# SAINT LUCIA

STATUTORY INSTRUMENT, 2010, No. 55

[ 17th May, 2010 ]

In exercise of the power conferred under section 43 of the Money Laundering (Prevention) Act, No. 8 of 2010, the Attorney General makes these Regulations:

**Citation**

**1.** These Regulations may be cited as the Money Laundering (Prevention) (Guidance Notes) Regulations 2010.

**Guidance notes**

**2.**— (1) The Guidance Notes set out in the Schedule regulates financial institutions.

(2) A breach of the Guidance Notes by a financial institution constitutes an offence and the financial institution is liable to a fine not exceeding $1million .

(3) A financial institution is deemed to have notice of the provisions of the Guidance Notes.

**SCHEDULE**

**(Regulation 2)**

**PART I**

**BACKGROUND**
*Group Practice*
*Interrelation of Parts III and IV of these Guidelines*

**WHAT IS MONEY LAUNDERING**
*Placement*
*Layering*
*Integration*

**RELEVANT OFFENCES**
*Money Laundering*
*Penalty*

**OTHER OFFENCES**
*Tipping Off*
*Penalty*
*Prejudicing the Investigation*
*Penalty*
*Failure to Disclose*
*Penalty*

**PART II**

**SCOPE OF THE GUIDELINES**
*Who and what services are governed by the guidelines*

**PART III**

**FOR THE GUIDANCE OF ALL FINANCIAL INSTITUTIONS**
*The duty of Vigilance*
*The Compliance Officer*
*Appointment of Compliance Officer*
*Appointment of Deputy to the Compliance Officer*
*Role and Responsibilities of the Compliance Officer*
*Details of Compliance Officer*

**COMPLIANCE MONITORING**
*Compliance Audits*
*Report to the Board of Directors or Audit Committee*

*The duty of vigilance of employees*
*The Consequence of Failure*

## PART I

### BACKGROUND

1. These Guidelines have been issued by the Financial Intelligence Authority (FIA) pursuant to section 5 (f) of the Money Laundering Prevention Act No. 8 of 2010 ("the Act") and the Proceeds of Crime Act, Cap. 3.04 in recognition of the risks the financial sector in Saint Lucia is exposed to with regard to the laundering of the proceeds of criminal activity. The Guidelines reflect best practice internationally and implement the recommendations of the Financial Action Task Force (FATF) and the Caribbean Financial Action Task Force (CFATF).

2. The Guidelines are designed to assist with the enforcement of the Act as they represent good industry practice. A financial institution should try as best as possible to adopt internal procedures, which are of equivalent standard. In determining whether a person has complied with the requirements of the Act, the authorities may take into account whether an institution can show that its internal systems and procedures measure up to the standards indicated by these Guidelines.

3. The FIA regards the adoption by financial institutions of adequate policies, procedures and practices for the deterrence and prevention of money laundering as vital and it intends to use these Guidelines as a yardstick for measuring the adequacy of systems to prevent money laundering.

4. Occurrences of money laundering, or the failure to have adequate policies, procedures and practices to guard against money laundering, may call into question the adequacy of systems and controls, or the prudence and integrity or fitness and appropriateness of the management of the financial institutions.

5. The Guidelines are designed to assist financial institutions in complying with the Money Laundering legislation by specifying the best practices in combating money laundering. The HA recognizes that financial institutions may have systems and procedures in place which, whilst not identical to those outlined in these Guidelines, nevertheless impose controls and procedures, that are at least equal to if not higher than those contained in these Guidelines. The FIA when assessing the adequacy of a financial institution's systems and controls will take this into account.

6. The FIA expects that there will be in existence evidence on file that all due diligence checks have been carried out on the accounts acquired during the purchase of a new business either in whole or in part.

7. These Guidelines are a statement of the standard expected by the FIA of all financial institutions in Saint Lucia. The FIA actively encourages all institutions to develop and maintain links with it to ensure that the internal systems and procedures are effective and up to date, so enabling them to implement their duty of vigilance.

***Group Practice***

8. Where a group whose headquarters are in Saint Lucia operates branches or controls subsidiaries in another jurisdiction, it should ensure that:

   a) such branches or subsidiaries observe these Guidelines or adhere to local standards if those are at least equivalent;

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

   c) each such branch or subsidiary informs itself as to its own local reporting point, equivalent to the FIA in Saint Lucia, and that it is familiar with the procedures for disclosure equivalent to those stated in Appendix F;

   d) such branch of subsidiary informs the home supervisor when they are unable to observe appropriate AML measures because it is prohibited by the laws of the host country.

***Interrelation of Parts III and IV of these Guidelines***

9. Part III of these Guidelines is addressed to financial institutions generally. Part IV sets out additional guidance for different types of financial businesses and each section is to be read in conjunction with Part III.

10. The laundering of criminal proceeds through the financial system is vital to the success of the criminal operation. To this end criminal networks seek to exploit the facilities of the world's financial institutions in order to benefit from such proceeds. Increased integration of the world's financial systems and the removal of barriers to the free movement of capital have enhanced the ease with which criminal proceeds can be laundered and have added to the complexity of audit trails.

**WHAT IS MONEY LAUNDERING?**

11. The phrase "money laundering" covers all procedures to conceal the origins of criminal proceeds so that they appear to originate from a legitimate source.

12. There are three stages of money laundering:

12.1 Placement: the physical disposal of cash proceeds. In the case of many serious crimes e.g. drug trafficking the proceeds take the form of cash which the criminal wishes to place in the financial system. Placement may be achieved by a wide variety of means according to the opportunity afforded to, and the ingenuity of the criminal, his advisers, and their network. Typically it may include:

   a) Placing cash on deposit at a bank (often intermingled with a legitimate credit to obscure the audit trail), thus converting cash into a readily recoverable debt;

   b) Physically moving cash between jurisdictions;

c) Making loans in cash to businesses which seem to be legitimate or are connected with legitimate businesses, thus also converting cash into debt;

d) Purchasing high value goods for personal use or expensive presents to reward existing or potential colleagues with cash;

e) Purchasing the services of high value individuals with cash;

f) Purchasing negotiable assets in one-off transactions; or

g) Placing cash in the client account of a professional intermediary.

12.2 **Layering:** This is the separating of the proceeds of crime from their source by creating sometimes complex layers of financial transactions designed to mask their origin and hamper the investigation, reconstruction and tracing of the proceeds; for example, by international wire transfers using nominees or "shell companies", by moving in and out of investment schemes or by repaying credit from the direct or indirect proceeds of crime.

12.3 **Integration:** This is the placing of the laundered proceeds back into the economy as apparently legitimate business funds, for example, by realizing property or legitimate business assets, redeeming shares or units in collective investment schemes acquired with criminal proceeds, switching between forms of investment, or by surrendering paid up insurance policies.

13. The criminal remains relatively safe from vigilance systems while proceeds are not moving through these stages and remain static. Certain points of vulnerability have been identified in the stages of laundering which the launderer finds difficult to avoid and where his activities are therefore more susceptible to recognition, in particular:

(a) Cross border flows of cash;

(b) Entry of cash into the financial system;

(c) Transfers within and from the financial system;

(d) Acquisition of investments and other assets;

(e) Incorporation of companies; and

(f) Formation of trusts.

14. Accordingly, vigilance systems require institutions and their key staff to be vigilant at these points along the audit trail where the criminal is most actively seeking to launder, i.e. to misrepresent the source of criminal proceeds. One of the recurring features of money laundering is the urgency with which, after a brief cleansing, the assets are often reinvested in a new criminal activity.

**RELEVANT OFFENCES**

**Money Laundering**

15. A money laundering offence is committed by:

(a) concealing or transferring proceeds of criminal conduct;

(b) arranging with another to retain the proceeds of criminal conduct;

(c) acquisition, possession or use of proceeds of criminal conduct.

15.1 Property includes money, moveable or immoveable property, corporeal or incorporeal property and interest in property.

15.2 **Penalty:** The punishment for engaging in a money laundering offence is:

(i) On summary conviction to a fine of not less than five hundred thousand dollars (but not exceeding one million dollars) or to a term of imprisonment of not less than 5 years (but not exceeding 10 years) or both.

(ii) On indictable conviction to a fine of not less than one million dollars (not exceeding two million dollars) or to a term of imprisonment of not less than 10 years (not exceeding 15 years) or both.

## OTHER OFFENCES

16. **Tipping Off**

It is an offence for anyone who knows, suspects or has reasonable grounds to suspect that a disclosure has been made, or that the authorities are acting or are proposing to act in connection with an investigation into money laundering, to prejudice an investigation by so informing the person who is the subject of a suspicion, or any third party of the disclosure, action or proposed action.

16.1 **Penalty:** The punishment on summary conviction is a term of five years (not exceeding 10 years) or a fine of not less than $50,000 or both.

17. **Prejudicing the Investigation**

It is an offence to cause or permit to be falsified or conceal or destroy or otherwise dispose of information which is likely to be material to an investigation into money laundering.

17.1 **Penalty:** The punishment on summary conviction is a term of not less than seven years (not exceeding 15 years) or a fine of not less than $500,000 or both.

18. **Failure to Disclose**

It is an offence if a person fails to report a suspicious transaction relating to money laundering within seven days from the date the transaction was deemed to be suspicious.

18.1 Penalty: the offender is punishable on indictment to a fine of $500.000.

## PART II

## SCOPE OF THE GUIDELINES

### WHO AND WHAT SERVICES ARE GOVERNED BY THE GUIDELINES

19. The Guidelines apply to the financial institutions which provide the following services specified in the Schedule 2 of the Act and any other service that may be designated by the FIA:

(a) A bank licensed under the Banking Act or any enactment replacing it:

(b) A building society registered under the Building Societies Act, or any enactment replacing it;

(c) A credit union registered under the Co-operative Societies Act or any enactment replacing it;

(d) An insurance company registered under the Insurance Act or any enactment replacing it;

(e) A company that performs international financial services under the international financial services legislation in force in Saint Lucia:

(f) A trust company, finance company or deposit taking company declared by the Minister by Order published in the Gazette to be a financial institution;

(g) Registered agents and trustees licensed under the Registered Agent and Trustee Licensing Act, Cap. 12.12;

(h) A trust licensed under the International Trusts Act;

(i) A person licensed to operate an exchange bureau;

(j) A person licensed as a dealer or investment adviser;

(k) A person who carries on cash remitting services;

(1) A person who carries on postal courier services;

(m) Real estate business;

(n) Car dealerships;

(o) Casinos (gaming houses);

(p) Courier services;

(q) Jewellery business;

(r) Internet gaining and waging services;

(s) Management companies;

(t) Asset management and advice-custodial services;

(u) Nominee services;

(v) Any business transaction conducted at a post office involving money order;

(w) Lending (including personal credits, factoring with or without recourse, financial or commercial transaction including forfeiting cheque cashing services;

(x) Finance leasing;

(y) Venture risk capital;

(z) Money transmission services;

(aa) Issuing and administering means of payment (e.g. credit cards, travelers' cheques and bankers' drafts);

(bb) Guarantees and commitments;

(cc) Trading for own account of customers in -

(i) money marked instruments (cheques, bills, certificates of deposit, etc);

(ii) foreign exchange;

(iii) financial futures and options;

(iv) exchange and interest rate instruments; and

(v) transferable instruments;

(dd) Underwriting share issues and the participation in such issues;

(ee) Money broking;

(ff) Deposit taking;

(gg) Bullion dealing;

(hh) Financial intermediaries;

(ii) Custody services;

(jj) Securities broking and underwriting;

(kk) Investment and merchant banking;

(ll) Asset management services;

(mm) Trusts and other fiduciary services;

(nn) Company formation and management services;

(oo) Collective investment schemes and mutual funds;

(pp) Attorneys-at-Law;

(qq) Accountants.

## PART III

## FOR THE GUIDANCE OF ALL FINANCIAL INSTITUTIONS

### THE DUTY OF VIGILANCE

20. Critical to the systems and procedures to prevent money laundering is a system to evaluate the personal and financial history of employees. This system should serve as a screening process in the recruitment of employees, so as to reduce the likelihood of hiring persons who may engage in money laundering and terrorism financing.

21. Proper screening procedures should be adopted to ensure that only honest, law-abiding persons are employed. Institutions will need to exercise discretion regarding the extent of the information they seek from a potential employee. The different circumstances of each application for employment, such as the office or post in the firm, will determine the level of screening required.

22. As the case with a potential customer verification work on a potential employee should be performed **prior** to an offer of employment being made. The risk of mere superficial checks is that, should the employee eventually engage in money laundering, the firm may be held liable for failure to implement a proper evaluation system.

**(a) Reference checks**

At least two (2) written references should be required and one of which must be from the previous employer (where applicable). The reason for termination needs to be stated and included in the previous employer's reference.

**(b) Checking the Authenticity of Academic Qualifications**

Only original documents, such as certificates, should be accepted. Where a transcript is required this should be sent directly to the company by the academic institution.

