SAINT LUCIA

STATUTORY INSTRUMENT, 2023, No. 53

ARRANGEMENT OF REGULATIONS

Regulation

PRELIMINARY

1. Citation
2. Interpretation
3. Application

PART I
ESTABLISHMENT AND MAINTENANCE OF RECORDS

4. Responsibility relating to establishment and maintenance of records
5. Records on the identity and transactions of customers
6. Maintenance of records in retrievable form
7. Provision of records to the Authority
8. Request to keep records
9. Records in relation transactions, verification and training

PART II
INTERNAL POLICIES, PROCEDURES OR CONTROLS

10. Responsibility relating to internal policies, procedures or controls
11. Development and application of internal policies, procedures or controls
12. Audit for compliance
13. Independent audit

PART III
SUSPICIOUS TRANSACTION REPORTING

14. Responsibility relating to suspicious transaction reporting
15. Internal reporting of suspicious transactions
16. Reporting of suspicious transactions to the Authority
17. Register of suspicious transactions
18. Notifying the Authority during an investigation
19. Receipt of report by the Authority

PART IV
COMPLEX TRANSACTIONS OR UNUSUAL TRANSACTIONS

20. Responsibility relating to complex transactions or unusual transactions
21. Transaction monitoring

PART V
COMPLIANCE OFFICER

22. Appointment of Compliance Officer
23. Resources and size of compliance function
24. Appointment of an alternate Compliance Officer
25. Role and responsibilities of a Compliance Officer
26. Reports of Compliance Officer

PART VI
PROGRAMMES AGAINST MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING

27. Responsibility relating to programmes against money laundering, terrorist financing and proliferation financing
28. Screening procedures when hiring employees
29. Staff training

PART VII
CUSTOMER IDENTITY AND CUSTOMER DUE DILIGENCE

30. Obligation to identify customer
31. Beneficiary of life insurance
32. Prior customer verification
33. Obligation when unable to comply with customer due diligence
34. Verification not required
35. Enhanced due diligence procedures
36. Correspondent banks
37. New technologies
38. Identification and record-keeping requirements relating wire transfers
39. Ordering financial institutions
40. Intermediary financial institutions
41. Beneficiary financial institution
42. Identification and record-keeping requirements relating to the transfer of virtual assets

43. Originating virtual asset service provider
44. Intermediary virtual asset service provider
45. Beneficiary virtual asset service provider

PART VIII
FORMS FOR SOURCE OF FUNDS DECLARATION

46. Source of funds declaration by financial institution
47. Source of funds declaration by person engaged in other business activity

PART IX
MISCELLANEOUS

48. Group obligations
49. Reliance on third parties within a financial group
50. Penalty for non-compliance

SCHEDULE

SAINT LUCIA

STATUTORY INSTRUMENT, 2023, No. 53

[24th May, 2023]

In exercise of the power conferred under section 43 of the Money Laundering (Prevention) Act, Cap. 12.20 the Attorney General makes these Regulations:

PRELIMINARY

Citation

1. These Regulations may be cited as the Money Laundering (Prevention) Regulations, 2023.

Interpretation

2. In these Regulations —

"accurate" in relation to identification and record-keeping requirements relating to —

(a) wire transfers, means information that has been verified for accuracy that a financial institution is required to verify the accuracy of the required originator information;

(b) the transfer of virtual assets, means information that has been verified for accuracy that a virtual asset service provider is required to verify the accuracy of the required originator or beneficiary information;

"Act" means the Money Laundering (Prevention) Act, Cap. 12.20;

"batch file" in relation to identification and record-keeping requirements relating to —

(a) wire transfers, means a series of transactions bundled together;

(b) the transfer of virtual assets, means several individual transfers of virtual assets which are bundled together for transmission;

"beneficiary" means —

(a) in relation to wire transfer, the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer; and

(b) in relation to life insurance or another investment linked to an insurance policy, a natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds when an insured event occurs, which is covered by the policy;

"beneficiary financial institution" in relation to identification and record-keeping requirements relating to wire transfers, means a financial institution which receives the wire transfer from the ordering financial institution directly or through an intermediary financial institution and makes the funds available to the beneficiary;

"beneficiary virtual asset service provider" means a virtual asset service provider which receives a transfer of virtual assets on behalf of a beneficiary;

"business relationship" means an arrangement between a person and a financial institution or person engaged in other business activity, the purpose of which is to facilitate the carrying out of financial and other related transactions on a regular basis;

"cash" includes —

(a) notes and coins in any currency that is designated as legal tender;

(b) postal orders;

(c) cheques of any kind, such as, traveller's cheques;

(d) banker's drafts;

(e) electronic cash;

(f) bearer bonds and bearer shares;

(g) gaming vouchers;

(h) betting receipts;

(i) fixed value gaming and casino tokens;

(j) any other bearer negotiable instruments;

"correspondent bank" means the bank that provides banking service to a respondent bank;

"correspondent banking" means the provision of a banking service by a correspondent bank to a respondent bank;

"customer" means an applicant for business, a person with whom a financial institution or person engaged in other business activity has a business relationship, or a person seeking to engage in a one-off transaction;

"customer due diligence" includes —

(a) undertaking measures for —

(i) identifying and verifying the identity of the customer,

(ii) identifying and verifying the identity of the beneficial owner,

(iii) obtaining information on the purpose and intended nature of a business relationship,

(iv) establishing, as appropriate, the source of funds and source of wealth of a customer or beneficial owner, and

(v) applying paragraphs (i) and (iv) to existing customers on the basis of materiality and risk; at appropriate times taking into account whether and when the measures had previously been applied to the customer and the adequacy of the data collected;

(b) ongoing due diligence;

"enhanced due diligence" means —

(a) the extended customer due diligence procedures, where appropriate, that are part of the customer acceptance process of a financial institution or person engaged in other business activity; or

(b) the intensified monitoring of accounts that are appropriate where a customer is or becomes a high-risk person, or a politically exposed person;

"intermediary financial institution" in relation to identification and record-keeping requirements relating to wire transfers, 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;

"intermediary virtual asset service provider" means a virtual asset service provider that receives and transfers virtual assets on behalf of the originating virtual asset service provider and the beneficiary virtual asset service provider, or another intermediary;

"key staff" means an employee of a financial institution or person engaged in other business activity who deals with customers and the transactions of the customers;

"legal arrangement" means a trust or partnership or other similar legal arrangements created between parties which lack separate legal personality;

"legal person" means an entity other than a natural person that establishes a permanent customer relationship with a financial institution or person engaged in other business activity or otherwise own property;

"licensed financial institution" means a financial institution licensed to carry on banking business under the Banking Act, Cap. 12.01;

"one-off transaction" means a transaction other than a transaction carried out in the course of an existing business relationship;

"ongoing due diligence" means conducting ongoing monitoring of a business relationship and scrutiny of transactions throughout the course of the relationship to ensure that the transactions being conducted are

consistent with the financial institution or person engaged in other business activity's knowledge of the customer, the business and risk profile, including where necessary, the customer's source of funds and source of wealth, and keeping the information obtained up-to-date and relevant, especially for high-risk customers and politically exposed persons;

"ordering financial institution" in relation to identification and record-keeping requirements relating to wire transfers, means a financial institution which initiates the wire transfer and transfers the funds on receiving the request for a wire transfer on behalf of the originator;

"originating virtual asset service provider" means a virtual asset service provider which conducts a transfer of virtual assets on behalf of an originator;

"physical presence" means meaningful mind and management located within a country and does not include mere presence of a local agent or low-level staff;

"proliferation financing" means the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and means of delivery and related materials including both technologies and dual-use goods used for non-legitimate purposes, in contravention of the United Nations Sanctions (Counter-Proliferation Financing) Act, Cap. 12.30 or, where applicable, international obligations;

"respondent bank" means a bank that receives banking services from a correspondent 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 group that is subject to consolidated supervision;

"verification subject" means an applicant for business, customer, beneficial owner, or a person on whose behalf a transaction is being performed;

"virtual asset service provider" —

(a) has the meaning assigned under the Virtual Asset Business Act, No. 24 of 2022; or

(b) a financial institution which conducts a virtual asset business.

