of such a person or entity.
- (4) Where, upon verification that the person or entity appearing in the Sanctions List is not a person or entity identified and designated or listed, there are clear indications that a person or entity, with a similar name as a person or entity identified pursuant to regulation 27, has been inadvertently affected by any action exercised pursuant to the provisions of Part V, the Committee shall recommend to the Minister to revoke the designation published in the *Gazette* and revoke a freezing order in respect of a person or entity inadvertently listed in the Sanctions List.
- (5) Nothing in these regulations shall preclude a person or entity subjected to designation and listing under relevant United Nations Security Council Resolutions from directly submitting a request for delisting to a relevant United Nations Security Council Sanctions Committee.

34. Immunity and confidentiality

- (1) An action, or suit, or other proceedings shall not lie against a person acting in the ordinary course of giving effect to Part V where such actions are taken in good faith.
- (2) A person entrusted to implement Part V shall not disclose information without proper authorization.

Part V – Miscellaneous provisions

[Please note: duplicate Part numbering as in original.]

35. Demand of communication call data

- (1) The Unit may demand communication call data from a relevant service provider as the Unit considers appropriate for giving effect to the provisions of the Act or these regulations.

- (2) Where the Unit has demanded communication call data pursuant to subregulation (1), a relevant service provider shall furnish the same immediately upon demand and in any case not later than seven days.
- (3) Notwithstanding the provisions of subregulation (1) herein, a service provider shall provide the Unit with communication call data spontaneously where the service provider have reasonable grounds to believe that the communication is or has been for furtherance of criminal offences.
- (4) The Unit shall ensure that communication call data received is treated in a confidential manner, safeguarded and used for purposes of enhancing analysis in respect of its mandate.

36. International Cooperation

- (1) Where a foreign State requests assistance to locate or seize property in Lesotho suspected to be tainted property in respect of an offence within its jurisdiction, the request shall be submitted to a relevant competent authority, save for the Police, where the request shall be submitted to the Director of Public Prosecutions.
- (2) A request for assistance on behalf of the Kingdom of Lesotho to a foreign State to locate or seize property in a foreign State may be made by a relevant competent authority, save for the Police where the request shall be made by the Director of Public Prosecutions.
- (3) A request made and received shall be accompanied by acknowledgement of receipt and provision of updates as the case may be by a competent authority or the Director of Public Prosecutions making or receiving the request.
- (4) If a competent authority or the Director of Public Prosecutions no longer needs the assistance requested, such shall be promptly communicated to the requested State.
- (5) Updates on requests made shall be submitted to a requesting foreign State within a reasonable time, and in any event not later than 90 working days.
- (6) When making a request for assistance in a foreign State, a competent authority or the Director of Public Prosecutions may provide the time within which assistance is requested which will depend on the urgency of the matter, and may indicate that the requested State can be contacted every 30, 60, or 90 days.
- (7) A request for assistance by a foreign State or a competent authority or the Director of Public Prosecutions shall be made in a language specified by the requested State and shall include information in Schedule 9.

37. General penalty

- (1) Where a person or an entity, including an accountable institution, fails to comply with a requirement under these regulations, such non-compliance shall be regarded as a commission of an offence, and shall be punishable and where no penalty is specified, upon conviction, to —
 - (a) in the case of non-compliance with requirements related to anti-money laundering measures, imprisonment for a period not exceeding 10 years or a fine of not less than M100, 000.00 or both; and
 - (b) in the case of non-compliance with requirements related to counter terrorist financing measures, imprisonment for a period not exceeding 15 years or a fine of not less than M150, 000.00 or both.
- (2) Notwithstanding subregulation (1), a sector supervisory authority or the Unit may impose against an accountable institution a financial penalty not exceeding M50, 000.00 for non-compliance with any regulation where no administrative sanction has been specified.