**(c)** If the individual has had a period of self **employment** proof of income earned, and the source, should be substantiated.

**(d)** Periods of **unemployment** should also be explained and substantiated by written references. Referees must be in a position to attest to the character of applicants and must not be relatives or personal friends. There should be some formal basis for the applicant's relationship with the referee e.g. the applicant's pastor, banker, teacher, former co-worker, business client, Member of Parliament, etc.

**(e)** The **financial history** of the applicant should be established as follows:

(i) Examination of the two most recent statements from each of his/ her bank accounts.

(ii) The applicant may also be asked to provide information on his credit history. A letter from each bank could establish this.

(iii) The real estate holdings of the applicant may be requested as well as any other assets and liabilities. This may be established by way of a standard balance sheet. (In order to monitor changes to the holdings, employees could therefore be required to submit annual statements of affairs).

(iv) Employers must seek an explanation for any unusual ownership patterns i.e. assets in excess of the applicants earning history.

23. The screening process is more stringent for an individual who is termed an officer of a regulated entity and those occupying sensitive posts.

24. An officer is any individual who has the power to, whether orally or in writing, enter an organization into a contract or legally binding obligation. Examples of persons who may be deemed an 'officer' include, but is by no means limited to a director of the company, president, vice-president, general manager, secretary, financial controller or treasurer. It is therefore imperative that an individual who occupies the office of an officer, be 'fit and proper'. To be 'fit and proper' an individual should not at a minimum, be convicted for an offence involving dishonesty or be an undischarged bankrupt. The review process should include information received in respect of a credit report, work history, police record, and any other reference information which may be required to make an appropriate determination.

25. Examples of what may be deemed as a sensitive post include but are not restricted to, a cashier, investment advisor, sales person, advisory staff, new customer and new business staff - insurance agent and broker, processing and claims handling staff.

26. In addition to the verification work described above it is required that an individual occupying the post of officer or a sensitive post has a police report done as part of the screening process.

27. In the event that the police report reveals information which is in contradiction to the fit and proper requirement, the offer of employment must not be made.

28. It is important to know your employees. Procedures should be in place to ensure high standards of integrity among employees. The standards should include a code of ethics for the conduct of all employees. The procedures should allow 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. The procedures should also include paying attention to employees whose lifestyles cannot be supported by his or her salary. The procedures should expressly provide for special investigation of employees who are associated with mysterious disappearances or unexplained shortages of funds.

29. Institutions should be constantly vigilant in deterring criminals from making use of any of the facilities described in Part I for the purpose of money laundering. The task of detecting crime is that of the law enforcement agencies. While financial institutions may on occasion be requested or, under due process of law, may be required to assist law enforcement agencies in that task, the duty of vigilance is necessary to prevent money laundering. The duty of vigilance consists mainly of the following five elements:

    a) Verification;

    b) Recognition of suspicious transactions;

    c) Record keeping;

    d) Reporting of suspicions;

    e) Training.

30. Institutions perform their duty of vigilance by having in place systems which enable them to:

    (a) Determine or receive confirmation of the true identity of customers requesting their services;

    (b) Recognize and report suspicious transactions to the FIA. In this respect any person who voluntarily discloses information to the FIA arising out of a suspicion or belief that any money or other property represents the proceeds of crime is protected under sections 35 and 36 of the Act from being sued for breach of the duty of confidentiality;

    (c) Keep records of all business transactions for the prescribed period of seven (7) years;

    (d) Train key staff;

    (e) Liaise closely with the FIA on matters concerning vigilance policy and systems; and

    (f) Ensure that internal auditing and compliance departments regularly monitor the implementation and operation of vigilance systems.

31. An institution should not enter into a business relationship or carry out a significant one-off transaction unless it has fully implemented the above systems. In particular, financial institutions should pay particular attention to all complex, unusual or large business transactions, or unusual patterns

of transactions, whether completed or not, and to insignificant but periodic transactions which have no apparent economic or lawful purpose.

32. Since the financial sector encompasses a widely divergent range of organizations, from large institutions to small financial intermediaries, the nature and scope of the vigilance system appropriate to any particular organization will vary depending on its size, structure and the nature of the business. However, irrespective of the size and structure, all institutions should exercise a standard of vigilance which in its effect measures up to these Guidelines.

33. Vigilance systems should enable key staff to respond effectively to suspicious occasions and circumstances by reporting them to the relevant personnel in-house and to receive training from time to time, whether from the institution or externally, to adequately equip them to play their part in meeting their responsibilities.

34 As an essential part of training, key staff should receive a current copy of their company's instruction manual(s) relating to entry, verification and records based on the recommendations contained in the Guidelines.

**THE COMPLIANCE OFFICER**

35. Section 16 (1) (n) of the Act stipulates that internal reporting procedures must provide for the identification of a person to whom a report must be made of any information or matter giving rise to some knowledge of or a suspicion that money laundering is taking place. The person is commonly titled the Compliance Officer.

36. All regulated entities are therefore required to have an officer appointed as the Compliance Officer. The compliance role is critical and the position should be a senior one in the firm's organizational structure. Depending on the size of the firm, there may be one such officer or the firm should set up a Compliance Department. It may be possible in very small operations, for example, for the dealer himself to be designated the Compliance Officer.

37. Compliance Officers must be fully acquainted with the provisions of the Act, its amendments and regulations as well as the Proceeds of Crime Act. They must, in particular, be cognizant of the requirements of confidentiality regarding money-laundering reports and investigations into money laundering.

**Appointment of Compliance Officer**

38. Financial institutions should appoint a Compliance Officer who is also responsible for the establishment and implementation of policies. programmes, procedures and controls for the purposes of preventing or detecting money laundering. Depending on the size of the firm, there may be one such officer or a Compliance Department.

39. The Officer should be separate and apart from the day-to-day activities/ operational aspects of the business. It is also imperative that the Compliance Officer, report directly to the Board of Directors (where possible). This measure will serve to preserve the integrity of the work carried out by the Compliance Officer, and additionally protect the individual from what may be deemed as victimization.

40. Any individual who occupies the office of Compliance Officer should be 'fit and proper' - that is to say, at a minimum, he/she has not been convicted of an offence involving dishonesty or is an undischarged bankrupt. Failure to adhere to this criterion should result in the individual immediately vacating the post.

41 To fulfill the role of the Compliance Officer such a person should:

(a) possess the trust and confidence of the management and staff;

(b) have sufficient knowledge of the organization, its products, services and systems;

(c) have access to all relevant information throughout the organization and, or have knowledge as to the existence of such information;

(d) warrant the trust and confidence of the enforcement agencies.

42. Once appointed, all staff should be aware of the identity of the Compliance Officer.

**Appointment of Deputy to the Compliance Officer**

43 In some instances, such as a group of companies, it may be necessary to have a deputy to the Compliance Officer. When appointing this deputy it is important that such a person possesses similar professional qualities as the Compliance Officer. Additionally, the deputy must have a comprehensive understanding of the legal and institutional expectations of the role. In the absence of the Compliance Officer (whether due to illness, vacation leave, etc.), the deputy must take on the full responsibility of the role. It is therefore critical that the Compliance Officer and his/her deputy are not absent at the same time, so as to ensure that the office is permanently staffed.

**Role and Responsibilities of the Compliance Officer**

**44.** The Compliance Officer should have the following minimum responsibilities:

(a) to establish and implement policies, programmes, procedures and controls as may be necessary for the purpose of preventing or detecting money laundering. This duty includes but is not limited to:

(i) organising training sessions for staff on various compliance related issues and for instructing employees as to their responsibilities in

respect of the provisions of the Act and the Proceeds of Crime Act;

(ii) the establishment of procedures to ensure high standards of integrity of employees;

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

(b) to make modifications or adjustments to aspects of (a) above that may be deemed necessary;

(c) to arrange for independent audits in order to ensure that the programmes as mentioned in (a) above, are being complied with;

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

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

(f) to prepare and compile the external reports of unusual transactions to the FIA;

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

(h) to remain informed of the local and international developments on money laundering;

(i) to prepare reports to the Board of Directors and other relevant persons on the institution's efforts in combating money laundering;

(j) to exercise control and review the performance of lower level AML officers within the organization and/or within each branch or unit;

(k) to maintain contact with the FIA.

**Details of Compliance Officer**

45. Financial institutions are hereby required to submit the following details on their Compliance Officer to the FIA within seven (7) days of his/her appointment:

(a) name

(b) job title

(c) telephone number (and extension where applicable)

(d) e-mail address

(e) current resume.

46. Any change in the office of the Compliance Officer should be communicated to the FIA within a month of such a change.

**COMPLIANCE MONITORING**

47. This act of establishing compliance procedures and policies creates the reasonable regulatory expectation that these will be followed by the financial institution at all times.

48. Section 16(1)(j) and (o) of the Act, has therefore made it mandatory for financial institutions to conduct independent audits to ensure anti money laundering systems, which includes programmes, procedures and controls, are operating in accordance with the institution's existing policy manual.

49. The compliance monitoring of the institution's system should be done on an ongoing basis by the Compliance Officer. Any deficiencies or findings which are noteworthy should be communicated in writing to the senior management of the institution, at least on a **monthly** basis,

50. The Compliance Officer should be accountable to the Board of Directors where possible. In such cases he/she is not, and should not be accountable to the senior management of the institution. Submission of monthly reports to senior management is for the purpose of providing information on existing_or potential areas in which deficiencies may occur and the corrective actions implemented or required to be implemented in order to rectify the situation.

51. The Compliance Officer is required to implement corrective actions as soon as deficiencies have been noted in the system. It is not acceptable for the Compliance Officer to argue that recommendations for change must be delayed until the next monthly management report submission. The next monthly report should be used as means of assessing the success (or otherwise) of the changes that have been implemented.

52. As soon as the Compliance Officer is aware that there is a significant problem within the institution he/she needs to notify management immediately.

53. It is recommended that an independent audit be conducted at least annually. with professionals retained **specifically** to assess the AML controls of the firm. This will aid in assessing the level of compliance with existing regulations within the organization and as a measure of the effectiveness of the work being done by the Compliance Officer.

**Compliance Audits**

54. The audits conducted, by both the Compliance Officer and the independent auditor, should include at a minimum:

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

(2) evaluation of the extent and frequency of training received by employees;

(3) testing of employees' knowledge of AML procedures;

(4) a review of investments by clients for possible structured transactions;

(5) analysis of a sampling of reportable transactions including a comparison of those transactions with reports submitted on those transactions;

(6) a review of transactions for possible suspicious transactions;

(7) testing of record keeping of all money laundering reports, identification documentation of customers and transaction records.

55. For compliance audits carried out by independent auditors, findings must be documented, and violations of the law and AML procedures must be promptly reported to the Compliance Officer of the firm and/or the Board of Directors.

56. There should be written audit procedures for assessing compliance with money laundering prevention legislation and guidelines. These audit procedures or programme steps should be reviewed on an ongoing basis in order to ensure their usefulness.

57. In carrying out the routine audit, the Compliance Officer should have the following information included in his working papers, at a minimum:

(a) date the work was performed;

(b) the rationale or method of selecting the sample;

(c) adequate narrative on the sample selected, (e.g. for testing the adequacy of customer identification — the name of the individual, customer number, means of identification used and any associated number, etc.);

(d) deficiencies noted;

(e) corrective action recommended and/or taken.

58. All working papers are required to be maintained for a period of five (5) years.

**Report to the Board of Directors or Audit Committee**

59. Reports should be submitted to the Board of Directors at least **quarterly.** A more detailed report than the one submitted to senior management, should be submitted to the Board of Directors.

60. The following is a list of items that should be included in this report:

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

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

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

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

(5) the number of internal reports that have been received from each separate division, product, area, subsidiary, etc.;

(6) the percentage of those reports submitted to the FIA;

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

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

(9) any recommendations concerning resource requirements to ensure effective compliance.

61. In dealing with customers, the duty of vigilance begins with the start of a business relationship or a significant one-off transaction and continues until either comes to an end. However, the keeping of records (from which evidence of the routes taken by any criminal proceeds placed in the financial system are preserved) continues as a responsibility as described below in these notes.

**THE DUTY OF VIGILANCE OF EMPLOYEES**

62. It cannot be overly stressed that all employees and in particular key staff are at risk of being or becoming involved in criminal activity if they are negligent in their duty of vigilance and they should be aware that they face criminal prosecution if they commit any of the offences under the Act.

63. Although on moving to new employment, employees will normally put out of their minds any dealings with customers of the previous employer, if such a customer becomes an applicant for business with the new employer and the employee recalls a previous suspicion, he/she should report this to his/her new Compliance Officer (or other senior colleague) according to the vigilance systems operating.

**THE CONSEQUENCE OF FAILURE**

64. For the institution involved, the first consequence of the failure in the duty of vigilance is likely to be commercial. Institutions that however unwittingly, become involved in money laundering, risk the loss of their

good market name and position and the incurring of non-productive costs and expenses.