Application

3. These Regulations apply to the prevention measures under Part 3 of the Act.

PART I
ESTABLISHMENT AND MAINTENANCE OF RECORDS

Responsibility relating to establishment and maintenance of records

4. A financial institution or person engaged in other business activity shall, in accordance with section 16(1)(a) and (b) of the Act as it relates to the establishment and maintenance of records comply with regulations 5 to 9.

Records on the identity and transactions of customers

5.—(1) Where a business relationship has been established, the financial institution or person engaged in other business activity shall maintain all relevant records on the identity and transactions of customers, for seven years, or longer if required by the Authority.

(2) Where a business relationship has been terminated, all relevant records on the identity and transactions of the customer must be retained for a period of seven years after termination.

Maintenance of records in retrievable form

6.—(1) Records must be maintained in retrievable form in accordance with section 16(8) of the Act.

(2) In subregulation (1), retrievable form includes —

(a) an original hard copy;

(b) notarized or certified copies of the original; or

(c) computerized or electronic form.

(2) Records held by third parties are not regarded as being in a readily retrievable form unless the financial institution or person engaged in other business activity is reasonably satisfied that the third party is itself an institution which is able and willing to keep such records and disclose the records to the financial institution or person engaged in other business activity when required.

Provision of records to the Authority

7. Where the Authority requires sight of records which according to a financial institution or person engaged in other business activity's policies and procedures would ordinarily have been destroyed, the financial institution or person engaged in other business activity is nonetheless required to conduct a search for those records and provide as much detail to the Authority as possible.

Request to keep records

8.—(1) Where an investigation into a suspicious customer or a suspicious transaction has been initiated, the Authority may request a financial institution or person engaged in other business activity to keep records until further notice, notwithstanding that the retention period of seven years under section 16(1)(a) of the Act has elapsed.

(2) In the absence of a request under subregulation (1), where a financial institution or person engaged in other business activity knows that an investigation is proceeding in respect of a customer, the financial institution or person engaged in other business activity shall not, without the prior approval of the Authority, destroy any relevant records notwithstanding that the retention period of seven years under section 19(1)(a) of the Act has elapsed.

Records in relation to transactions, verification and training

9.—(1) A financial institution or person engaged in other business activity shall keep records in relation to transactions and verification in such a manner that allows the financial institution or person engaged in other business activity to comply expeditiously with information requests from the Authority.

(2) Records under subregulation (1) must comprise —

(a) a description of the nature of all the evidence received in relation to the identity of the subject for verification;

(b) the evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy; and

(c) details relating to all transactions which is sufficient to permit reconstruction of individual transactions.

(3) Without prejudice to subregulation (1), a financial institution or person engaged in other business activity shall keep records in relation to all training conducted by the financial institution or person engaged in other business activity, in relation to money laundering, terrorist financing and proliferation financing

(4) Records under subregulation (3) must comprise —

(a) details and contents of the training programme;

(b) target audience of training;

(c) names of staff attending training;

(d) dates of training sessions; and

(e) assessment methods and results, where applicable.

PART II
INTERNAL POLICIES, PROCEDURES AND CONTROLS

Responsibility relating to internal policies, procedures and controls

10. A financial institution or person engaged in other business activity shall, in accordance with section 16(1)(g) develop and apply internal policies, procedures or controls, comply with regulations 11 and 12.

Development and application of internal policies, procedures or controls

11.—(1) In developing internal policies, procedures or controls to combat money laundering, terrorist financing and proliferation financing under section 16(1)(g) of the Act, a financial institution

or person engaged in other business activity shall develop internal policies, procedures or controls that are —

(a) approved by —

(i) in the case of a legal person and in accordance with section 16(1)(g) of the Act, senior management or the board of directors, and

(ii) in any other case, the owner or managing director;

(b) signed by —

(i) in the case of a legal person, the board of directors, and

(ii) in any other case, the owner or managing director;

(c) clearly and accurately documented; and

(d) updated to reflect changes, when necessary.

(2) In applying the internal policies, procedures or controls under section 16(1)(g) of the Act, a financial institution or person engaged in other business activity must apply internal policies, procedures or controls that include —

(a) customer due diligence under Part VII;

(b) enhanced due diligence procedures for new and ongoing business relationships and transactions under regulation 35;

(c) electronic funds transfer procedures;

(d) internal reporting procedures under section 19 of the Act;

(e) procedures for reporting suspicious activities and transactions;

(f) record keeping procedures in accordance with the requirements of the Act;

(g) appropriate measures to conduct a risk assessment of its operations in relation to money laundering, terrorist financing and proliferation financing;

(h) internal controls and procedures that are appropriate in view of the nature of business, money laundering and terrorist financing risk profile of the entity identified through the risk assessment;

(i) training requirements;

(j) taking appropriate measures for key staff to be —

(i) made aware of the provisions of the Act, Proceeds of Crime Act, Cap. 3.04, Anti-Terrorism Act, Cap. 3.16, United Nations (Counter Proliferation Financing) Act, Cap. 12.30 and these Regulations and the internal policies, procedures and controls for detecting and preventing money laundering, terrorist and proliferation financing,

(ii) trained in recognizing and dealing with transactions or activities which may be related to money laundering, terrorist financing and proliferation financing,

(iii) continuously trained and supervised, in order to ensure adequate competence with regard to the functions under subparagraphs (i) and (ii).

Audit for compliance

12. A financial institution or person engaged in other business activity shall, in accordance with section 16(1)(j) as it relates to audits for compliance, comply with regulation 13.

Independent audit

13.—(1) An independent audit must be conducted at least annually, with a professional retained specifically for that purpose or a suitably qualified internal auditor who is not involved in the compliance function of the financial institution or person engaged in other business activity.

(2) An independent audit must assess the policies, procedures and controls of the financial institution or person engaged in other business activity for compliance with the Act, Regulations, guidelines issued by the Authority or the Central Bank and the existing policy manual of the financial institution or person engaged in other business activity and as a measure of the effectiveness of the work being done by a Compliance Officer.

(3) An independent audit must include at a minimum —

(a) ensuring the anti-money laundering, counter terrorist and proliferation financing policies, procedures and controls are adequate and commensurate with the financial institution or person engaged in other business activity's risk assessment;

(b) testing of internal procedures for employee evaluation with respect to integrity, personal employment and financial history;

(c) evaluating of the extent and frequency of training received by employees and an assessment of the appropriateness of the training content;

(d) testing of employees' knowledge of anti-money laundering, counter terrorist and proliferation financing procedures;

(e) reviewing transactions for possible suspicious transactions, including a comparison of those transactions with reports submitted on those transactions;

(f) reviewing transactions for possible suspicious transactions;

(g) testing of record keeping of all suspicious activity reports, identification documentation of customers, beneficial owners and transaction records.

(h) assessing compliance by the financial institution or person engaged in other business activity with established policies, procedures and processes;

(i) assessing the process for identifying and reporting suspicious activities;

(j) assessing the information systems and processes which supports the established compliance programme of the financial institution or person engaged in other business activity.

(4) The findings of an independent audit must be documented, and violations of the law and anti-money laundering, counter terrorist and proliferation financing procedures must be immediately reported to the board of directors.