Schedules

Schedule 1 (Regulation 2)

Designated person or entity

1. Individual, entity, group, or undertaking designated by the Committee of the United Nations Security Council established pursuant to Resolution 1267 (1999) (the 1267 Committee), as being an individual associated with Al-Qaida, entity, group, or undertaking associated with Al-Qaida;
2. Individual, entity, group, or undertaking designated by the Committee of the United Nations Security Council established pursuant to Resolution 1988 (2011) (the 1988 Committee), as being associated with the Taliban in constituting a threat to the peace, stability and security of afghanistan, or individual, entity, group, or undertaking associated with the Taliban;
3. Any natural or legal person or entity identified and submitted, to the relevant United Nations Security Council Committee for designation or listing, by the Kingdom of Lesotho or another country pursuant to the United Nations Security Council Resolution 1373 (2001);
4. Any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to the United Nations Security Council Resolution 1718 (2006) and its successor resolutions by the United Nations Security Council in annexes to the relevant resolutions, or by the United Nations Security Council Committee established pursuant to Resolution 1718 (2006) (the 1718 Sanctions Committee) pursuant to the United Nations Security Council Resolution 1718 (2006); and
5. Any natural or legal person or entity designated for the application of targeted financial sanctions pursuant to the United Nations Security Council Resolution 1737 (2006) and its successor resolutions by the United Nations Security Council in annexes to the relevant resolutions, or by the United Nations Security Council Committee established pursuant to paragraph 18 of Resolution 1737 (2006) (the 1737 Sanctions Committee) pursuant to Resolution 1737 (2006) and its successor resolutions.

Schedule 2 (Regulation 2)

DNFBPs

1. Casinos including internet and ship-based casinos;
2. Real estate agents;
3. Dealers in precious metals;
4. Dealers in precious stones;
5. Lawyers, notaries, and other legal professionals who are sole practitioners, partners or employed within law firms, but do not include internal professionals that are employees of other types of businesses or government agencies;
6. Accountants working as sole practitioners, partners or employed accountants working within an accountancy firm but do not include accountants that are employees of other types of businesses or government agencies;
7. Trust and company service providers which include persons or businesses providing any of the following services to third parties —
 - (a) acting as a formation agent of legal persons;
 - (b) acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

- (c) providing a registered office; business address or accommodation, correspondence or administrative address of a company, a partnership or any other legal person or arrangement;
- (d) acting as or arranging for another person to act as a trustee of an express trust or performing the equivalent function for another firm of legal arrangement; or
- (e) acting as or arranging for another person to act as a nominee shareholder for another person.

Schedule 3 (Regulation 2)

Sector supervisory authorities

1. Casino Board established under the Casino Act 1989²;
2. Central Bank of Lesotho established under the Central Bank of Lesotho Act 2000³;
3. Department of Cooperatives;
4. Financial Intelligence Unit established under the Act;
5. Law Society of Lesotho established under the Law Society Act 1983⁴;
6. Lesotho Institute of Accountants established under the Accountant Act 1977⁵;
7. Mining Board established under the Mines and Minerals Act 2005⁶;
8. Ministry responsible for trade;
9. Registrar General as defined under the Societies Act 1966⁷;
10. Registrar of Companies as defined under the Companies Act⁸; and
11. Registrar of Deeds.

2

Act [No. 4 of 1989](#)

3

Act [No. 2 of 2000](#)

4

No. 13 of 1983

5

Act [No. 9 of 1977](#)

6

Act [No. 4 of 2005](#)

7

Act [No. 20 of 1966](#)

8

Act [No. 18 of 2011](#)

Schedule 4 (Regulation 2)

Serious offences

1. corruption and bribery;
2. counterfeiting and piracy of products;
3. counterfeiting currency;
4. environmental crime;
5. extortion;
6. forgery;
7. fraud;
8. illicit arms trafficking;
9. Illicit trafficking in Narcotic Drugs and Psychotic Substances;
10. illicit trafficking in stolen and other goods;
11. insider trading and market manipulation;
12. kidnapping, illegal restraint and hostage-taking;
13. migrant smuggling;
14. money laundering;
15. murder, grievous bodily harm;
16. participation in an organised criminal group and racketeering;
17. piracy;
18. robbery or theft;
19. sexual exploitation, including sexual exploitation of children;
20. smuggling;
21. terrorism, including terrorist financing;
22. trafficking in human beings.

Schedule 5 (Regulation 10)

Enhanced due diligence measures for higher-risk countries

1. Requiring a financial institution to obtain —
 - (a) additional information on the client or customer (e.g. occupation, volume of assets, information available through public databases), and updating more regularly the identification data of the client or customer and beneficial owner;
 - (b) additional information on the intended nature and business relationship;
 - (c) information on the source of funds or source of wealth of the client or customer;
 - (d) information on the intended or performed transactions; and
 - (e) the approval of senior management to commence or continue with the business relationship.