65. The second consequence may be to raise issues of supervision and fit and proper standing as explained under the heading "Background".

66. The third consequence is the risk of criminal prosecution of the institution for the commission of an offence under the Act.

67. For the individual employee, it should be self evident that the consequences of failure are not dissimilar to those applicable to institutions. The employee's good name within the industry is likely to suffer and he or she may face the risk of prosecution for the commission of an offence under the Act.

68. It should be noted that certain offences under the Act are concerned with assistance given to the criminal. There are two aspects to such criminal assistance:

    (a) the provision of opportunity to obtain, conceal, retain or invest criminal proceeds; and

    (b) the knowledge or suspicion (actual or, in some cases, imputed) of the person assisting the criminal, that criminal proceeds are involved.

69. The determination of involvement is avoidable on proof that knowledge or suspicion was reported without delay in accordance with the vigilance systems of the institution.

**VERIFICATION (KNOW YOUR CUSTOMER (KYC))**

70. The following points of guidance will apply according to:

    a) the legal personality of the applicant for business (which may consist of a number of verification subjects); and

    b) the capacity in which he or she is applying.

71. An institution undertaking verification should establish to its reasonable satisfaction that every verification subject, relevant to the application for business, really exists. All the verification subjects of joint applicants for business should normally be verified. On the other hand, where the guidelines imply a large number of verification subjects it may be sufficient to carry out verification to the letter on a limited group only, such as the senior members of the family, the principal shareholders, the main directors of the company, etc.

72. An institution should carry out verification in respect of the parties operating the account. Where there are underlying principals, however, the true nature of the relationship between the principals and the account signatories must also be established and appropriate enquiries performed on the former, especially if the signatories are accustomed to acting on

their instructions. In this context "principals" should be understood in its widest sense to include, for example, beneficial owners, settlers, controlling shareholders, directors, major beneficiaries, etc., but the standard of due diligence will depend on the exact nature of the relationship.

73. Attention is drawn to the exemptions to verification set out at paragraphs 106 -112 below.

**WHEN MUST IDENTITY BE VERIFIED**

74. Whenever an account is to be opened, a new signatory added to an account, or a significant one-off transaction undertaken, the prospective customer must be identified. Once identification procedures have been satisfactorily completed, then the business relationship has been established and as long as records are maintained as required in these Guidelines, no further evidence of identity is required when transactions are subsequently undertaken. However, irrespective of the exemptions noted in paragraphs 106 - 112, identity must be verified in all cases where money laundering is known or suspected.

**VERIFICATION OF SUBJECT**

*FACE **TO FACE CUSTOMERS***

***Individuals***

75. The verification subject may be the account holder himself or one of the principals of the account.

76. An individual trustee should be treated as a verification subject unless the institution has completed verification of the trustee in connection with a previous business relationship or one-off transaction and termination has not occurred. Where the applicant for business consists of individual trustees, all of them should be treated as verification subjects unless they have no individual authority to operate a relevant account or otherwise to give relevant instructions.

***Partnerships and Unincorporated Businesses***

77. Institutions should treat as verification subjects all partners/directors of a firm which is an applicant for business who are relevant to the application and have individual authority to operate a relevant account or otherwise to give relevant instructions. Verification should proceed as if the partners were directors and shareholders of a company in accordance with the principles applicable to non-quoted corporate applicants (see paragraph 39 below). In the case of a limited partnership, the general partner should be treated as the verification subject. Limited partners need not be verified unless they are significant investors.

***Companies (including corporate trustees)***

78. Unless a company is quoted on a recognized stock exchange or is a subsidiary of such a company or is a private company with substantial premises and pay roll of its own, steps should be taken to verify the company's underlying beneficial owner/s - namely those who ultimately own or control the company.

79. The expression "underlying beneficial owner/s" includes any person/s on whose instructions the signatories of an account, or any intermediaries instructing such signatories, are for the time being accustomed to act.

***Intermediaries***

80. If the intermediary is a locally regulated institution and the account is in the name of the institution but on behalf of an underlying customer (perhaps with reference to a customer name or account number), this may be treated as an exempt case but otherwise the customer himself (or other person on whose wishes the intermediary is prepared to act) should be treated as a verification subject.

81. Subject to paragraphs 102, 109, and 110, if documentation is to be in the customer's name but the intermediary has power to operate any bank, securities or investment account, the intermediary should be treated as a verification subject.

82. Where an institution suspects that there may be an undisclosed principal (whether individual or corporate) it should monitor the activities of the customer to determine whether the customer is in fact merely an intermediary. If a principal is found to exist, further enquiry should be made and the principal should be treated as a verification subject.

***Other institutions***

83. Where an applicant for business is an institution but not a firm or company (such as an association, institute, foundation, charity, etc.), all signatories who customarily operate the account should be treated as verification subject/s.

***Politically Exposed Persons (PEPs)***

84. Financial institutions are asked to apply enhanced due diligence when dealing with politically exposed persons (PEPs). Business relationships with individuals holding important public positions and with companies clearly related to them may expose the institution to a significant reputational and/or legal risk.

85. The PEP risk is associated with providing financial and business services to government ministers or officials from countries with widely-known problems of bribery, corruption and financial irregularity within their

government and society. This risk is particularly acute in countries that do not have AML standards that meet internationally accepted norms.

86. There is the risk that such persons, especially in countries were corruption is widespread, may abuse their public powers for their own illicit enhancement through the receipt of bribes, embezzlement, diverting international aid payments, etc. in exchange for arranging for favourable decisions, contracts or job appointments. The proceeds of such corruption are often transferred to other jurisdictions and concealed in financial institutions there.

87. Where a financial institution is considering forming a business relationship with a person whom it suspects of being a PEP it must exercise enhanced due diligence to identify that person fully.

88. Financial institutions should gather sufficient information from a new customer, and check publicly available information, in order to establish whether or not the customer is a PEP. They should investigate the source of funds before accepting a PEP as a client. The decision to establish business relationships with or open an account for a PEP should be taken at a senior management level. Financial institutions should continue to apply enhanced due diligence to a PEP client/account on an ongoing basis.

89. All financial institutions should assess countries with which they have financial relationships, and which are most vulnerable to corruption. One source of information is the Transparency Corruption Perceptions Index at www.transparency.org

**NON -FACE —TO- FACE CUSTOMERS**

90. Financial institutions are sometimes asked to open accounts or form business relationships with persons who are not available for a personal interview, for example in the case of non-resident customers. Financial institutions should apply equally effective customer identification procedures and on-going monitoring standards to non-face-to-face customers as for those available for personal interview.

91. Even though the same documentation can be provided by face-to-face and non-face-to-face customers, there is a greater difficulty in matching the customer with the documentation in the case of non-face-to-face customers.

92. In accepting business from non-face-to-face customers financial institutions should:

    (a) Apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview;

    (b) ensure that there are specific and adequate measures to mitigate the higher risk.

93. These measures to mitigate risk may include:
    (i) Certification of documents presented;
    (ii) Requisition of additional documents to complement those which are required for non-face-to-face customers;
    (iii) Independent verification of documents by contacting a third party.

**Correspondent Banking**

94. Correspondent banking refers to the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). Financial institutions are required by FATF to apply appropriate levels of due diligence to such accounts by gathering sufficient information from and performing enhanced due diligence processes on correspondent bank prior to setting up correspondent accounts. These include:

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

    (b) Obtaining authenticated/certified copies of banking licences or similar authorization documents, as well as any additional licences needed 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 respondent bank's board and management composition;

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

    (g) Obtaining details regarding the group structure within which the respondent bank may fall, as well as any subsidiaries it may have;

    (h) Obtaining proof of its years of operation, along with access to its audited financial statements (5 years if possible);

    (i) Information as to its external auditors;

    (j) Ascertaining whether the bank has established and implemented sound customer due diligence, anti-money laundering policies and strategies and appointed a Compliance Officer (at managerial level), to include obtaining a copy of its AML policy and guidelines;

    (k) Caution to be exercised by correspondent bank, shall be cautious while continuing relationships with correspondent banks located in countries with poor KYC standards and countries identified as "non-

cooperative" in the fight against money laundering and terrorist financing;

(l) Ascertaining whether the correspondent bank, in the last 7 years (from the date of the commencement of the business relationship or negotiations therefore), has been the subject of, or is currently subject to any regulatory action or any AML prosecutions or investigations. A primary source from which this information may be sought and ascertained would be the regulator for the jurisdiction in which the correspondent bank is resident. Information may also be available from its website;

(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 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) 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. The bank shall also ensure that the respondent bank is able to provide the relevant customer identification data/information immediately on request.

(s) Documenting the AML/CFT responsibility of each institution.

While local banks currently may not provide correspondent banking services to foreign banks, they may have banking relationships with overseas financing institutions and must therefore ensure that the above procedures are engaged vis-à-vis such relationships.

**Internet and Cyber business**

**95.** The Financial Action Task Force in its Report on Money Laundering Typologies, 200-2001 stated that "transactions performed by access to financial services through the internet do not appear to present specific risks for money laundering in and of themselves. Rather it is the three characteristics of the internet that together tend to aggravate certain "conventional money laundering risks:

a. the ease of access through the internet

b. the depersonalization of contact between the customer and the institution; and

c. the rapidity of electronic transactions.

96. Any financial services provider offering services over the internet should implement procedures to verify the identity of its clients. Care should be taken to ensure that the same supporting documentation is obtained from internet customers as for other customers, particularly where face - to face verification is not practical. In view of the additional risks of conducting business over the internet, financial institutions should monitor on a regular basis the activity in customers' accounts opened on the internet.

97. Regarding the difficulties of following internet links between possible criminal proceeding and the individual attempting to launder such funds and finance of terrorism, the FATF within its 2000 — 2001 typologies report offered the following suggestions:

(a) Require Internet Service Providers (ISPs) to maintain reliable subscriber registers with appropriate identification information.

(b) Require ISPs to establish log files with traffic data relating internet-protocol number to the subscriber and to telephone numbers used in the connection.

(c) Require that this information be maintained for a reasonable period.

(d) Ensure that this information may be available internationally in a timely manner when conducting criminal investigations.

98. Other products of emerging technology include:

(a) smartcards;

(b) E-cash.

99. **Smartcards**

Also called stored value cards, or electronic purses, are plastic cards that contain a microchip that is encoded with details. This allows the card to be used instead of cash. Such cards are particularly at risk for money laundering for the following reasons:

(a) they provide anonymity, since the owner's details are not included on the card

(b) they are more portable than cash; and

(c) they eliminate the paper trail associated with a transaction.

100. **E-Cash**

In concept electronic cash or e-cash would replace the need for notes and coins for transactions carried out via the internet. With e-cash value is purchased from an authorized provider, similar to what obtains for the

smartcard. The value is then stored to either a safe repository on-line or to the customer's home computer. When the e-cash is spent the corresponding value is then credited to a retailer's e-cash account which is later followed by the deposit to the retailer's regular bank account. The security of the e-cash system is mainly concerned with ensuring that value cannot be created by unauthorized institutions or that the value cannot be spent more than once.

101. In addition to the risk factors for money laundering identified above for smartcards, e-cash is particularly vulnerable because identification is made by a password (which can be stolen).

**Exempt Cases**

102. Unless a transaction is a suspicious one, verification is not required in the following defined cases, which fall into two categories: those which do not require third party evidence in support; and those which do. However, where an institution knows or suspects that laundering is or may be occurring or has occurred, the exemptions and concessions as set out below do not apply and the case should be treated as a case requiring verification (or refusal) and, more importantly, reporting.

**CASES NOT REQUIRING THIRD PARTY EVIDENCE IN SUPPORT**

***Exempt institutional applicants***

103. Verification of the institution is not needed when the applicant for business is an institution itself subject either to these Guidelines or to their equivalent in another jurisdiction. Reasonable effort should be made to ensure that such institutions actually exist and are contained on the relevant regulator's list of regulated institutions or by checking with a correspondent bank in the home country.

***Small one-off transactions***

104. Verification is not required in the case of small one-off transactions (whether single or linked) unless at any time between entry and termination it appears that two or more transactions which appeared to have been small one-off transactions are in fact linked and constitute a significant one-off transaction. For the purposes of these Guidelines, transactions which are separated by an interval of three months or more are not required, in the absence of specific evidence to the contrary, to be treated as linked.

105. These Guidelines do not require any institution to establish a system specifically to identify any aggregate linked one-off transactions but institutions should exercise care and judgment in assessing whether transactions should be treated as linked. If, however, an existing system does indicate that two or more one-off transactions are linked, it should act upon this information in accordance with its vigilance system.

***Certain postal, telephonic and electronic business***

106. In the following paragraph the expression "non paying account" is used to mean an account or investment product which does not provide:

(a) cheque or other money transmission facilities; or

(b) the facility for transfer of funds to other types of account which do provide such facilities; or

(c) the facility for repayment or transfer to a person other than the applicant for business whether on closure or maturity of the account, or on realization or maturity of the investment, or otherwise.