(5) A financial institution or person engaged in other business activity must have written audit procedures for assessing compliance with anti-money laundering, counter terrorist and proliferation financing legislation and guidelines that must be reviewed on an ongoing basis in order to ensure usefulness.

PART III
SUSPICIOUS TRANSACTION REPORTING

Responsibility relating to suspicious transaction reporting

14. A financial institution or person engaged in other business activity shall, in order to carry out the responsibilities under section 16(1)(k) as it relates to reporting of suspicious transactions, comply with regulations 15 to 19.

Internal reporting of suspicious transactions

15.—(1) Key staff, including senior management, shall —

(a) report a suspicious transaction to the Compliance Officer; and

(b) provide in a report made under paragraph (a) details of the information giving rise to any knowledge or reasonable grounds for the suspicion held, including the full details of the customer.

(2) The requirement to report a suspicious activity or transaction under subregulation (1) includes the reporting of any attempted activity or transaction that the financial institution or person engaged in other business activity has turned away.

(3) Except where regulation 31 applies, for the purposes of subregulations (1) and (2), a report must be made in circumstances where an applicant for business or a customer fails to provide adequate information or supporting evidence to verify his or her identity or, in the case of a legal person, the identity of any beneficial owner.

(4) A Compliance Officer shall, on receipt of an internal report concerning a suspicious activity or transaction, investigate the details of the report and determine whether —

(a) the information contained in the report supports the suspicion; and

(b) there is the need under the circumstances to submit a report to the Authority.

(5) Where a Compliance Officer decides that the information does not substantiate a suspicion of money laundering, terrorist financing or proliferation financing, the Compliance Officer shall —

(a) record that decision, outlining the nature of the information to which the suspicious transaction relates, the date he or she received the information, the full name of the person who provided him or her with the information and the date he or she took the decision that the information did not substantiate a suspicion of money laundering or other criminal conduct;

(b) state the reason for his or her decision; and

(c) make the record for his or her decision available to the Authority on request.

(6) Where a Compliance Officer is uncertain as to whether the details of the report received by him or her substantiate the suspicion, he or she shall make a report of the suspicious transaction to the Authority.

(7) For the purposes of this regulation, a financial institution or person engaged in other business activity shall provide a Compliance Officer with reasonable access to all relevant information which may be of assistance to him or her and which is available to the financial institution or person engaged in other business activity.

Reporting of suspicious transactions to the Authority

16.—(1) A Compliance Officer shall make a report to the Authority of a suspicious transaction or attempted transaction relating to money laundering or other criminal conduct.

(2) A report of a suspicious transaction made under subregulation (1) must be in Form 1 of the Schedule.

(3) A report under this regulation must be delivered in sealed and confidential envelopes by hand.

Register of suspicious transactions

17.—(1) A Compliance Officer shall maintain a register of all suspicious transaction reports made to the Authority under regulation 16.

(2) Notwithstanding subregulation (1), registers shall be kept by the Compliance Officer in relation to all internal reports of suspicious transactions received, including the details for his or her decision not to report to the Authority.

(3) A register under subregulations (1) and (2) must contain details of —

(a) the date of the report;

(b) the person who made the report;

(c) the person to whom the report was forwarded;

(d) a reference by which supporting evidence is identifiable; and

(e) the receipt of acknowledgement from the Authority.

(4) A register shall be kept in relation to all enquiries made by the Authority.

(5) A register under subregulation (4) must be separate from other records and contain at a minimum —

(a) the date and nature of the enquiry; and

(b) the details of the customer or account involved.

Notifying the Authority during an investigation

18. Where a Compliance Officer considers a suspicion to be urgent, including, if the subject of the suspicious transaction is part of a current investigation, the Compliance Officer shall immediately notify the Authority.

Receipt of report by the Authority

19.—(1) The receipt of suspicious transaction reports shall be acknowledged by the Authority.

(2) The Authority may obtain information from a financial institution or person engaged in other business activity and other sources whether or not a suspicious transaction report has been made by a financial institution or person engaged in other business activity.

PART IV
COMPLEX TRANSACTIONS OR UNUSUAL TRANSACTIONS

Responsibility relating to complex transactions or unusual transactions

20. A financial institution or person engaged in other business activity shall, in order to carry out the responsibility under section 16(1)(m) of the Act as it relates to complex transactions or unusual transactions, comply with transaction monitoring under regulation 21.

Transaction monitoring

21.—(1) A financial institution or person engaged in other business activity shall monitor complex transactions, unusual or large transactions, or unusual patterns of transactions, whether completed or not.

(2) Transaction monitoring under subregulation (1) must be risk based and account reviews must be carried out on an ongoing basis.

(3) Where a transaction is inconsistent in amount, origin, destination or type with a client's known, legitimate business or personal activities or has no apparent economic or visible lawful purpose, the transaction must be considered unusual and the financial institution or person engaged in other business activity is to be put on enquiry as to whether the business relationship is being used for money laundering, terrorist or proliferation financing.

(4) Where a financial institution or person engaged in other business activity observes unusual or complex activity in relation to a client's account, the financial institution or person engaged in other business activity shall make inquiries as to the nature of the activity or transaction and make a written record of its analysis or findings in relation to the unusual or complex activities and the written record is to be made available to the Authority on request.

PART V
COMPLIANCE OFFICER

Appointment of a Compliance Officer

22.—(1) In appointing a Compliance Officer under section 16(1)(n) of the Act, a financial institution or person engaged in other business activity shall appoint a person who —

(a) is at the management level in accordance with section 16(1)(n) of the Act;

(b) is fit and proper in accordance with section 16(1)(n), and at a minimum, he or she shall —

(i) not have been convicted of an offence involving drug trafficking, money laundering, terrorist financing, dishonesty or any other financial crime, or be an undischarged bankrupt,

(ii) have the appropriate character, antecedents, habits, associations and public reputation;

(c) possesses the trust and confidence of the management and staff;

(d) has sufficient anti-money laundering, counter terrorist and proliferation financing knowledge or qualifications, in addition to knowledge of the financial institution's or person engaged in other business activity's products, services and systems;

(e) has access to all relevant information throughout the organization;

(f) maintains the trust and confidence of the enforcement and supervisory agencies;

(g) is adequately versed with the Act, these Regulations and guidelines, the Proceeds of Crime Act, Cap. 3.04, Anti-Terrorism Act, Cap. 3.16 and the United Nations Sanction (Counter-Proliferation Financing) Act, Cap. 12.30.

(2) A financial institution or person engaged in other business activity shall inform all staff at the financial institution or person engaged in other business activity of the identity of the Compliance Officer.

(3) A financial institution or person engaged in other business activity shall submit on the Compliance Officer to the Authority and in the case of a licensed financial institution to the Central Bank and the Authority within seven days of his or her appointment the following details —

(a) completed Compliance Officer Form that must be in Form 2 of the Schedule;

(b) job descriptions for all positions currently held within the financial institution or person engaged in other business activity;

(c) current resume.

(4) Subject to this regulation, with the approval of the Authority, very small reporting entities may appoint an individual to perform a dual function, which includes the role of a Compliance Officer.

Resources and size of the compliance function

23. The resources and size of the compliance function, including, the number of compliance staff, must be commensurate with the size of the operation and risk of the financial institution or person engaged in other business activity.

Appointment of an alternate Compliance Officer

24.—(1) A financial institution or person engaged in other business activity shall appoint an alternate Compliance Officer.

(2) Where the Compliance Officer is absent, whether due to illness, vacation leave, resignation or other reason, the alternate Compliance Officer shall carry out the functions of the Compliance Officer.

(3) An alternate Compliance Officer shall possess relevant professional qualities or experience and have a comprehensive understanding of the legal and institutional expectations of the role.