2. Requiring a financial institution to —
 - (a) conduct enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
 - (b) ensure that the first payment to be carried out through an account in the client's or customer's name shall be made with a bank applying adequate anti-money laundering and counter the financing of terrorism measures;
 - (c) review and amend, or if necessary terminate, corresponding relationships with financial institutions in the higher risk country concerned;
 - (d) increase its supervisory examination and external audit requirements for its branches and subsidiaries based in the higher risk country concerned;
 - (e) apply specific mechanisms or systematic reporting of financial transactions;
 - (f) increase its external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the higher risk country concerned; and
 - (g) introduce enhanced relevant reporting mechanisms or systematic reporting of financial transactions.
3. Refusing the establishment of branches and subsidiaries or representative offices at a higher risk country which does not have adequate anti-money laundering and counter the financing of terrorism systems.

Schedule 6 (Regulation 28 (1))

Successor Resolutions to the United Nations Security Council Resolutions 1267 (1999), 1989 (2011)

1. Resolution 1333 (2000);
2. Resolution 1367 (2001);
3. Resolution 1390 (2002);
4. Resolution 1455 (2003);
5. Resolution 1526 (2004);
6. Resolution 1617 (2005);
7. Resolution 1735 (2006);
8. Resolution 1822 (2008);
9. Resolution 1904 (2009);
10. Resolution 1988 (2011); and
11. Resolution 1989 (2011).

Schedule 7 (Regulation 27(4(e))

Designation under Resolutions 1718 (2006), 1737 (2006) , 1747 (2007), 1803 (2008) and 1929 (2010)

1. Resolution 1718 (2006) —
 - (a) a person or entity engaged in the Democratic People's Republic of Korea (DPRK)'s nuclear-related, other WMD-related and ballistic missile-related programs;

- (b) a person or entity providing support for DPRK's nuclear-related, other WMD-related and ballistic missile-related programs, including through illicit means;
 - (c) a person or entity acting on behalf of or at the direction of a person or entity designated under paragraph (a) or (b) or;
 - (d) a legal person or entity owned or controlled, directly or indirectly, by a person or entity designated under paragraph (a) or (b).
2. Resolutions 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010) —
- (a) a person or entity engaged in Iran's proliferation sensitive nuclear activities or the development of nuclear weapon delivery systems;
 - (b) a person or entity directly associated with or providing support for Iran's proliferation sensitive nuclear activities or the development of nuclear weapon delivery systems;
 - (c) a person or entity acting on behalf or at a direction of a person or entity in paragraph (a) or (b) or by entities owned or controlled by them;
 - (d) a person or entity acting on behalf or at the direction of the individuals and entities of the Islamic Revolutionary Guard Corps designated pursuant to resolution 1929 (2010);
 - (e) an entity owned or controlled, including through illicit means, by the individuals and entities of the Islamic Revolutionary Guard Corps designated pursuant to resolution 1929 (2010);
 - (f) a person or entity acting on behalf or at the direction of the entities of the Islamic Republic of Iran Shipping Lines (IRISL) designated pursuant to resolution 1929 (2010);
 - (g) entities owned or controlled, including through illicit means by the entities of the Islamic Republic of Iran Shipping Lines (IRISL) designated pursuant to resolution 1929 (2010); or
 - (h) a person or entity determined by the United Nations Security Council or the Committee to have assisted a designated person or entity in evading sanction of, or in violating the provisions of resolutions 1737 (2006), 1747 (2007), 1803 (2008) or 1929 (2010).

Schedule 8 (Regulation 27(8))**Standard form for listing****Consolidated List: Cover sheet for the Kingdom
of Lesotho submissions to the Committee***Please complete as many of the following fields as possible***I. IDENTIFICATION INFORMATION FOR INDIVIDUALS**

Surname: _____

First Name: _____

Middle Name: _____

Maiden Surname: _____

Gender: _____

Date of Birth: _____ Place of Birth: _____

Place of Birth: _____

(provide all known details, including city, region, province/state, country, village, etc.)