107. Given the above definition, where an applicant for business pays or intends to pay monies to an institution by post, or electronically, or by telephoned instruction, in respect of a non-paying account and:

(a) it is reasonable in all the circumstances for payment to be made by such means; and

(b) such payment is made from an account held in the name of the applicant for business at another regulated institution or recognized foreign regulated institution; and

(c) the name/s of the applicant for business corresponds with the name/s of the paying account-holder; and

(d) the receiving institution keeps a record of the applicant's account details with that other institution; and

(e) there is no suspicion of money laundering, the receiving institution is entitled to rely on verification of the applicant for business by that other institution, to the extent that it is reasonable to assume that verification has been carried out and completed.

***Certain mailshots, off-the-page and coupon business***

108. The exemptions set out in paragraphs 106 and 107 also apply to mailshots, off-the-page and coupon business placed over the telephone or by other electronic media. In such cases, the receiving institution should also keep a record of how the transaction arose.

**CASES REQUIRING THIRD PARTY EVIDENCE IN SUPPORT**

***Reliable Introductions***

109. Verification may not be needed in the case of a reliable introduction from a locally regulated institution which does this preferably in the form of a written introduction (see suggested form at Appendix B). Judgment should be exercised as to whether a local introduction may be treated as reliable, utilizing the knowledge which the institution has of local institutions generally, supplemented as necessary by appropriate enquiries. Details of

the introduction should be kept as part of the records of the customer introduced.

110. Verification may not be needed where a written introduction is received from an introducer who is:

(a) a professionally qualified person or independent financial advisor operating from a recognized foreign regulated institution; and

(b) the receiving institution is satisfied that the rules of his/her professional body or regulator (as the case may be) include ethical guidelines, which taken in conjunction with the money laundering regulations in his/her jurisdiction, include requirements at least equivalent to those in these Guidelines; and

(c) the individual concerned is reliable and in good standing and the introduction is in writing, including an assurance that evidence of identity would have been taken and recorded, which assurance may be separate for each customer.

Details of the introduction should be kept as part of the records of the customer introduced.

111. Verification is not needed where the introducer of an applicant for business is either an overseas branch or member of the same group as the receiving institution. In such cases, written confirmation or evidence of the relationship should be obtained from the holding or parent company.

112. To qualify for exemption from verification, the terms of business between the institution and the introducer should require the latter to:

(a) complete verification of all customers introduced to the institution or to inform the institution of any unsatisfactory conclusion in respect of any such customer;

(b) keep records in accordance with these Guidelines; and

(c) supply copies of any such records to the institution upon demand.

113. In the event of any dissatisfaction on any of these, the institution should (unless the case is otherwise exempt) undertake and complete its own verification of the verification subjects arising out of the application for business either by:

(a) carrying out the verification itself; or

(b) relying on the verification of others in accordance with these Guidelines.

Where a transaction involves an institution and an intermediary, each needs separately to consider its own position to ensure that its own obligations regarding verification and records are duly discharged.

114. The best time to undertake verification is not so much at entry as prior to entry. Subject to paragraphs 102 and 112, verification should whenever possible be completed before any transaction is completed. It would not be appropriate to complete settlement of the relevant financial transaction, to transfer or pay any money out to a third party, or dispatch documents of title before adequate verification is obtained.

115. If it is necessary for sound business reasons to open an account or carry out a significant one-off transaction before verification can be completed, this should be subject to stringent controls which should ensure that any funds received are not passed to third parties. Alternatively, a senior member of key staff may give appropriate authority. This authority should not be delegated. Any such decision should be recorded in writing. A suggested form of authority to deal with this type of situation is set out in Appendix C.

116. Verification, once begun, should normally be pursued either to a conclusion or to the point of refusal. If a prospective customer does not pursue an application, key staff may consider that this is in itself suspicious.

117. In the case of telephone business, where payment is or is expected to be made from a bank or other account, the verifier should:

a) satisfy himself/herself that such account is held in the name of the applicant for business at or before the time of payment, and

b) not remit the proceeds of any transaction to the applicant for business or his /her order until verification of the relevant verification subjects has been completed.

**METHODS OF VERIFICATION**

118. These Guidelines do not seek to specify what, in any particular case, may or may not be sufficient evidence to complete verification. They do set out what, as a matter of good practice, may reasonably be expected of institutions. Since, however, these Guidelines are not mandatory or exhaustive, there may be cases where an institution has properly satisfied itself that verification has been achieved by other means which it can justify as reasonable in all the circumstances.

119. Verification is a cumulative process. Except for small one-off transactions, it is not appropriate to rely on any single piece of documentary evidence.

120. The best possible documentation of identification should be required and obtained from the verification subject. For this purpose "best possible" is likely to mean that which is the most difficult to replicate or acquire unlawfully because of its reputable and/or official origin.

121. File copies of documents should, whenever possible, be retained. Alternatively, reference numbers and other relevant details should be recorded.

122. The process of verification should not be unduly influenced by the particular type of account or services being applied for.

123. It is important to obtain references from banks and other professional firms. These references should be requested by the financial institution and be received directly from the banks and other firms providing such references. Under no circumstances should a letter of reference be accepted from the new customer as it could be forged or altered. Verify bank references and document confirmations.

***Individuals***

124. A personal introduction from a known and respected customer and/or member of key staff is often useful but it may not remove the need to verify the subject in the manner provided in these Guidelines. The introduction should in any case contain the full name and permanent address of the verification subject and relevant information contained in paragraph 126.

125. Save in the case of reliable introductions, the institution should, whenever feasible, interview the verification subject in person.

126. The relevance and usefulness in this context of the following information should be considered:

a) full name/s used;

b) date and place of birth;

c) nationality;

d) current permanent address including postal code (Any address primed on a personal account cheque tendered to open the account, if provided, should be compared with the address);

e) telephone and fax number;

f) occupation and name of employer (if self employed, the nature of the self employment); and

g) specimen signature of the verification subject (if a personal account cheque is tendered to open the account, the signature on the cheque should be compared with the specimen signature).

127. In this context "current permanent address" means the verification subject's actual residential address, as it is an essential part of identity.

128. To establish identity the following documents are considered to be appropriate, in descending order of acceptability:

(a) current valid passport;

(b) national identity card;

(c) armed forces identity card; and

(d) driver's licence, which bears a photograph.

129, Documents sought should be pre-signed by, and if the verification subject is met face to face, preferably bear a photograph of, the verification subject.

130. Documents which are easily obtainable in any name should not be accepted uncritically. Examples include:

(a) birth certificates;

(b) credit cards;

(c) business cards;

(d) national health or insurance cards;

(e) provisional health or insurance cards;

(f) provisional driver's licences;

(g) student union cards.

131. It is acknowledged that there will sometimes be cases, particularly involving young persons and the elderly, where the appropriate documentary evidence of identity and independent verification of address are not possible. In such cases a senior member of key staff could authorize the opening of an account if he is satisfied with the circumstances and should record these circumstances in the same manner and for the same period of time as the identification records.

132. If the verification subject is an existing customer of an institution acting as an intermediary in the application, the name and address of that institution and that institution's personal reference on the verification subject should be recorded.

133. If information cannot be obtained from the above-mentioned to enable verification to be completed and the account to be opened, a request may be made to another institution or institutions for confirmation of such information from its/their records. A form of such request for confirmation (as opposed to a mere banker's reference) is set out in Appendix D. Failure of that institution to respond positively and without undue delay should put the requesting institution on its guard.

***Companies***

134. All account signatories should be duly accredited by the company.

135. The relevance and usefulness in this context of the following documents (or their foreign equivalent) should be carefully considered:

(a) Certificate of Incorporation (duly notarized where such body is incorporated in Saint Lucia);

(b) Notice of Directors;

(c) Notice of Secretary;

(d) The most recent annual return filed with the Registrar, duly notarized where such corporate body is incorporated outside Saint Lucia;

(e) The name(s) and address(es) of the beneficial owner/s and/or the person/ s on whose instructions the signatories to the account are empowered to act;

(f) Articles of Association or by laws;

(g) Resolution, Bank Mandate, signed application form or any valid account opening authority, including full names of all directors and their specimen signatures and signed by no fewer than the number of directors required to make up a quorum;

(h) Copies of identification documents should be obtained from at least two directors (if there is more than one) and authorized signatories in accordance with the general procedure for the verification of the identity of individuals;

(i) Copies of Powers of Attorney or other authorities given by the directors in relation to the company;

(j) A signed director's statement as to the nature of the company's business;

(k) A statement of the source of funds and purpose of the account should be completed and signed. This should show the expected turnover or volume of activity in the account;

(l) For large corporate accounts, the following may be obtained: annual reports/audited financial statements, description and place of principal line(s) of business, list of major business units, suppliers and customers, etc. where appropriate; and

(m) A confirmation as described in paragraph 133.

136. As legal controls vary between jurisdictions, particular attention may need to be given to the place of origin of such documentation and the background against which it is produced.

***Partnerships and Unincorporated Businesses***

137. The relevance and usefulness of obtaining the following (or other foreign equivalent) should be carefully considered as part of the verification procedure:

(a) The partnership agreement:

(b) The information listed in paragraph 126 in respect of the partners and managers relevant to the application for business; and

(c) A copy of the mandate from the partnership or unincorporated business authorizing the establishment of the business relationship and confirmation of any authorized signatories.

***Clubs, Societies and Charities***

138. In the case of accounts to be opened for clubs, societies and charities, the financial institution should satisfy itself as to the legitimate purpose of the organization by, for example, requesting a copy of the constitution. Where there is more than one signatory to the account, the identity of at least two signatories should be verified initially and, when signatories change, care should be taken to ensure that the identity of at least two current signatories have been verified.

***Trustees***

139. A trustee should verify the identity of a settler/guarantor or any person adding assets to the trust in accordance with the procedures relating to the verification of identity of clients. In particular, the trustee should obtain the following minimum information:

(a) **Settler or any person transferring assets to the trust:** name, business, trade or occupation, and other information in accordance with the procedures relating to the verification of client identity outlined in these Guidelines;

(b) **Beneficiaries:** name, address and other identification information such as passport number, etc;

(c) **Protector: name,** address, business occupation and any relationship to the senior;

(d) **Purpose and nature of the trust:** a statement of the true purpose of the trust being established, even where it is a purpose or charitable trust;

(e) **Source of funds:** identify and record the source(s) of funds settled on the trust and the expected level of funds so settled; and

(f) **Authorization of payments:** the trustee should also ensure that payments from the trust are authorized and made in accordance with its terms.

***Other Institutions***

140. Signatories should satisfy the provisions of paragraphs 126 onwards as appropriate.

***Politically Exposed Persons (PEPs)***

141. Ongoing enhanced scrutiny must be applied to transactions by senior foreign political figures, their immediate family and closely related persons and entities (i.e politically exposed persons - PEPs). They include:

(a) a senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not);

(b) *a* senior official of a major foreign political party;

(c) any corporation, business or other entity formed by, or for the benefit of, a senior political figure;

(d) 'immediate family' i.e. parents, siblings, spouse, children and in-laws as well as 'close associates' (i.e. person known to maintain unusually close relationship with PEPs).

142. All regulated entities must:

(i) ascertain identity of the account holder and the account's beneficial holder:

(ii) obtain adequate documentation regarding the PEP;

(iii) understand the PEP's anticipated account activity;

(iv) determine the PEP's source of wealth;

(v) apply additional oversight to the PEP's account.

143. Institutions should pay particular attention to:

(a) requests to establish an account with an institution unaccustomed to doing business with foreign persons and that has not sought out business of that type;

(b) requests for secrecy with transaction e.g. booking transaction in the name of another person or entity whose beneficial owner is not disclosed or readily apparent;

(c) use of accounts at the nation's central bank or other government-owned bank, or of government accounts, as the source of funds in a transaction;

(d) routing of transactions into or through a secrecy jurisdiction;

(e) deposits or withdrawals of multi monetary instruments just below reporting threshold on or around the same day;

(f) a pattern, where, after a deposit or wire transfer is received, funds from encashment or investment is shortly thereafter wired to another financial institution (particularly off-shore or secrecy jurisdiction);

(g) frequent minimal balance or zeroing out of an account for purposes other than maximizing the value of the funds held in the account e.g. placing the funds in an overnight investment and having the funds then returned to the account;

(h) enquiry by or on behalf of PEP regarding exceptions to reporting requirements.

144. An institution should consult several sources of information to assist it in determining whether to conduct business with an individual who may be a PEP, including:

(a) reports by non-government organizations that identify corruption, fraud and abuse e.g. Corruption Perceptions Index of Transparency International;

(b) reports on corruption and money laundering issued by international financial institutions e.g. World Bank, and the International Monetary Fund (IMF);

(c) information published on the World Wide Web by foreign countries;

(d) the World Fact Book published by the Central Intelligence Agency (CIA).