(4) A Compliance Officer and an alternate Compliance Officer shall not be absent at the same time.

Role and responsibilities of a Compliance Officer

25.—(1) A Compliance Officer shall be —

(a) independent and accountable and report directly to the Board of Directors, where possible, and in the absence of a Board of Directors, the General Manager or owners;

(b) the central point of contact —

(i) for the Authority, or

(ii) in the case of a licensed financial institution, for the Central Bank and the Authority;

(c) separate from the day-to-day activities and operational aspects of the business.

(2) A Compliance Officer shall at a minimum —

(a) establish and implement policies, procedures and controls as may be necessary to combat money laundering, terrorist financing and proliferation financing including —

(i) organizing training sessions for staff on various compliance related issues and instructing employees as to their responsibilities in respect of the provisions of the Act, the Proceeds of Crime Act, Cap. 3.04 Anti-Terrorism Act, Cap. 3.16 and United Nations Sanction (Counter-Proliferation Financing) Act, Cap. 12.30,

(ii) the establishment or review of procedures to ensure high standards of integrity for employees,

(iii) the development or review of a system to evaluate the personal employment and financial history of staff;

(b) make modifications or adjustments to policies, procedures and controls under paragraph (a) that are necessary;

(c) arrange for independent audits under regulation 13 in order to assess the extent to which the policies, procedures and controls under regulation 11 are being complied with;

(d) analyze transactions and verify whether any of them are subject to reporting, in accordance with the relevant laws;

(e) review all internally reported unusual transaction reports on completeness and accuracy with other sources;

(f) prepare and compile suspicious transaction reports of unusual transactions to the Authority;

(g) undertake closer investigations in respect of unusual or suspicious transactions, as directed by the Authority;

(h) undertake tests of the policies, procedures or controls and, where high-risks are identified, enhance the policies, procedures or controls to manage and mitigate the risk and in carrying out this test, the Compliance Officer must have the following information included in his or her working papers, at a minimum —

(i) the date the work was performed,

(ii) the rationale or method of selecting the sample,

(iii) an adequate narrative on the sample selected, including for testing the adequacy of customer identification, the name of the individual, customer number, means of identification used and any associated number or any other related matter,

(iv) the deficiencies noted,

(v) corrective action recommended or taken;

(i) undertake transaction testing and monitoring;

(j) prepare monthly reports to senior management for the purpose of providing information on existing or potential areas in which deficiencies were identified as part of the risk-based monitoring programme of the anti-money laundering, counter terrorist and proliferation financing controls of the financial institution or person engaged in other business activity and the corrective actions implemented or required to be implemented in order to rectify the situation;

(k) to exercise control and review the performance of lower-level compliance staff within the organization or within each branch or unit;

(l) to function as the authorized contact with the Authority for matters of financial intelligence in nature including investigations and requests for information;

(m) to conduct a risk assessment in accordance with sections 14I and 16B of the Act;

(n) implement any recommendations of the Authority or in the case of a licensed financial institution, the Central Bank, and report on any remediation actions to the Authority or in the case of a licensed financial institution, the Central Bank;

(o) to remain informed of the local and international developments on money laundering, terrorist and proliferation financing.

(3) Where the various responsibilities under this regulation are performed by different members of the compliance staff, the authorized contact under subregulation (2)(l) is the individual who is assigned the responsibilities under subregulation (2)(f) and (g).

(4) A Compliance Officer shall be cognizant of the requirements of confidentiality regarding money laundering, terrorist and proliferation financing reports and investigations and shall receive reports from key staff, of any information or matter giving rise to some knowledge of or a suspicion that money laundering or other criminal conduct is taking place.

Reports of Compliance Officer

26.—(1) A Compliance Officer shall submit reports to the board of directors at least quarterly.

(2) A report under subregulation (1) must include —

(a) changes made or recommended in respect of new legislation;

(b) serious compliance deficiencies that have been identified relating to current policies and procedures, indicating the seriousness of the issues and the action taken, or recommendations for change;

(c) a risk assessment of any new types of products and services, or any new channels for distributing them and the money laundering, terrorist and proliferation financing compliance measures that have either been implemented or are recommended;

(d) the means by which the effectiveness of ongoing procedures have been tested;

(e) the number of internal reports that have been received from each separate division, product, area, subsidiary or other matter;

(f) the percentage of those reports submitted to the Authority;

(g) any perceived deficiencies in the reporting procedures and any changes implemented or recommended;

(h) findings from independent assessments and examinations;

(i) information on the implementation of any remedial action issued by the Authority or in the case of a licensed financial institution, the Central Bank;

(j) information identifying staff training during the period, the method of training and any significant issues arising out of the training;

(k) recommendations concerning resource requirements to ensure effective compliance.

PART VI
PROGRAMMES AGAINST MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING

Responsibility relating to programmes against money laundering, terrorist financing and proliferation financing

27. A financial institution or person engaged in other business activity shall, in accordance with section 16(1)(o), comply with regulations 28 and 29.

Screening procedures when hiring employees

28.—(1) In developing programmes against money laundering and terrorist financing including developing internal policies, procedures

and controls for adequate screening procedures to ensure high standards when hiring employees under section 16(1)(o)(i) of the Act, a financial institution or person engaged in other business activity shall cause verification work on a potential employee to be performed prior to an offer of employment.

(2) Verification work under subregulation (1) includes —

(a) reference checks;

(b) checking the authenticity of academic qualifications; and

(c) obtaining a police certificate of character.

(3) A financial institution or person engaged in other business activity shall establish and implement procedures to ensure high standards of integrity among employees that —

(a) includes a code of ethics for the conduct of all employees;

(b) allows for regular reviews of employees' performance and their compliance with established rules and standards, as well as provide for disciplinary action in the event of breaches of these rules;

(c) includes paying attention to employees whose lifestyles are not supported by his or her salary; and

(d) expressly provides for special investigation of employees who are associated with mysterious disappearances or unexplained shortages of funds.

Staff training

29.—(1) A financial institution or person engaged in other business activity shall, under section 16(1)(o)(ii) provide education and training for all of its directors or all other persons involved in its management and staff.

(2) Training must be provided to all staff within thirty days of appointment.

(3) The content of training must be sufficient for awareness of —

(a) the Act, these Regulations, the Anti-Terrorism Act, Cap. 3.16, the United Nations Sanctions (Counter-Proliferation Financing) Act, Cap. 12.30 and any other enactment

relating to money laundering, terrorist financing and proliferation financing;

(b) any guidelines and instructions issued by the Authority or in the case of a licensed financial institution, the Central Bank;

(c) the relevant regional and international conventions, United Nations Security Council Resolutions and standards of compliance established from by the Caribbean Financial Action Task Force, Financial Action Task Force and other organizations of which Saint Lucia is a member or in which Saint Lucia holds associate or observer status, relating to money laundering, terrorist financing and proliferation financing;

(d) obligations under the enactments and instruments under paragraphs (a) and (c), both personal and those of the financial institution or person engaged in other business activity;

(e) the roles and responsibilities in the financial institution or person engaged in other business activity the staff undertakes and this training must be commensurate with the roles and responsibilities;

(f) the manual containing the anti-money laundering, counter terrorist and proliferation financing policies, procedures and internal controls of the financial institution or person engaged in other business activity;

(g) a description of the nature and processes of money laundering, terrorist financing and proliferation financing;

(h) the recognition and handling of suspicious transactions, including their personal liability for failure to report information or suspicions;

(i) customer identification, record keeping and other procedures.

(4) A financial institution or person engaged in other business activity shall conduct training on such frequent basis as it may determine, but in any case, at least once each year.

(5) A financial institution or person engaged in other business activity shall provide more extensive initial and continuing training to the Compliance Officer than that provided to other persons.