Citizenship: _____

Languages Spoken _____

Title (e.g.) honorary, professional, or religious):

National Identification Number: _____ Passport Number _____

Residential Address: _____

Postal Address: _____

Current Location: _____ Previous Location: _____

Mother's Full Names: _____

Father's Full Names: _____

Undertakings and entities owned or controlled, directly or indirectly by the individual

_____Other relevant details: _____

(such as physical description, distinguishing marks and characteristics)

IDENTIFICATION - For Groups, Undertaking, or Entity

Name: _____

Also Known As (A.K.A.): _____

Where possible, note whether it is a strong or weak A.K.A

Now Known As (N.K.A) _____

Formerly Known As (F.K.A) _____

Address(es): _____

Headquarters and branches. _____

Complete one or more of the following:

- (a) participating in the financing, planning, facilitating, or perpetrating acts or activities by, in conjunction with, under the name of, on behalf of, or in support of Al-Qaida (AQ), Usama bin Laden (UBL), or the Taliban, or any cell, affiliate, splinter groups or derivative thereof
 - Name(s) of cell, affiliate, splinter or derivative thereof
- (b) supplying, selling or transferring arms and related material to AQ, UBL or the Taliban, or any cell, affiliate, splinter group or derivative thereof
 - Name(s) of cell, affiliate, splinter or derivative thereof
- (c) recruiting for AQ, UBL or the Taliban, or any cell, affiliate, splinter group or derivative thereof
 - Name(s) of cell, affiliate, splinter or derivative thereof
- (d) otherwise supporting acts or activities of AQ, UBL or the Taliban, or any cell, affiliate, splinter group or derivative thereof
 - Name(s) of cell, affiliate, splinter or derivative thereof
- (e) other associations with AQ, UBL or the Taliban, or any cell, affiliate, splinter group or derivative thereof
 - Name(s) of cell, affiliate, splinter or derivative thereof
- (f) entity owned or controlled, directly or indirectly, by, or otherwise supporting, an individual or entity on the Consolidated List
 - Name(s) of individual or entity on the Consolidated List
- (g) acquiring, developing, manufacturing, transporting or transferring, in possession, or using biological, chemical, or nuclear weapons and their means of delivery and related materials for terrorist purposes
 - Name(s) of non-state actor or entity
- (h) engaging or attempting to engage as an accomplice by assisting, financing, or participating in acquiring, developing, manufacturing, transporting or transferring, in possession, or using biological, chemical, or nuclear weapons and their means of delivery and related materials for terrorist purposes
 - Name(s) of non-state actor or entity

Please attach a Statement of Case which should provide as much as possible on the basis for listing indicated above, including: (1) specific findings demonstrating the association or activities alleged; (2) the nature of supporting evidence (e.g., intelligence, law enforcement, judicial, media, admissions by subject, etc.) and (3) supporting evidence or documents that can be supplied. Include details of any connection with a currently listed individual or entity. Indicate what portion(s) of the Statement of Case the Committee may publicly release or release to Member States upon request.

III. POINT OF CONTACT

(The individual(s) below may serve as a point of contact for further questions on this case: (THIS INFORMATION SHALL REMAIN CONFIDENTIAL))

Name: _____ Position /Title _____

Schedule 9 (Regulation 35 (7))

Information on request for assistance

1. Identification of the office or authority presenting or submitting the request and the authority conducting the investigation, prosecution or proceedings in the requesting state, including contact particulars for the office or authority presenting or submitting the request, the contact particulars of the relevant investigating officer or prosecutor;

2. Need for requirement for translation services;
3. Details of any prior contact between officers of a competent authority and office of the director of public prosecutions and requesting foreign state or requested state as the case may be;
4. Acknowledgement or update on the request made;
5. Time limits within which compliance with the request is required and the reason for the urgency on the time limit;
6. A need for confidentiality the reason thereof if any;
7. A description of the basis upon which a request is made, including whether the request is based on bilateral treaty, convention, conviction, or reciprocity;
8. Summary of relevant facts of the case necessitating the request;
9. A description of the offence and applicable penalty, with an excerpt or copy of the relevant parts of the law of the requesting state;
10. A description of the assistance requested;
11. A clear and precise explanation of the connection between the investigation, prosecution or proceedings and the assistance sought;
12. A description of the procedures to be followed by the authorities of the requested state in executing the request to ensure that the request achieves its purpose, including any special procedures to enable any evidence to be admissible in the requesting state and reasons why the procedures are required;
13. An indication whether the requesting state wishes its officials or other specified persons to be present at or participate in the execution of the request and the request why that is requested;
14. A certified translation of a language of the requesting state into a language specified by a requested state where necessary.