***Risk-based (KYC)***

145. The means and mechanisms of laundering funds change. Accordingly institutions should be aware of emerging trends which create a greater risk for money laundering. Primary concern should be for determining the legitimacy of the source of funds entering the financial system and the real owners of these funds. Risks may be categorized as high or low depending on the circumstances.

146. ***Low Risk Indicators***

(a) Those facility holders identified in regulation 103 as exempt e.g. licensed financial institutions and other institutions which are subject to these Guidelines;

(b) Saint Lucian residents whose accounts/facilities are serviced solely either by salary deductions, or financing arrangements via regulated financial institutions.

147. ***High Risk Indicators***

(a) Intermediary arrangements (where the real or beneficial owner of the funds is not the facility holder); Anonymity factor;

(b) Financial service intermediaries that are not subject to prudential regulation;

(c) Non Saint Lucian residents;

(d) Large cash transaction;

(e) Transactions from countries or jurisdictions which have inadequate AML systems. The Financial Action Task Force has a listing of Non-Cooperative countries and Territories ("NCCT"), which can be found at the website http://www.oecd.org/fatf/NCCT_en.htm Countries included in this listing should be treated as having financial institutions with no or poorly regulated AML systems;

(f) Persons resident in or maintaining trading operations in locations that are known to have significant established organized crime environments;

Country Trends:

The following regions are considered to be high risk in terms of laundering activities:

(i) Latin America;

(ii) Pacific Rim Region;

(iii) Central and South America;

(iv) Central and Eastern Europe;

(v) Africa (in particular, West Africa);

(g) Persons resident in or maintaining trading operations in known drug producing/transshipment locations;

(h) Persons from or maintaining trading operations in locations that are experiencing political instability or with a history of this;

(i) PEPs.

Institutions are required to implement enhanced due diligence for transactions involving high risk activities. This requires:

(i) stricter know-your-customer procedures e.g. more detailed information on customer's background, reputation, etc;

(ii) management information systems in order to monitor accounts with greater frequency than low risk accounts;

(iii) senior management approval for establishment of accounts;

(iv) senior management to monitor accounts.

## RESULTS OF VERIFICATION

### *Satisfactory*

148. Once verification has been completed (and subject to the keeping of records in accordance with these Guidelines), no further evidence of identity is needed when transactions are subsequently undertaken, **except** *in* cases where either doubt arises as to the identity of the client or about the veracity or adequacy of previously obtained customer identification data. Where doubts arise, the entire due diligence process must be carried out anew, from start to finish. This is known as the "duty of continuous verification."

149. The duty of continuous verification also requires the institution to monitor accounts for their consistency continuously against the stated account purpose or the source of funds, or pattern.

150. The file of each applicant for business should show the steps taken and the evidence obtained in the process of verifying each verification subject or, in the appropriate cases, details of the reasons which justify the case being an exempt case.

### *Unsatisfactory*

151. In the event of a failure to complete verification of any relevant verification subject or where there are no reasonable grounds for suspicion, any business relationship with, or one-off transaction for, the applicant for business should be suspended and any funds held to the applicant's order returned in the form in which it was received, until verification is subsequently completed (if at all). Funds should never be returned to a third party but only to the source from which they came. If failure to complete verification itself raised suspicion, a report should be made to the Reporting Officer/ Compliance Officer for determination as to how to proceed. Generally institutions should consider making a suspicious transaction report when unable to obtain satisfactory evidence or verification of identity of customers or beneficial owners.

## RECOGNITION OF SUSPICIOUS CUSTOMERS/TRANSACTIONS

152. A suspicious transaction will often be one which is inconsistent with a customer's known legitimate business or activities or with the normal business for that type of account. It follows that an important pre-condition of recognition of a suspicious transaction is for the institution to know enough about the customer's business to know that a transaction or series of transactions is / are unusual.

153. Although these Guidelines tend to focus on new business relationships and transactions, institutions should be alert to the implications of the financial flows and transaction patterns of existing customers, particularly where

there is a significant unexpected and unexplained change in the behaviour of the account.

154. Against such patterns of legitimate business, suspicious transactions should be recognizable as falling into one or more of the following categories:

a) any unusual financial activity of the customer in the context of his own usual activities;

b) any unusual transaction in the course of his usual financial activity;

c) any unusually linked transactions;

d) any unusual employment of an intermediary in the course of some usual transaction or financial activity;

e) any unusual method of settlement; and

f) any unusual or disadvantageous early redemption of an investment product.

155. From time to time, the authorities or management may determine that because a high incidence of money laundering is associated with persons from certain countries or regions, additional precautions are required to safeguard against use of accounts or other facilities by such persons, their immediate relatives, associates and representatives. The source of wealth and economic activities that generated the level of wealth should be substantiated. Under these circumstances, it may be necessary to request a letter of reference (confirmed), in addition to other identification requirements, from a regulated bank which is not from the countries or regions in question.

156. The Compliance Officer should be well versed in the different types of transactions which the institution handles and which may give rise to opportunities for money laundering. Examples of common and relevant transaction types, are set out in Appendix A. These are not intended to be exhaustive.

**REPORTING OF SUSPICIONS**

157. Reporting of suspicions is an important defence against possible accusation of assisting in the retention or control of the proceeds of money laundering/ criminal conduct, or of acquiring, possessing or using the proceeds of criminal conduct. In practice, a Compliance Officer will normally only have suspicion, without having any particular reason to suppose that the suspicious transaction or other circumstances relate to the proceeds of one sort of crime or another.

158. It should be noted in this context that the suspicion of criminal conduct is more than the absence of certainty that someone is innocent. It is rather an inclination to believe that there has been criminal conduct.

159. Institutions should ensure:

(a) that key staff know to whom their suspicions should be reported; and

(b) that there is a clear procedure for reporting such suspicions without delay to the Compliance Officer.

A suggested format of an internal report form is set out in Appendix E.

160. Key staff should be required to report any suspicion of laundering either directly to their Compliance Officer, or if the institution so decides, to their line manager for preliminary investigation in the event that there are any known facts which may negate the suspicion.

161. Employees should comply at all times with the approved vigilance systems of their institution and will be treated as having met appropriate standards of vigilance if they disclose their suspicions to the Compliance Officer or other appropriate senior colleague according to the vigilance systems in operation in their institutions.

162. On receipt of a report concerning a suspicious customer or a suspicious transaction, the Compliance Officer should determine whether the information contained in such report supports the suspicion. He should investigate the details in order to determine whether in all the circumstances he in turn should submit a report to the FIA.

163. If the Compliance Officer decides that the information does substantiate *a* suspicion of laundering, he/she should disclose this information immediately. If he/she is genuinely uncertain as to whether such information substantiates a suspicion, he/she should nevertheless report. If in good faith he/she decides that the information does not substantiate a suspicion, he/she would be well advised to record fully the reasons for his/her decision not to report to the FIA in the event that his judgment is later found to be wrong.

164. It is for each institution or group to consider whether its vigilance systems should require the Compliance Officer to report suspicions within the institution or group to the inspection or compliance department at head office.

**REPORTING TO THE FINANCIAL INTELLIGENCE AUTHORITY**

165. If the Compliance Officat a disclosure should be made, a report preferably in the form set out in Appendix F should be sent to the FIA.

166. If the Compliance Officer considers that a report should be made urgently (e.g. where the account is already part of a current investigation), initial notification to FIA should be made by facsimile.

167. The receipt of a report will be promptly acknowledged by the FIA. The report will be forwarded to trained financial investigation officers who alone will have access to it. They may seek further information from the

reporting institution and elsewhere. It is important to note that after a reporting institution makes an initial report in respect of a specific suspicious transaction, that initial report does not relieve the institution of the need to report further suspicions in respect of the same customer or account and the institution should report any further suspicious transactions involving the customer.

168. Discreet inquiries will be made to confirm the basis of the suspicion but the customer is never approached. In the event of a prosecution the source of the information is protected, as far as the law allows. Maintaining the integrity of the confidential relationship between law enforcement agencies and institutions is regarded by the former as of paramount importance.

169. Vigilance systems should require the maintenance of a register of all reports made to the FIA pursuant to this paragraph. Such register should contain details of:

a) the date of the report;

b) the person who made the report;

c) the person/s to whom the report was forwarded;

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

e) the receipt of acknowledgement from the FIA.

**KEEPING OF RECORDS**

170. Once a business relationship has been established, the institution is required to maintain all relevant records on the identity and transactions of their customers, both locally and internationally, for seven (7) years, or longer if required by the Authority.

171. It may be necessary for institutions to retain business transaction records for a period exceeding the date of termination of the last business transaction where certain circumstances predate this event, for example:

(a) date of closure of the account;

(b) date of termination of business relationship; or

(c) date of insolvency.

**TIME LIMITS**

172. In order to facilitate the investigation of any audit trail concerning the transactions of their customers, institutions should observe the following:

*(a)* ***Entry*** **records:** institutions should keep all account opening records. including verification documentation and written introductions, for a period of at least **7 years** after *termination* or, where an account has become dormant, seven years from the last transaction.

(b) **Ledger records:** institutions should keep all account ledger records for a period of at least **7 years** following the date on which the relevant transaction or series of transactions is completed.

(c) **Supporting records:** institutions should keep all records in support of ledger entries, including credit and debit slips and cheques, for a period of at least **7 years** following the date on which the relevant transaction or series of transactions is completed.

173. Where an investigation into a suspicious customer or a suspicious transaction has been initiated, the FIA may request an institution to keep records until further notice, notwithstanding that the prescribed period for retention has elapsed. Even in the absence of such a request, where an institution knows that an investigation is proceeding in respect of its customer, it should not, without the prior approval of the FIA, destroy any relevant records even though the prescribed period for retention may have elapsed.

**CONTENTS OF RECORDS**

174. Records in relation to verification will generally comprise:

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

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

175. Institutions should retain customer identification records, current files and business correspondence since it may be necessary to establish a financial profile of any suspected account as part of an investigation. To satisfy this requirement, additional information such as the following may be sought:

(a) volume of funds flowing through the account;

(b) origin of the funds;

(c) forms by which the funds were offered or withdrawn, e.g. cash or cheque;

(d) identification of the person undertaking the transaction including the names and address of the beneficial owners of the account or product and also any counter-party;

(e) form of instruction and authority.

176. Details of securities and investments transacted including:

a) the nature of such securities/investments;

b) valuation(s) and price(s);

c) memoranda of purchase and sale;

d) source(s) and volume of funds and bearer securities;

e) destination(s) of funds and bearer securities;

f) memoranda of institution(s) arid authority(ies);

g) book entries;

h) custody of title documentation;

i) the nature of the transaction;

j) the date of the transaction; and

k) the form (e.g. cash, cheque) in which funds are offered and paid out.

177. Institutions should document a formal anti-money laundering policy including evidence of compliance with sections 9(1)(f) and 11(b) of the Act relating to audit and training. At a minimum, records should be maintained on the following:

(a) details and contents of the training programme;

(b) names of staff receiving training;

(c) dates of training sessions; and

(d) assessment of training.

178. In the case of electronic transfers, institutions should retain records of payments made with sufficient detail to enable them to establish:

(a) the identity and address of the remitting customer;

(b) origin of the funds (the account number, when being transferred from an account);

(c) as far as possible the identity of the ultimate recipient;

(d) the form of instruction and authority; and

(e) destination of the funds.

179. In circumstances where electronic transfers do not give complete originator information, institutions are required to give enhanced scrutiny to these.

180. All institutions should maintain transaction records in such a manner that will allow them to comply expeditiously with information requests from the Authority. The records must be sufficient to permit reconstruction of individual transactions.

181. A retrievable form may consist of:

(a) an original hard copy;

(b) copies;

(c) microform; or

(d) computerized or electronic form.

182. Records held by third parties are not regarded as being in a readily retrievable form unless the institution is reasonably satisfied that the third party is itself an institution which is able and willing to keep such records and disclose them to it when required.

183. Where the FIA requires sight of records which according to an institution's vigilance systems would ordinarily have been destroyed, the institution is nonetheless required to conduct a search for those records and provide as much detail to the FIA as is possible.

**REGISTER OF ENQUIRIES**

184. An institution should maintain a register of all enquiries made to it by the FIA. The register should be kept for a period of at least 7 years and separate from other records and should contain at a minimum the following details:

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

(b) details of the account(s) involved.

**STAFF TRAINING**

185. Institutions have a duty to ensure that key staff receive sufficient training to alert them to the circumstances whereby they should report customers/ clients and/or their transactions to the Compliance Officer. Such training should include making key staff aware of the basic elements of:

(a) the Act and any Regulations made thereunder, and in particular the personal obligations of key staff thereunder, as distinct from the obligations of their employers thereunder;

(b) vigilance policy and vigilance systems;

(c) the recognition and handling of suspicious transactions;

(d) other pieces of anti- money laundering legislation identified at the beginning of these Guidelines;

(e) any Code of Conduct/Practice issued under regulatory legislation or voluntarily adopted by various industry associations; and

(f) any additional guidelines and instructions issued by the FIA.