PART VII
CUSTOMER IDENTITY AND CUSTOMER DUE DILIGENCE

Obligation to identify customer

30.— (1) A financial institution or person engaged in other business activity shall —

(a) identify a customer, whether a customer has an established business relationship or a one-off transaction, and whether a natural, legal person or legal arrangement and shall verify the customer's identity using reliable, independent source documents, data or information;

(b) subject to paragraph (a), verify that a person purporting to act on behalf of a customer is properly authorized and verify the identity of the person;

(c) identify a beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from reliable sources so as to be satisfied of the identity of the beneficial owner;

(d) for the purposes of paragraphs (a) to (c), obtain information regarding a customer's principal residential address and occupation;

(e) understand and obtain information on, the purpose and intended nature of a business relationship; and

(f) establish procedures and controls to address all risks including risks associated with identifying and verifying non-face-to-face business relationships and transactions and specific and effective customer due diligence in respect of non-face-to-face customers;

(g) conduct ongoing due diligence on a business relationship including —

(i) scrutinising transactions undertaken throughout the course of the business relationship to ensure that

transactions being conducted are consistent with the financial institution or person engaged in other business activity's knowledge of the customer, the customer's business and risk profile, including where necessary, the customer's source of funds; and

(ii) ensuring that documents, data or information collected during customer due diligence is kept current and relevant to customer due diligence, by reviewing existing records on a risk sensitive basis, taking into account whether and when customer due diligence measures have been previously undertaken, the rating applied to various categories of customers, the approved frequency to facilitate the reviews of customer due diligence information with increased frequency of reviews for higher risk categories of customers.

(2) Without prejudice to subregulation (1)(a), for customers that are legal persons or legal arrangements, a financial institution or person engaged in other business activity shall —

(a) understand the ownership and control structure of the customer and the nature of the customer's business;

(b) identify the customer and verify the identity of the customer by means of the following information —

(i) name, legal form and proof of existence,

(ii) the constitutional documents that regulate and bind the legal person or legal arrangement,

(iii) satisfactory evidence of the identity of the director, manager, general partner, president, chief executive officer or such other person who is in an equivalent senior management position in the legal person or legal arrangement;

(iv) any authorized signatories not captured in paragraph (iii),

(v) the address of the registered office and, if different, a principal place of business.

(3) Without prejudice to subregulation (1)(c) and (2), for customers that are legal arrangements, a financial institution or person engaged in other business activity shall identify and take reasonable measures to verify the identity of beneficial owners by means of the following information —

(a) in the case of trusts, the identity of the settlor, the trustee, 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; or

(b) in the case of other types of legal arrangements, the identity of persons in equivalent or similar positions.

Beneficiary of life insurance

31.—(1) Without prejudice to the customer due diligence measures required under the Act and these Regulations for the customer and the beneficial owner, a financial institution or person engaged in other business activity shall conduct, on the beneficiary of life insurance and other investment related insurance policies, as soon as the beneficiary is identified or designated and shall do so no later than at the time of the pay out, the following customer due diligence measures—

(a) in the case of a beneficiary that is identified as a specifically named natural or legal person or legal arrangement, taking the name of the person; and

(b) in the case of a beneficiary that is designated by characteristics or by class or by other means, obtaining sufficient information concerning the beneficiary to satisfy the financial institution or person engaged in other business activity that it will be able to establish the identity of the beneficiary at the time of the pay out; and

(c) in the case of a beneficiary under paragraph (a) or (b), verifying the identity of the beneficiary.

(2) A financial institution or person engaged in other business activity shall include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced customer due diligence measures are applicable.

(3) A financial institution or person engaged in other business activity shall take enhanced due diligence measures which must include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary at the time of pay-out if it determines that a beneficiary who is a legal person or a legal arrangement presents a high risk.

(4) A financial institution or person engaged in other business activity shall, at the time of the pay-out, take reasonable measures to determine whether the beneficiary and, where required, the beneficial owner of the beneficiary are politically exposed persons.

(5) Where high risks are detected in relation to a politically exposed person identified under sub regulation (4), the financial institution or person engaged in other business activity shall inform senior management before the pay-out of the policy proceeds and senior management shall conduct enhanced due diligence on the business relationship with the policyholder and, if necessary, consider making a suspicious transaction report.

Prior customer verification

32.—(1) A financial institution or person engaged in other business activity shall adopt risk management procedures concerning the conditions under which a customer may utilize a business relationship prior to verification under regulation 30.

(2) Conditions under subregulation (1) include —

(a) measures which place a limitation on the number, types and amount of transactions that customer may conduct;

(b) requiring management approval before the business relationship is established; and

(c) measures which require the monitoring of a large, complex or unusual transaction which the entity considers not to be normal for the business relationship.

Obligation when unable to comply with customer due diligence

33. Subject to regulation 32, where a financial institution or person engaged in other business activity is unable to obtain information required by these Regulations to satisfy relevant customer due diligence

measures, the financial institution or person engaged in other business activity shall —

(a) not open the account, commence business relations or perform the transaction;

(b) terminate the business relationship; and

(c) consider making a suspicious transaction report in relation to the customer.

Verification not required

34.—(1) Unless a transaction is a suspicious transaction, customer due diligence regarding verification of the identity of a customer or an applicant for business are not required where the customer or applicant for business is —

(a) a central or local government organization, statutory body or agency of government;

(b) a company, that is listed on a recognized stock exchange and subject to disclosure requirements which impose requirements to ensure adequate transparency of beneficial ownership, or majority-owned subsidiary of the company.

(2) A financial institution or person engaged in other business activity shall not verify the identity of an applicant for business, or the beneficial owner where a business relationship is formed or a one-off transaction is carried out with, or for an applicant for business pursuant to an introduction effected by a financial institution or person engaged in other business activity and who, on that introduction, provides a written assurance to the financial institution or person engaged in other business activity which confirms —

(a) the identity of the applicant for business, and the identity of the beneficial owner, if applicable, of the applicant for business;

(b) the nature and intended purpose of the business relationship;

(c) that the introducer has identified and verified the identity of the applicant for business, and, where required, the beneficial owner of the applicant for business, under procedures maintained by the introducer in accordance with applicable laws;

(d) that the introducer has identified the source of the funds of the applicant for business; and

(e) that the introducer shall make available on request and without delay, copies of identification and verification data and any other relevant documentation relating to customer due diligence in respect of the applicant for business and, where applicable, the beneficial owner of the applicant for business.

(3) A financial institution or person engaged in other business activity who relies on an introduction effected under subregulation (2) in respect of an applicant for business, is liable for any failure of the introducer to obtain and record satisfactory identification and verification documentation, or to make the record available on request and without delay.

(4) The ultimate responsibility for compliance with the customer due diligence requirements is that of the financial institution or person engaged in other business activity who relies on an introduction under subregulation (2).

Enhanced due diligence procedures

35.—(1) A financial institution or person engaged in other business activity shall perform enhanced due diligence —

(a) in relation to business relationships and transactions where a higher risk of money laundering, terrorist financing and proliferation financing has been identified by the financial institution or person engaged in other business activity or through supervisory or national guidance;

(b) where a customer, transaction or an applicant for business is from a foreign country that has been identified by credible sources as having serious deficiencies in its anti-money laundering, counter terrorist and proliferation financing regime or a prevalence of corruption;

(c) in relation to correspondent banking relationships, under regulation 36;

(d) in the event of an unusual or suspicious transaction; or

(e) in relation to business relationships and transactions with persons, including reporting entities, from countries for which enhanced due diligence is requested by the Financial Action Task Force.