186. The effectiveness of a vigilance system is directly related to the level of awareness engendered in key staff, both as to the background of international crime against which the Act and other anti-money laundering legislation

have been enacted including these Guidelines as well as to the personal legal liability of each of them for failure to perform the duty of vigilance and to report suspicions appropriately.

**TRAINING PROGRAMMES**

187. While each institution should decide for itself how to meet the need to train members of its key staff in accordance with its particular commercial requirements, the following programmes will usually be appropriate:

188. ***Generally***

Training should include:

(a) the company's instruction manual;

(b) a description of the nature and processes of laundering;

(c) an explanation of the underlying legal obligations contained in the Act and any Regulations made thereunder; and other anti-money laundering legislation and guidelines;

(d) an explanation of vigilance policy and systems, including particular emphasis on verification and the recognition of suspicious transactions and the need to report suspicions to the Compliance Officer (or equivalent).

189. ***Specific Appointees***

**(a) Cashier/foreign exchange operators/dealers/salespersons/advisory staff**

Key staff who are dealing directly with the public are the first point of contact with money launderers and their efforts are vital to the implementation of vigilance policy. They need to be aware of their legal responsibilities and the vigilance systems of the institution, in particular the recognition and reporting of suspicious transactions. They also need to be aware that the offer of suspicious funds or the request to undertake a suspicious transaction should be reported to the Compliance Officer in accordance with vigilance systems, whether or not the funds are accepted or the transaction proceeded with.

**(b) Account opening/new customer and new business staff/processing and settlement staff**

Key staff who deal with account opening, new business and the acceptance of new customers, or who process or settle transactions and/or the receipt of completed proposals and cheques, should receive the training given to cashiers, etc. In addition, verification should be understood and training should be given in the institution's procedures

for entry and verification. Such staff also needs to be aware that the offer of suspicious funds or the request to undertake a suspicious transaction may need to be reported to the Compliance Officer in accordance with vigilance systems, whether the funds are accepted or the transaction proceeded with.

**(c) Administration/operations supervisors and managers**

A higher level of instruction covering all aspects of vigilance policy and systems should be provided to those with the responsibility for supervising or managing staff. This should include:

(i) the Act and any Regulations made thereunder;

(ii) the offences and penalties arising from the relevant primary legislation for non-reporting or assisting money launderers;

(iii) procedures in relation to the service of production and restraint orders;

(iv) internal reporting procedures; and

(v) the requirements for verification and records.

**(d) Compliance Officers**

In depth training concerning all aspects of the relevant laws, vigilance policy and systems will be required for the Compliance Officer. In addition, the Compliance Officer will require extensive initial and continuing instruction on the validation and reporting of suspicious transactions, on the feedback arrangements and on new trends of criminal activity.

**(e) Updates and Refreshers**

It will also be necessary to make arrangements for updating and refresher training at regular intervals to ensure that key staff remain familiar with and are updated as to their responsibilities.

## PART IV

## VULNERABILITY OF FINANCIAL SECTOR BUSINESS TO MONEY LAUNDERING

### SECTION A: BANKING

190. In addition to this Part, all banking institutions whether on shore or offshore are expected to comply with the provisions of Part III of these Guidelines. Because commercial banking is heavily cash based, it is particularly at risk from the placement of criminal proceeds.

**VIGILANCE**

191. Vigilance should govern all the stages of the bank's dealings with its customers including:

(a) accounts opening;

(b) non-account holding customers;

(c) safe custody and safe deposit boxes;

(d) deposit-taking;

(e) lending;

(f) marketing and self-promotion.

***Account Opening***

192. In the absence of a satisfactory explanation, the following should be regarded as suspicious customers:

(a) a customer who is reluctant to provide usual or customary information or who provides only minimal, false or misleading information;

(b) a customer who provides information which is difficult or expensive for the bank to verify.

***Non-account holding customers***

193. Banks which undertake transactions for persons who are not account holders with them should be particularly careful to treat such persons (and any underlying beneficial owners of them) as verification subjects.

***Safe custody and safe deposit boxes***

194. Particular precaution need to be taken in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such facilities are made available to non-account holders, the verification procedures set out in these Guidelines should be followed.

***Deposit taking***

195. In the absence of a satisfactory explanation, the following should be regarded as suspicious transactions:

(a) substantial cash deposits, singly or in accumulations, particularly when:

(i) the business in which the customer is engaged would normally be conducted, not in cash or in such amounts of cash, but by cheques, banker's drafts, letters of credit, bills of exchange, or other instruments;

(ii) such a deposit appears to be credited to an account only for the purpose of supporting the customer's order for a banker's draft, money transfer or other negotiable or readily marketable money instrument;

(iii) deposits are received by other banks and the bank is aware of a regular consolidation of funds from such accounts prior to a request for onward transmission of funds unless the bank is aware of any commercial reason why the transmission should be done;

(iv) the customer or its representatives avoid direct contact with the bank;

(v) the use of nominee accounts, trustee accounts or client accounts which appear to be unnecessary for, or inconsistent with, the type of business carried on by the underlying customer/beneficiary;

(vi) the use of numerous accounts for no clear commercial reason where fewer would suffice (as this may suggest an attempt to disguise the scale of the total cash deposits);

(vii) the use by the customer of numerous individuals (particularly persons whose names do not appear on the mandate for the account) to make deposits;

(viii) frequent insubstantial cash deposits which taken together are substantial;

(ix) there are frequent switches of funds between accounts in different names in different jurisdictions;

(x) matching of payments out with credits paid in by cash on the same or previous day;

(xi) substantial cash withdrawal takes place from a previously dormant or inactive account;

(xii) substantial cash is withdrawn from an account which has just received an unexpected large credit from overseas; and

(xiii) making use of a third party (e.g. a professional firm or trust company) to deposit cash or negotiable instruments, particularly if these are promptly transferred between clients or trust accounts.

***Lending***

196. It needs to be borne in mind that loan and mortgage facilities (including the issuing of credit and charge cards) may be used by launderers at the **layering** or **integration** stages.

***Marketing and self-promotion***

197. In the absence of a satisfactory explanation, a customer may be regarded as suspicious if:

(a) he declines to provide information which normally would make him eligible for valuable credit or other banking services; or

(b) he makes insufficient use of normal banking facilities, such as higher interest rate facilities for large credit balances.

**VERIFICATION**

198. For general guidance on verification, banks should refer to the relevant heading under these Guidelines.

199. Where a customer of one part of a bank applies for business at another part of the bank and the former has completed verification (including that of all the verification subjects related to that applicant), no further verification is required by the latter as long as the verification records are freely available to the bank.

200. When requested, either directly or through an intermediary to open an account for a company or trust administered by a local fiduciary, a bank should ordinarily expect to receive an introduction (on the lines of Appendix B) in respect of every verification subject arising from that application (See also paragraph 208).

**SECTION B: INVESTMENT BUSINESS**

201. Regulated institutions which provide investment services, should comply with the provisions of Part III of these Guidelines.

**RISKS OF EXPLOITATION**

202. Because the management and administration of investment products is not generally cash based, it is probably less at risk from the placement of criminal proceeds than is much of the banking sector. Most payments are made by way of cheque or transfer from another institution and it can therefore be assumed that in a case of laundering, placement has already been achieved. Nevertheless, the purchase of investments for cash is not unknown, and therefore the risk of investment business being used at the placement stage cannot be ignored. Payment in cash will therefore need further investigation, particularly where it cannot be supported by evidence of a legitimate cash-based business as the source of funds.

203. Funds management is likely to be at particular risk at the layering stage of laundering. The liquidity of investment products under management is attractive to launderers since it allows them quickly and easily to move the criminal proceeds from one product to another, mixing them with lawful proceeds and facilitating integration.

204. Fund management is also at risk at the integration stage in view of:

(a) the easy opportunity to liquidate investment portfolios containing both lawful and criminal proceeds, while concealing the nature and origins of the criminal proceeds;

(b) the wide variety of available investments;

(c) the ease of transfer between investment products.

205. The following investments are particularly at risk:

(a) collective investment schemes and other "pooled funds" (especially where unregulated);

(b) high risk/high reward funds (because the launderers cost of funds is by definition low and the potentially high reward accelerates the integration process).

***Borrowing against security of investments***

206. Secured borrowing is an effective method of layering and integration because it puts a legitimate financial business (the lender) with a genuine claim to the security in the way of those seeking to restrain or confiscate the assets.

**VERIFICATION**

207. Mutual funds, fund managers and administrators will note the particular relevance in their case of exemptions to the need for verification set out in Part III above.

***Customers dealing direct***

208. Where a customer deals with a mutual fund, fund manager or administrator direct, the customer is the applicant for business to the fund manager or administrator and accordingly determines who the verification subject(s) is / (are). In the exempt case referred to in respect of mailshot, off-the-page or coupon business, a record should be maintained indicating how the transaction arose and recording details of the paying institution's branch sort code number and account number from which the cheque or payment is drawn.

***Intermediaries and underlying customers***

209. Where an agent/intermediary introduces a principal/customer to the mutual fund or fund manager and the investment is made in the principal's/ customer's name, then the principal/customer is the verification subject. For this purpose it is immaterial whether the customer's own address is given or that of the agent/intermediary.

***Nominees***

210. Where an agent/intermediary acts for a customer, whether for a named client or through a client account, but deals in his own name, then the agent/intermediary is a verification subject and (unless the applicant for business is a recognized foreign regulated institution under Part III) the customer is also a verification subject.

211. It the applicant for business is a recognized foreign regulated institution, identified under Part III, the fund manager may rely on an introduction from the applicant for business (or written assurance that it will have verified any principal/customer for whom it acts as agent/intermediary).

***Delay in verification***

212. If verification has not been completed within a reasonable time, then the business relationship or significant one-off transaction in question should not proceed any further.

213. Where an investor has the benefit of cancellation rights, or cooling off rights, the repayment of money arising in these circumstances (subject to any shortfall deduction where applicable) does not constitute "proceeding further with the business." However, since this could offer a route for laundering money, investment businesses should be alert to any abnormal exercise of cancellation/cooling off rights by any investor, or in respect of business introduced through any single authorized intermediary. In the event that abnormal exercise of these rights become apparent, the matter should be treated as suspicious and reported through the usual channels. In any case, repayment should not be to a third party.

***Redemption prior to completion of verification***

214. Whether a transaction is a significant one-off transaction or is carried out within a business relationship, verification of the customer should normally be completed before the customer receives the proceeds of redemption. However, a mutual fund, a fund manager or an administrator will be considered to have taken reasonable measures of verification where payment is made either:

(a) to the legal owner of the investment by means of a cheque where possible crossed "account payee"; or

(b) to a bank account held (solely or jointly) in the name of the legal holder of the investment by any electronic means of transferring funds.

***Switch transactions***

215. A significant one-off transaction does not give rise to a requirement of verification if it is a switch under which all of the proceeds are directly re-invested in another investment which itself can, on subsequent resale, only result in either:

(a) a further reinvestment on behalf of the same customer; or

(b) a payment being made directly to him and of which a record is kept.

**Savings vehicles and regular investment contracts**

216. Except in the case of a small one-off transaction (and subject always to any exemptions identified in Part III) where a customer has:

(a) agreed to make regular subscriptions to a mutual fund, and

(b) arranged for the collection of such subscriptions (e.g. by completing a direct debit mandate or standing order), the mutual fund, fund manager or administrator should undertake verification of the customer (or satisfy himself that the case is otherwise exempt under Part III above).

217. Where a customer sets up a regular savings scheme whereby money subscribed by him is used to acquire investments to be registered in the name or held to the order of a third party, the person who funds the cash transactions is to be treated as the verification subject. When the investment is realized, the person who is the legal owner (if not the person who funded it) is also to be treated as a verification subject.

***Reinvestment of income***

218. A number of retail savings vehicles offer customers the facility to have income reinvested. The use of such a facility should be seen as entry into a business relationship and the reinvestment of income under such a facility should not be treated as a transaction which triggers the requirement of verification.

**SECTION C: FIDUCIARY SERVICES**

219. For the purpose of these Guidelines "fiduciary services" comprise any of the following activities carried on as a business, either singly or in combination:

(a) formation and/or administration of trusts;

(b) acting as corporate and/or individual trustee;

(c) formation and/or administration of Saint Lucia and/or foreign-registered companies;

(d) provision of corporate and/or individual directors;

(e) opening and/or operating bank accounts on behalf of clients. A "fiduciary" is any person carrying on any such business in or from within Saint Lucia. Fiduciaries should comply with the provisions of Part III of these Guidelines.

**VERIFICATION**

220. Good practice requires key staff to ensure that engagement documentation (client agreement, etc.) is duly completed and signed at the time of entry.

221. Verification of new clients should include the following or equivalent steps:

(a) Where a settlement is to be made or when accepting trusteeship from a previous trustee, the sealer, and/or where appropriate the principal beneficiary (ies), should be treated as verification subjects;

(b) In the course of the formation of companies, the identity of beneficial owners should be verified;

(c) The documentation and information concerning a new client for use by the administrator who will have day-to-day management of the new client's affairs should include a note on any required further input on verification from any agent/intermediary of the new client, together with a reasonable deadline for the supply of such input. After which suspicion should be considered aroused.

***Client Acceptance Procedures***

*222.* **Annual Audit Statement**

A service provider should obtain a separate report on its compliance with the client acceptance procedures from an independent auditor.

223. **Procedures for a Professional Service Client "PSC"**

(a) The definition of "PSC" is any organization or person, such as a law firm, accountant, banks trust companie, company management companies and similar professional organizations who contract the services of a service provider on behalf of their clients.

(b) A service provider should obtain from each PSC which instructs a service provider, details of the business address, contact communication numbers and principals or professionals involved in the PSC. A service provider should obtain evidence of first hand involvement in the verification of those details.

(c) A service provider should obtain satisfactory sources of reference to provide adequate indication of the reputation and standing of the PSC.

(d) A service provider should retain records for a period of seven **(7) years** following the discontinuation of the service provided to the PSC.

(e) Before a service provider undertakes to form a company on the instructions of a PSC, the service provider should take reasonable steps to ensure that the PSC has adequate due diligence procedures in place.

(f) Where, prior to the coming into force of any enactment or a code of conduct, the information and agreement referred to in this part has not been obtained by a service provider, the service provider should have regard to the same in future dealing with the End User Client (EUC) or the PSC, and should endeavour to obtain the same as and when the opportunity arises but should within a year seek to produce the required information and agreement.

***224.*** **Procedures for End User Clients "EUC"**

(a) The definition of "EUC" is a client of a service provider who contracts the services of a service provider for its own benefit.

(b) A service provider should maintain written procedures to ensure that the identity of each EUC is known.

(c) A service provider should maintain records for a period of seven (7) years following the discontinuation of the service provided to the EUC.

(d) A service provider should maintain on its files a reference from a banking organisation being a service provider of a recognized banking body or from a professional service organization in respect of the EUC.

(e) When a service provider is instructed by an individual, the service provider should maintain on its file a copy of the individual's passport or identity card with photo identification.

(f) A service provider should maintain on its file contact communication numbers and addresses for each EUC and should annually remind the EUC that it should notify the service provider within a reasonable period of any change of such EUC's communication numbers and addresses and that it should advise the service provider of any changes in share ownership which are required to be reflected in the share register of any company incorporated on behalf of the EUC.

(g) Where, prior to the coming into force of any enactment or a code of conduct in relation to service providers, a service provider has not obtained communication numbers, addresses, references or passport or identity card with photo identification as referred to herein, the service provider should endeavour to obtain any such items as and when the opportunity arises.

**Additional Requirement Where Fiduciary Services are Provided**

225. A service provider should to the extent relevant to the services being provided, maintain on its files evidence of the opening of the bank and investment accounts, and copies of statements of those accounts.

226. A service provider should, to the extent relevant to the services being provided, maintain on its files in respect of clients for whom it provides fiduciary services:

(a) copies of minutes of meetings of shareholders;

(b) copies of minutes of meetings of directors;

(c) copies of minutes of meetings of committees;

(d) copies of registers of beneficial owners, directors and offices; and

(e) copies of registers of mortgages, charges and other encumbrances.

227. Where instructions are accepted by a service provider to act as trustee for a trust, the service provider should obtain satisfactory references in accordance with the above on the party giving the instructions for the engagement or appointment of a new trustee. The service provider should satisfy itself that assets settled into the trust are not or were not made as part of a criminal or illegal transaction or disposition of assets.

**SECTION D: INSURANCE**

228. Regulated institutions which provide insurance business need to comply with the provisions in Part III of these Guidelines.

229. Insurance business, whether life assurance, term assurance, pensions, annuities or any type of assurance and insurance business, presents a number of opportunities to the criminal for laundering at all its stages. At its simplest this may involve placing cash in the purchase of a single premium product from an insurer followed by early cancellation and reinvestment, or the setting up of an offshore insurance company into which to channel cash obtained illegally in the guise of premiums.

**VERIFICATION**

230. Whether a transaction will result in an entry into a significant one-off transaction and/or is to be carried out within a business relationship, verification of the customer should be completed prior to the acceptance of any premiums from the customer and/or the signing of any contractual relationship with an applicant for business.

***Switch transactions***

231. A significant one-off transaction does not give rise to a requirement of verification if it is a switch under which all of the proceeds are directly paid to another policy of insurance which itself can, on subsequent surrender, only result in either:

(a) a further premium payment on behalf of the same customer; or

(b) a payment being made directly to him and of which a record is kept.

***Payments from one policy of insurance to another for the same customer***

232. A number of insurance vehicles offer customers the facility to have payments from one policy of insurance to fund the premium payments to another policy of insurance. The use of such a facility should not be seen as entry into a business relationship and the payments under such a facility should not be treated as a transaction which triggers the requirement of verification.

***Employer-sponsored pension or savings schemes***

233. In all transactions undertaken on behalf of an employer-sponsored pension or savings scheme, the insurer should undertake verification of:

(a) the principal employer; and

(b) the trustees of the scheme (if any).

234. Verification of the principal employer should be conducted by the insurer in accordance with the procedures for verification of corporate applicants for business.

235. Verification of any trustees of the scheme should be conducted and will generally consist of an inspection of the trust documentation, including:

(a) the trust deed and/or instrument and any supplementary documentation;

(b) a memorandum of the names and addresses of current trustees (if any);

(c) extracts from public registers;

(d) references from professional advisers or investment managers.

***Verification of members: without personal investment advice***

236. Verification is not required by the insurer in respect of a recipient of any payment of benefits made by or on behalf of the employer or trustees (if any) of an employer sponsored pension or savings scheme if such recipient does not seek personal investment advice.

***Verification of members: with personal investment advice***

237. Verification is required by the insurer in respect of an individual member of an employer sponsored pension or savings scheme if such member seeks personal investment advice, save that verification of the individual member may be treated as having been completed where:

(a) verification of the principal employer and the trustees of the scheme (if any) has already been completed by the insurer; and

(b) the principal employer confirms the identity and address of the individual member to the insurer in writing.

**RECORDS**

238. Records should be kept by the insurer after termination in accordance with Part III. In the case of a life company, termination includes the maturity or earlier termination of the policy.

239. As regards records of transactions, insurers should ensure that they have adequate procedures:

(a) to access initial proposal documentation including, where these are completed, the client financial assessment (the "fact find"), client needs analysis, copies of regulatory documentation, details of the payment method, illustration of benefits, and copy documentation in support of verification by the insurers;

(b) to access all post-sale records associated with the maintenance of the contract, up to and including maturity of the contract; and

(c) to access details of the maturity processing and/or claim settlement including completed "discharge documentation".

240. In the case of long-term insurance, records usually consist of full documentary evidence gathered by the insurer or on the insurer's behalf between entry and termination. If an agency is terminated, responsibility for the integrity of such records rests with the insurer as the product provider.

241. If an appointed representative of the insurer is itself registered or authorized under the relevant legislation, the insurer, as principal, can rely on the representative's assurance that he will keep records on the insurer's behalf. (It is of course open to the insurer to keep such records itself. In such a case it is important that the division of responsibilities be clearly agreed between the insurer and such representative).

242. If the appointed representative is not itself so registered or authorized, it is the direct responsibility of the insurer as principal to ensure that records are kept in respect of the business that such representative has introduced to it or effected on its behalf.

**SECTION E: INTERNET AND CYBERBUSINESS**

243. Any financial institution offering services over the internet should implement procedures to verify the identity of its clients. Care should be taken to ensure that the same supporting documentation is obtained from internet customers as for other customers particularly where face to face verification is not practical. In view of the additional risks of conducting business over the internet, financial institutions should monitor activity in customer accounts opened on the internet on a regular basis.

## PART V

## APPENDICES

## APPENDIX A

### EXAMPLES OF SUSPICIOUS TRANSACTIONS

(1) **MONEY LAUNDERING USING CASH TRANSACTIONS**

(a) Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.

(b) Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.

(c) Customers who deposit cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.

(d) Company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.).

(e) Customers who constantly pay in or deposit cash to cover requests for money transfers, bankers' drafts or other negotiable and readily marketable money instruments.

(f) Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.

(g) Frequent exchange of cash into other currencies.

(h) Branches that have a great deal more cash transactions than usual. (Head Office statistics detect aberrations in cash transactions).

(i) Customers whose deposits contain counterfeit notes or forged instruments.

(j) Customers transferring large sums of money to or from overseas locations with instruments for payment in cash.

(k) Large cash deposits using night safe facilities, thereby avoiding direct contact with bank staff.

2. **MONEY LAUNDERING USING BANK ACCOUNTS**

(a) Customers who wish to maintain a number of trustee or client accounts which do not appear consistent with the type of business, including transactions which involve nominees.

(b) Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.

(c) Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).

(d) Reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the institution to verify.

(e) Customers who appear to have accounts with several institutions within the same locality, especially when the bank is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.

(f) Matching of payments out with credits paid in cash on the same or previous day.

(g) Paying in large third party cheques endorsed in favour of the customer.

(h) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

(i) Customers who together simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.

(j) Greater use of safe deposit facilities; increased activity by individuals.

(k) The use of sealed packets deposited and withdrawn.

(l) Companies' representatives avoiding contact with the branch.

(m) Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other clients, company and trust accounts.

(n) Customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.

(o) Insufficient use of normal banking facilities (e.g. avoidance of high interest rate facilities for large balances).

(p) Large number of individuals making payments into the same account without an adequate explanation.

**3. MONEY LAUNDERING USING INVESTMENT RELATED TRANSACTIONS**

(a) Purchasing of securities to be held by the institution in safe custody, where this does not appear appropriate given the customer's apparent standing.

(b) Request by customers for investment management or administration services (either foreign currency securities) where the source of the funds is unclear or not consistent with the customer's apparent standing.

(c) Large or unusual settlements of securities in cash form.

(d) Buying and selling of a security with no discernible purpose or in circumstances, which appear unusual.

4. **MONEY LAUNDERING BY OFFSHORE INTERNATIONAL ACTIVITY**

(a) Customer introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent.

(b) Use of letters of credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

(c) Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.

(d) Unexplained electronic fund transfers by customers, foreign currency drafts or other negotiable instruments to be used.

(e) Frequent requests for traveler's cheques or foreign currency drafts or other negotiable instruments to be issued.

(f) Frequent paying in of travelers' cheques or foreign currency drafts particularly if originating from overseas.

5. **MONEY LAUNDERING INVOLVING FINANCIAL INSTITUTION EMPLOYEES AND AGENTS**

(a) Changes in employee characteristics, (e.g. lavish lifestyles or avoiding taking holidays).

(b) Changes in employee or agent performance, (e.g. the salesman selling products for cash has remarkable or unexpected increase in performance).

(c) Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

## 6. MONEY LAUNDERING BY SECURED AND UNSECURED LENDING

(a) Customers who repay problem loans unexpectedly.

(b) Request to borrow against assets held by the institution or a third party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.

(c) Request by a customer for an institution to provide or arrange finance where the source of the customer's financial contribution to deal is unclear, particularly where property is involved.

## 7. SALES AND DEALING STAFF

### (a) New Business

Although long-standing customers may be laundering money through an investment business it is more likely to be a new customer who may use one or more accounts for a short period only and may use false names and fictitious companies. Investment may be direct with a local institution or indirect via an intermediary who "doesn't ask too many awkward questions", especially (but not only) in a jurisdiction where money laundering is not legislated against or where the rules are not rigorously enforced.

The following situations will usually give rise to the need for additional enquiries:

(i) A personal client for whom verification of identity proves unusually difficult and who is reluctant to provide details.

(ii) A corporate/trust client where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation.

(iii) A client with no discernible reason for using the firm's service e.g. clients with distant address who could find the same services nearer their home base; clients whose requirements are not in the normal pattern of the firm's business which could be more easily serviced elsewhere.

(iv) Any transaction in which the counterparty to the transaction is unknown.

### (b) Intermediaries

There are many clearly legitimate reasons for a client's use of an intermediary. However, the use of intermediaries does introduce further parties into the transaction thus increasing opacity and, depending on the designation of the account, preserving anonymity. Likewise there are a number of legitimate reasons for dealing via intermediaries on a "numbered account" basis; however, this is also a useful tactic which may be used by the money launderer to delay, obscure and avoid detection.

Any apparently unnecessary use of an intermediary in the transaction should give rise to further enquiry.