(2) Enhanced due diligence procedures under subregulation (1) must include —

(a) having appropriate risk management systems to determine whether the customer or potential customer is a high risk;

(b) developing a clear policy and internal guidelines, procedures and controls for the identification, enhanced due diligence requirements and ongoing monitoring procedures for high risk transactions and customers;

(c) obtaining senior management approval for the commencement of business relationships with such customers or to continue business relationships with those who are found to be or subsequently become high risk;

(d) taking reasonable measures to establish source of wealth and source of funds, and

(e) ensuring the proactive monitoring of activity on such accounts and transactions, so as to identify indicators of activities which may be unscrupulous or corrupt.

Correspondent banks

36.—(1) A financial institution shall gather sufficient information from and perform enhanced due diligence prior to setting up correspondent banking relationships or other similar relationships including —

(a) obtaining authenticated or certified copies of Certificates of Incorporation and Articles of Incorporation and other company documents to show registration of the institution within its identified jurisdiction of residence;

(b) obtaining authenticated or certified copies of banking licenses or similar authorization documents, and additional licenses to deal in foreign exchange;

(c) determining the supervisory authority which has oversight responsibility for the respondent bank;

(d) determining the ownership of the financial institution;

(e) obtaining details of the board and management composition of the respondent bank;

(f) determining the location and major activities of the financial institution;

(g) obtaining details regarding the group structure within which the respondent bank falls and subsidiaries of the respondent bank;

(h) obtaining proof of years of operation, and access to audited financial statements for five years, if possible;

(i) information as to the external auditors;

(j) ascertaining if the bank has established and implemented sound customer due diligence, anti-money laundering, counter terrorist and proliferation financing policies and strategies, appointed a Compliance Officer, at managerial level, and included a copy of its anti-money laundering, counter terrorist and proliferation financing policy and guidelines;

(k) cautioning to be exercised by correspondent bank, that shall be cautious while continuing relationships with correspondent banks located in countries with poor customer due diligence standards and procedures and countries identified as non-cooperative in the fight against money laundering and terrorist financing;

(l) ascertaining whether the correspondent bank, in the last seven years from the date of the commencement of the business relationship or negotiations, has been the subject of, or is currently subject to any regulatory action or any money laundering, terrorist or proliferation financing prosecutions or investigations;

(m) requiring confirmation that the foreign corresponding bank do not permit their accounts to be used by shell banks,

i.e. the bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regular financial group;

(n) establishing the purpose of the correspondent account;

(o) documenting the respective anti-money laundering, counter terrorist and proliferation financing responsibilities of each institution in the operation of the corresponding account;

(p) identifying any third parties that may use the correspondent banking services;

(q) ensuring that the approval of senior management is obtained for the account to be opened;

(r) in the case of the correspondent bank, examining and satisfying itself that the respondent bank has verified the identity of the customers having direct access to the accounts and are subject to checks under 'due diligence' on an on-going basis;

(s) causing the respondent bank to provide the relevant customer identification data immediately on request;

(t) documenting the anti-money laundering, counter terrorist and proliferation financing responsibility of each institution.

(2) A local bank that provides correspondent banking services to foreign banks and has banking relationships with overseas financing institutions shall adopt the procedures under subregulation (1).

(3) A financial institution shall —

(a) not enter into, or continue any correspondent banking relationship with shell banks;

(b) take reasonable measures to satisfy themselves that respondent financial institutions do not permit their accounts to be used by shell banks.

New technologies

37. A financial institution or person engaged in other business activity shall —

(a) assess the money laundering, terrorist and proliferation financing risk that may arise from the development of new products and services and business practices, including new supply channels, and the use of new or developing technologies, relating to both new and pre-existing products;

(b) have policies in place and take measures to prevent the misuse of technology for money laundering, terrorist financing and proliferation financing including policies for the level of verification used to be appropriate to the risk associated with the particular product or service;

(c) undertake the risk assessments prior to the launch or use of such products, practices and technologies and take appropriate measures to manage and mitigate the risks;

(d) carry out ongoing monitoring of the use of new technologies in business relationships that they are engaged in and take appropriate measures to manage and mitigate identified risks.

Identification and record-keeping requirements relating to wire transfers

38. A financial institution or person engaged in other business activity shall, in accordance with section 17(1)(b) undertake customer due diligence measures under regulations 39 to 41.

Ordering financial institutions

39.—(1) In the case of domestic and cross-border wire transfers, an ordering financial institution shall retain records of payments made with sufficient detail to enable it to establish —

(a) accurate originator information, including —

(i) the name of the originator,

(ii) the account number of the originator where such an account is used to process the transaction or, in the

absence of an account, a unique transaction reference number which permits traceability of the transaction, and

(iii) the address of the originator, or national identification number, or customer identification number, or date and place of birth of the originator;

(b) the beneficiary information, including —

(i) the name of the beneficiary,

(ii) the account number of the beneficiary where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

(2) An ordering financial institution shall, where several individual wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, ensure that —

(a) the batch file contains the required and accurate originator and full beneficiary information, that is fully traceable within the beneficiary country; and

(b) the account number or unique transaction reference number of the originator is included in the wire transfer transaction.

(3) An ordering financial institutions shall verify its customer's information where there is a suspicion of money laundering or terrorist financing.

(4) An ordering financial institution shall maintain all originator and beneficiary information collected in accordance with record keeping requirements under the Act.

(5) An ordering financial institution shall not execute a wire transfer that does not comply with the requirements in this regulation.

Intermediary financial institutions

40.—(1) In the case of a cross-border wire transfer, an intermediary financial institution shall ensure that originator and beneficiary information that accompanies a wire transfer is retained with the wire transfer.

(2) An intermediary financial institution shall take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

(3) An intermediary financial institution shall adopt and implement risk-based policies and procedures for determining —

(a) when to execute, reject, or suspend wire transfers lacking required originator or beneficiary information; and

(b) the appropriate follow-up actions.

Beneficiary financial institution

41.—(1) A beneficiary financial institution 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 required originator or beneficiary information;

(b) verify the identity of the beneficiary, if the identity has not been previously verified;

(c) maintain all beneficiary information collected in accordance with record keeping requirements under the Act;

(d) implement risk-based policies and procedures for determining —

(i) when to execute, reject, or suspend a wire transfer lacking required originator or beneficiary information, and

(ii) the appropriate follow-up action.

(2) In the case of a money services business that controls the ordering and beneficiary side of a wire transfer, the money services business shall —

(a) take into account all the information from both the ordering and beneficiary sides in order to determine whether a suspicious activity report has to be filed; and

(b) file a suspicious transaction report in the country affected by the suspicious wire transfer, and make relevant transaction information available to the Authority.

Identification and record-keeping requirements relating to the transfer of virtual assets

42. A financial institution or person engaged in other business activity shall, in accordance with section 17(1)(h), undertake due diligence measures under regulations 43 to 45.

Originating virtual asset service provider

43.—(1) An originating virtual asset service provider shall —

(a) when conducting a transfer of virtual assets to a beneficiary, collect and record the following information —

(i) accurate originator information, including —

(A) the name of the originator;

(B) the account number of the originator where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and

(C) the address of the originator, or national identification number, or customer identification number, or date and place of birth of the originator,

(ii) beneficiary information, including —

(A) the name of the beneficiary,

(B) the account number of the beneficiary where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction;

(b) provide the information under paragraph (a) to the beneficiary virtual asset service provider securely and simultaneously with the transfer of virtual assets;

(c) where several individual virtual asset transfers from a single originator are bundled in a batch file for transmission to beneficiaries, ensure that —

(i) the batch file contains the required and accurate originator and full beneficiary information, that is fully traceable within the beneficiary country, and

(ii) the account number or unique transaction reference number of the originator is included in the wire transfer transaction;

(d) verify information on the customer information where there is a suspicion of money laundering or terrorist financing;

(e) maintain all originator and beneficiary information collected in accordance with record keeping requirements under the Act.

(2) An originating virtual asset service provider shall not execute a transfer of virtual assets if it does not comply with the requirements in this Part.

Intermediary virtual asset service provider

44. An intermediary virtual asset service provider shall —

(a) ensure that all information received on the originator and the beneficiary that accompanies a transfer of virtual assets is kept with the transfer of virtual assets;

(b) take reasonable measures, which are consistent with straight-through processing, to identify transfers of virtual assets that lack required originator information or required beneficiary information;

(c) adopt and implement risk-based policies and procedures for determining —

(i) when to execute, reject or suspend a transfer of virtual assets lacking required originator or beneficiary information,

(ii) the appropriate follow-up actions.

Beneficiary virtual asset service provider

45. A beneficiary virtual asset service provider shall —

(a) on receipt of a transfer of virtual assets, collect and record the following information —

(i) originator information, including —

(A) the name of the originator;

(B) the account number of the originator where such an account is used to process the transfer or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction, and

(ii) accurate beneficiary information, including —

(A) the name of the beneficiary,

(B) the account number of the beneficiary where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction;

(C) the address of the beneficiary, or national identification number, or customer identification number, or date and place of birth of the originator;

(b) verify the identity of the beneficiary, if the identity has not been previously verified;

(c) maintain all beneficiary information collected in accordance with record keeping requirements under the Act;

(d) adopt and implement risk-based policies and procedures for determining —

(i) when to execute, reject, or suspend a transfer of virtual assets lacking required originator or beneficiary information, and

(ii) the appropriate follow-up actions.

(2) A virtual asset service provider that controls the originating and beneficiary side of the transfer of virtual assets, shall —

(a) take into account all the information from both the originating and beneficiary sides in order to determine whether a suspicious transaction report has to be filed; and

(b) file a suspicious transaction report in the country affected by the suspicious transfer of virtual assets, and make relevant transaction information available to the Authority.

PART VIII
FORMS FOR SOURCE OF FUNDS DECLARATION

Source of funds declaration by financial institution

46. For the purposes of section 21(1) of the Act, a source of fund declaration with a financial institution must be in Form 3 of the Schedule.

Source of funds declaration by person engaged in other business activity

47. For the purposes of section 21(1) of the Act, a source of funds declaration by a person engaged in other business activity must be in Form 4 of the Schedule.

PART IX
MISCELLANEOUS

Group obligations

48.—(1) A financial institution or person engaged in other business activity shall, where a group whose headquarters is in Saint Lucia operates branches or controls subsidiaries in another jurisdiction, cause anti-money laundering, counter terrorist and proliferation financing group-wide programmes to be implemented, which must be applicable and appropriate to all branches and majority-owned subsidiaries of the financial group.

(2) The programmes under subregulation (1) must include measures for —

(a) the application of anti-money laundering, counter terrorist and proliferation financing measures by the foreign branches and subsidiaries of a financial institution or person engaged in other business activity, consistent with the requirements of the Act and these Regulations;

(b) that such branches and subsidiaries are informed about current group policy;

(c) that each branch or subsidiary informs itself as to its own local reporting point, equivalent to the Authority in Saint Lucia, and that it is familiar with the procedures for disclosure equivalent to those stated in Form 1 of the Schedule;

(d) that the branch or subsidiary informs the home supervisor when unable to observe appropriate anti-money laundering, counter terrorist and proliferation financing measures because it is prohibited by the laws of the host country;

(e) implementation of policies and procedures for sharing information required for the purposes of customer due diligence and money laundering, terrorist and proliferation financing risk management;

(f) the provision of customer, account, and transaction information from branches and subsidiaries to group-level compliance, audit or anti-money laundering, counter terrorist and proliferation financing functions, when necessary for anti-money laundering, counter terrorist and proliferation financing purposes including information and any analysis of transactions or activities which appear unusual and branches and subsidiaries must receive such information from these group-level functions when relevant and appropriate to risk management;

(g) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off;

(h) where the minimum anti-money laundering, counter terrorist and proliferation financing requirements in the host country in which a foreign branch or subsidiary is located is less strict than the requirements under the Act or these Regulations, the financial institution or person engaged in other business activity shall apply the requirements of the Act and these Regulations to the foreign branch or subsidiary to the extent that the host country laws permit;

(i) where the laws in the host country in which a foreign branch or subsidiary is located does not permit the proper implementation of the Act and these Regulations, a financial institution or person engaged in other business

activity shall apply appropriate measures to manage the money laundering, terrorist and proliferation financing risks of the foreign branch and subsidiary in the group and advise the Authority and in the case of a licensed financial institution, the Central Bank, of the measures taken.

Reliance on third parties within a financial group

49. A financial institution or person engaged in other business activity shall not rely on a third party that is part of the same financial group, unless —

(a) the group applies customer due diligence and record-keeping requirements in accordance with the Act and anti-money laundering, counter terrorist and proliferation financing programmes in accordance with regulation 48;

(b) the implementation of those customer due diligence and record-keeping requirements and anti-money laundering, counter terrorist and proliferation financing programmes is subject to supervision at a group level by the relevant supervisor; and

(c) any higher country risk is adequately mitigated by the group's anti-money laundering, counter terrorist and proliferation financing policies.

Penalty for non-compliance

50.—(1) A financial institution or person engaged in other business activity that fails to comply with these Regulations commits an offence and is liable to a fine not exceeding one million dollars.

(2) Where an offence under subregulation (1) has been committed by a financial institution or person engaged in other business activity that is a body corporate, notwithstanding and without prejudice to the liability of that body, a person, who at the time of the commission was a director or senior management is liable to be prosecuted as if he or she had personally committed that offence.

(3) Notwithstanding this regulation, a financial institution or person engaged in other business activity that commits an offence for contravention of the Act in relation to a matter that is provided for in these Regulations shall be proceeded against under the Act and not under these Regulations.

SCHEDULE

FORMS

FORM 1

(Regulation 16(2))

SUSPICIOUS TRANSACTION REPORT

CONFIDENTIAL In accordance with the Money Laundering (Prevention) Act	S/A Ref: Ref Date (DD/MM/YY)

COMPLETE AS APPROPRIATE – EITHER TYPE OR PRINT FORM

1. Tick as appropriate: ___ Confirmation of Telephone Report__Initial Report__Supplemental Report ___ Corrected Report

FINANCIAL INSTITUTION OR PERSON ENGAGED IN OTHER BUSINESS ACTIVITY INFORMATION (REGULATED INSTITUTED OR OTHER)

2. Name (of Regulated Institution or Other)
3. Address (of Regulated Institution or Other)
4. Telephone number 5. Fax number

PARTICULARS OF SUSPECT

6. Name (full name of person, business or company)
7. Address
8. Date of Birth (DD/MM/YY)
9. Occupation
10. Employer
11. Telephone number - business 12. Telephone number - residence
13. Form(s) of identification produced by suspect
14. Suspect's relationship with financial institution or person engaged in other business activity
15. Is suspect employed by financial institution or person engaged in other business activity? (YES/NO (If "Yes" give details)

16. Other relevant information (please include details of identification or references taken, associated parties, addresses, telephone numbers etc.)
17. If this report is linked to other reports, please provide details:

Notes: 1. Please complete a separate form in respect of each suspect person, company or business.

2. If you have any questions regarding the completion of this form, please telephone (758) 451-7126

SUSPICIOUS TRANSACTION REPORT

18. Reasons for Suspicion	
19. Signed by (name of person compiling report)	20. Contact Name (Reporting Officer/Compliance Officer where applicable)
21. Telephone Number	22. Fax Number
23. Telephone number	24. Fax number
Financial Intelligence Authority P.O. Box GM 959 Gable woods Mall Post Office Sunny Acres Castries	TRANSACTION COMPLETED Yes No

When submitting this report, please append any additional material that you may consider suitable and which may be of assistance to the recipient, i.e. bank statements, vouchers, international transfers, inter-account transfers, telegraphic transfers, details of associated accounts etc.

FORM 2

(Regulation 22(3)(a))

COMPLIANCE OFFICER FORM

PART A GENERAL INFORMATION
1.Name of Financial Institution or person engaged in other business activity:
PART BPERSONAL DETAILS OF COMPLIANCE OFFICER
2.First Name: 3.Middle Name: 4.Surname:
5.Have you ever had a change of name? (If yes, give details and attach deed poll, etc.)
6.Country of Birth: 7.Identification Number/Passport Number/ Driver's Licence Number (List any two (2) and attach copies)
8.Citizenship:
9.Date of Birth: 10.Email Address:
11.Residential Address: 12.Telephone Number: Work: Home: Mobile:
13.Level of Education: Secondary, Tertiary, Postgraduate, etc. Kindly state any professional qualifications/memberships: e.g., CAMS (Attach copy of qualifications)
14.How long have you been acting in the role of Compliance Officer?
15.Have you ever received any AML/CFT or compliance training? Yes ☐ No ☐
16.Other position held within the entity (Attach job description or organization chart)
PART CFIT AND PROPER REQUIREMENTS
17.Have you ever been charged in Saint Lucia or elsewhere for any criminal offence, regulatory offence or criminal misconduct? (Submit a Police Certificate of Character) Yes ☐ No ☐
18.Have you ever been convicted in Saint Lucia, or elsewhere, for any offence Yes ☐ No ☐

19.Have you ever been a principal officer of an entity that was, during your period of association, charged or convicted of an offence or sanctioned by a Regulatory Body or Supervisor? Yes ☐ No ☐
20.Have you at any time, in Saint Lucia or anywhere else been declared bankrupt or are you the subject of any bankruptcy proceedings? Yes ☐ No ☐
21.Have you at any time, failed to satisfy a judgment debt under a Court Order made in Saint Lucia or anywhere else? Yes ☐ No ☐
22.Have you ever been disqualified or restricted in Saint Lucia or elsewhere by a court from acting as a director of a company? Yes ☐ No ☐
23.Have you ever been refused entry to any profession? Yes ☐ No ☐
24.Have you ever been dismissed or compelled to resign from any office or employment? Yes ☐ No ☐
PART D DECLARATION I am authorized to file this form on behalf of the Financial Institution or person engaged in other business activity. I declare that the information provided is true, correct and complete. The Signature of the Authorised Person is Mandatory. Name: Signature: Position: Date:

FORM 3

(Regulation 46)

DECLARATION OF SOURCE OF FUNDS FOR TRANSACTION EXCEEDING $25,000 WITH A FINANCIAL INSTITUTION

<table>
<tr><td colspan="4">Name and Address of Financial Institution</td><td>Date of Transaction (dd/mm/yy)</td></tr>
<tr><td colspan="4"></td><td>Account Number</td></tr>
<tr><td colspan="5">DECLARATION OF SOURCE OF FUNDS FORM
Section 28 of the Money Laundering (Prevention) Act
Information on Business or Depositor (if different to account holder)</td></tr>
<tr><td colspan="5">NAME</td></tr>
<tr><td colspan="5">Current Address</td></tr>
<tr><td>Resident Status:</td><td colspan="2">Resident</td><td colspan="2">Non-resident</td></tr>
<tr><td>Date of Birth</td><td>Place of Birth</td><td>Nationality</td><td colspan="2">Occupation</td></tr>
<tr><td>Telephone Numbers</td><td>Home:</td><td>Work:</td><td colspan="2">Mobile:</td></tr>
<tr><td colspan="5">Information on account holder</td></tr>
<tr><td colspan="5">Name</td></tr>
<tr><td>Date of Birth</td><td>Place of Birth</td><td>Nationality</td><td colspan="2">Occupation</td></tr>
<tr><td>Telephone Numbers</td><td>Home:</td><td>Work:</td><td colspan="2">Mobile:</td></tr>
<tr><td>Resident Status:</td><td colspan="2">Resident</td><td colspan="2">Non-resident</td></tr>
<tr><td colspan="5">Identification (Valid Picture ID required)</td></tr>
<tr><td>National ID</td><td>Passport</td><td>Driver’s Licence</td><td>Other</td><td>Identification detail</td></tr>
<tr><td colspan="5">Description/Nature of Business Transaction:

Deposit Wire Transfer Currency exchange

Mandatory Instrument Other (specify)</td></tr>
<tr><td colspan="5">Amount and Currency</td></tr>
</table>

FINANCIAL INSTITUTION ARE REQUIRED BY LAW TO VERIFY THE SOURCE OF FUNDS BEING DEPOSITED BEFORE ACCEPTING DEPOSITS AND TO DISCLOSE SUCH INFORMATION TO LAW ENFORCEMENT AUTHORITIES IF REQUIRED. THE MAKING OF A FALSE DECLARATION AS TO THE SOURCE OF FUNDS CONSTITUTES AN OFFENCE UNDER SECTION 21(2) OF THE MONEY LAUNDERING (PREVENTION) ACT. I DECLARE THAT THE SOURCE OF FUNDS IS: (Show supporting evidence, e.g. Receipt, invoice, title deeds etc)		
Transaction Approved: Yes No (If no state reason)		
Depositer's Signature:	Transaction taken by: (signature and title)	Witness

FORM 4

(Regulation 47)

DECLARATION OF SOURCE OF FUNDS FOR TRANSACTIONS EXCEEDING $25, 000.00 WITH A PERSON ENGAGED IN OTHER BUSINESS ACTIVITIES

Name and Address of Person Engaged in Other Business Activity			Date of Transaction: (dd/mm/yy)
DECLARATION OF SOURCE OF FUNDS FORM Section 21 of the Money Laundering (Prevention) Act Customer/Client Information			
NAME			
Current Address:			
Resident Status:	Resident		Non-resident
Date of Birth	Place of Birth	Nationality	Occupation

Telephone Numbers	Home:	Work:	Mobile:	
Customer/Client Agent Information (if applicable)				
Name:				
Date of Birth	Place of Birth	Nationality	Occupation	
Telephone Numbers	Home:	Work:	Mobile:	
Resident Status:	Resident		Non-resident	
Identification: (Valid Picture ID required)				
National ID	Passport	Driver's Licence	Other	Identification details:
Description/Nature of Business Transaction				
Amount and Currency				
FINANCIAL INSTITUTIONS ARE REQUIRED BY LAW TO VERIFY THE SOURCE OF FUNDS BEING DEPOSITED BEFORE ACCEPTING DEPOSITS AND TO DISCLOSE SUCH INFORMATION TO LAW ENFORCEMENT AUTHORITIES IF REQUIRED. THE MAKING OF A FALSE DECLARATION AS TO THE SOURCE OF FUNDS CONSTITUTES AN OFFENCE UNDER SECTION 21(2) OF THE MONEY LAUNDERING (PREVENTION) ACT. I DECLARE THAT THE SOURCE OF FUNDS IS: (Show supporting evidence, e.g. Receipt, invoice, title deeds etc.)				

Transaction Approved: Yes No (If no state reason)		
Customer's Signature:	Transaction taken by: (signature and title)	Witness

Made this 22nd day of May, 2023.

LESLIE MONDESIR,
Attorney General.

SAINT LUCIA
PRINTED BY THE NATIONAL PRINTING CORPORATION
CASTRIES
2023 [Price : $26.50]