(c) **Dealing patterns & abnormal transactions**

The aim of the money launderer is to introduce as many layers as possible. This means that the money will pass through a number of sources and through a number of different persons or entities. Long-standing and apparently legitimate customer accounts may be used to launder money innocently, as a favour, or due to the exercise of undue pressure.

Examples of unusual dealing patterns and abnormal transactions may be as follows:

(1) **Dealing patterns**

(i) A large number of security transactions across a number of jurisdictions.

(ii) Transactions not in keeping with the investor's normal activity, the financial markets in which the investor is active and the business which the investor operates.

(iii) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual, e.g. churning at the client's request.

(iv) Low grade securities purchased in an overseas jurisdiction, sold locally and high grade securities purchased with the proceeds.

(v) Bearer securities held outside a recognized custodial system.

(2) **Abnormal transactions**

(i) **A** number of transactions by the same counter-party in small amounts of the same security, each purchased for cash and then sold in one transaction, the proceeds being credited to an account different from the original account.

(ii) Any transaction in which the nature, size or frequency appears unusual, e.g. early termination of packaged products at a loss due to front end loading; early cancellation, especially where cash had been tendered and/or the refund cheque is to a third party.

(iii) Transfer of investments to apparently unrelated parties.

(iv) Transactions not in keeping with normal practice in the market to which they relate, e.g. with reference to market size and frequency, or at off-market prices.

(v) Other transactions linked to the transaction in question which could be designated to disguise money and divert it into other forms or other destinations or beneficiaries.

## 8. SETTLEMENTS

(a) **Payment**

Money Launderers will often have substantial amounts of cash to dispose of and will use a variety of sources. Cash settlement through an independent financial adviser or broker may not in itself be suspicious; however large or unusual settlements of securities deals in cash and settlements in cash to a large securities house will usually provide cause for further enquiry.

Examples of unusual payment settlement may be as follows:

(i) A number of transactions by the same counter-party in small amounts of the same security, each purchased for cash and then sold in one transaction.

(ii) Large transaction settlement by cash.

(iii) Payment by way of cheque or money transfer where there is a variation between the account holder/signatory and the customer.

(b) **Registration and delivery**

Settlement by registration of securities in the name of an unverified third party should always prompt further enquiry.

Bearer securities, held outside a recognized custodial system, are extremely portable and anonymous instruments, which may serve the purpose of the money launderer well. Their presentation in settlement or as collateral should therefore always prompt further enquiry as should the following:

(i) Settlement to be made by way of bearer securities from outside recognized clearing systems.

(ii) Allotment letters for new issues in the name of the persons other than the client.

(c) **Disposition**

As previously stated, the aim of money launderers is to take "dirty" cash and turn it into "clean" spendable money or to pay for further shipments of drugs etc. Many of those at the root of the underlying crime will be seeking to remove the money from jurisdiction in which the cash has been received, with a view to its being received by those criminal elements for whom it is ultimately destined in a manner which cannot easily be traced. The following situations should therefore give rise to further enquiries;

(i) Payment to a third party without any apparent connection with the investor.

(ii) Settlement either by registration or delivery of securities to be made to an unverified third party.

(iii) Abnormal settlement instructions including payment to apparently unconnected parties.

## 9. COMPANY FORMATIONMANAGEMENT

(a) **Suspicious circumstances relating to the customer's behaviour:**

*(i)* The purchase of companies which have no obvious commercial purpose.

*(ii)* Sales invoice totals exceeding known value of goods.

*(iii)* Customers who appear uninterested in legitimate tax avoidance schemes.

*(iv)* The customer pays over the odds or sells at an undervaluation.

*(v)* The customer makes unusually large cash payments in relation to business activities which would normally be paid by cheques, banker's drafts etc.

*(vi)* Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

*(vii)* Customers who have numerous bank accounts and pay amounts of cash into all those accounts which, if taken in total, amount to a large overall sum.

*(viii)* Paying into bank accounts large third party cheques endorsed in favour of the customers.

(b) **Potentially suspicious secrecy might involve:**

*(i)* Excessive or unnecessary use of nominees.

*(ii)* Unnecessary granting of power of attorney.

*(iii)* Performing "execution only" transactions.

*(iv)* Using a client account rather than paying for things directly.

*(v)* Use of mailing address.

*(vi)* Unwilling to disclose the source of funds.

*(vii)* Unwillingness to disclose identity of ultimate beneficial owners.

(c) **Suspicious circumstances in groups of companies:**

*(i)* Subsidiaries which have no apparent purpose.

*(ii)* Companies which continuously make substantial losses.

*(iii)* Complex group structures without cause.

*(iv)* Uneconomic group structures for tax purposes.

*(v)* Frequent changes in shareholders and directors.

*(vi)* Unexplained transfers of significant sums through several bank accounts.

*(vii)* Use of bank accounts in several currencies without reason.

10. **OTHER:**

(i) application for business from a potential client in a distant place where comparable service could be provided "closer to home";

(ii) application for business outside the insurer's normal pattern of business;

(iii) trafficking or terrorist activity is prevalent;

(v) any want of information or delay in the provision of information to enable verification to be completed;

(vi) any transaction involving an undisclosed party;

(vii) a transfer of the benefit of a product to an apparently unrelated third party;

(viii) use of bearer securities outside a recognized clearing system in settlement of an account or otherwise.

11. **NOTES:**

(i) None of the above factors on their own necessarily mean that a customer or other person is involved in money laundering. However. it may be that a combination of some of these factors could arouse suspicions.

(ii) What does or does not give rise to a suspicion will depend on the particular circumstances.

## APPENDIX B

## LOCAL RELIABLE INTRODUCTION

Name and address of introducer: ……..……..

Name of applicant for business: ……..……
Address of applicant for business:……..
……
……
Telephone Number of applicant for business: ……
Fax Number of applicant for business: ……...

---

1. We are an institution regulated by **[name of regulatory body]** in **[country].**
2. We are providing this information in accordance with paragraph 113 of the Guidelines.

***(Please tick 3A or 3B, and 3C or 3D. Alternatively, tick 3E).***

**3A** The applicant for business was an existing customer of ours as at **[date]**

***O r***

**3B** We have completed verification of the applicant for business and his/her/ its name and address as set out at the head of this introduction corresponds with our records.

***And:***

**3C** The applicant for business is applying on his own behalf and not as nominee, trustee or in a fiduciary capacity for any other person;

***Or***

**3D** The applicant for business is acting as nominee, trustee or in a fiduciary capacity for other persons whose identity has been established by us and appropriate documentary evidence to support the identification is held by us and can be produced on demand.

*Alternatively:*

**3E** We have not completed verification of the applicant for business the following reason:

The above information is given in strict confidence for your own use only and without any guarantee, responsibility or liability on the part of this institution or its officials.

Signed: ……
Full name: ……...
Official position: …….

**NOTES ON COMPLETION OF THE LOCAL RELIABLE INTRODUCTION**

1. The full name and address of the person the introducer is introducing should be given. Separate introduction should be provided for joint accounts, trustees, etc. The identity of each person who has power to operate the account or to benefit from it should be given.

2. It is not necessary to verify the identity of clients of the introducer who were clients before the introduction of these Guidelines but the introducer should ensure that the name and address of the client is accurate and complete and in accordance with its records.

3. 3B should be ticked if the introducer has satisfactorily verified the identity and address of the client and has adequate records to demonstrate that fact under any money laundering guidance applicable to it. The receiving institution is not obliged to undertake any future verification of identity.

4. If 3E is ticked, the introducer should give an explanation in deciding whether or how to undertake verification of identity.

5. The introduction should be signed by a director of the introducer or by someone with capacity to bind the firm.

## APPENDIX C

## AUTHORITY TO DEAL BEFORE CONCLUSION OF VERIFICATION

Name of institution: .....

Name of introducer: .....

Address of introducer: .....

Introducer's regulator: .....

Introducer's registration/licence number: .....

Name of applicant for business: .....

Address of application for business (if known): .....
……
……

Telephone number of applicant for business: ……

Fax number of applicant for business: .....

***By reason of the exceptional circumstances set out below and notwithstanding that verification of the identity of the applicant for business or of a verification subject relating to the application has not been concluded by us in accordance with the Guidelines issued by the Financial Intelligence Authority, I hereby authorize:***

The opening of an account with ourselves in the name of the applicant for business

The carrying out by ourselves of a significant one-off transaction for the applicant for business (delete as applicable)

The exceptional circumstances are as follows:

I confirm that a copy of this authority has been delivered to the Compliance Officer of this institution

Signed: .....

Full Name: .....

Official Position: .....

Date: .....

Notes: This authority should be signed by a senior manager or other equivalent member of key staff in person. It is not delegable.

## APPENDIX D

## REQUEST FOR VERIFICATION OF CUSTOMER IDENTITY

| To: | [Address of financial Institution to which Request is sent] | From: | [Stamp of institution sending the letter] |
|---|---|---|---|

Dear Sirs

**REQUEST FOR VERIFICATION**

In accordance with the Anti Money Laundering Guidelines issued by Saint Lucia's Financial Intelligence Authority, we write to request your verification of the identity of our prospective customer detailed below.

Full name of customer: .....

Title (Mr/Mrs/Miss/Ms) ***specify:*** .....

Address including postcode .....

(as given by customer): .....

Date of birth: .....Account No. (if known): .....

Example of customer's signature: .....

***Please respond positively and promptly by returning the tear-off portion below***

---

To: The Manager (originating branch) From: (Receiving Institution)

Request for verification of the identity of [title and full name of customer]

With reference to your enquiry dated ..... we:

1. Confirm that the above customer is/is not known to us.
2. Confirm/cannot confirm the address shown in your enquiry.
3. Confirm/cannot confirm that the signature reproduced in your enquiry appears to be that of the above customer.

The above information is given in strict confidence, for your private use only, and without any guarantee or responsibility on the part of this institution or its officials.

Signed: .....

Full name: ..... Position: .....

## APPENDIX E

**INTERNAL REPORT FORM**

| | |
|---|---|
| NAME OF CUSTOMER/PROSPECTIVE CUSTOMER: | |
| FULL ACCOUNT NAME(S): | |
| ACCOUNT NO .(S) | |
| DATE(S) OF OPENING | DATE OF CUSTOMER'S BIRTH:<br>DD_____/MM_____/YY_____ |
| PASSPORT NUMBER: | |
| IDENTIFICATION AND REFERENCES: | |
| CUSTOMER'S ADDRESS: | |
| DETAILS OF TRANSACTIONS AROUSING SUSPICION: | |
| As relevant:<br>Amount (Currency) _____ Date:_____ | |
| Sources of Funds: | |
| Other Relevant Information:<br>Name and Position of Employee making Report:<br>Signature _____ Date:_____ | |
| Compliance Officer: (The Compliance Officer should briefly set out the reason for regarding the transactions to be reported as suspicious or, if he decides against reporting, his reasons for that decision.)<br>Signature of Compliance Officer: _____ Date: _____ | |
| Senior Management Approval:<br>Name of Senior Manager | |
| Approved/Rejected (delete as appropriate) Date:_____ | |
| REASONS: | |
| DATE REPORT MADE TO AUTHORITY (if appropriate): | |

## APPENDIX F

## DISCLOSURE TO THE FINANCIAL INTELLIGENCE AUTHORITY

1) It would be of great assistance to the FIA if disclosures were made in the standard form at the end of this Appendix.

2) Disclosures may be delivered in sealed and confidential envelopes by hand, by post, or, in urgent cases, by fax.

3) The quantity and quality of data delivered to the FIA should be such as -

- To indicate the grounds for suspicion;
- To indicate any suspected offence; and
- To enable the Investigating Officer to apply for a court order, as necessary.

4) The receipt of disclosure will be acknowledged by the FIA.

5) Such disclosure will usually be delivered and access to it available only to an appropriate investigating or other law enforcement agency. In the event of prosecution the source of data will be protected as far as the law allows.

6) Neither the FIA nor an investigating officer will approach the customer in connection with the investigation unless criminal conduct is identified.

7) The FIA and an investigating officer may seek additional data from the reporting institution and other sources with or without a court order. Enquiries may be made discreetly to confirm the basis of a suspicion.

8) The FIA will, so far as possible and on request, promptly supply information to the reporting institution to enable it to be kept informed as to the current status of a particular investigation resulting from its disclosure.

9) It is an important part of the reporting institution's vigilance systems that all contacts between its departments and branches and the FIA be copied to the Reporting Officer/Compliance Officer so that he can maintain an informed overview.

**SUSPICIOUS ACTIVITY REPORT**

**Form S/A 1- Page 1**

*CONFIDENTIAL*

**In accordance with the Money Laundering** (Prevention) Act.

| |
|---|
| **S/A Ref:** |
| **Reporting Entity 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

**REPORTING ENTITY INFORMATION (REGULATED INSTITUTED OR OTHER)**

| | |
|---|---|
| 2. Name (of Regulated Institution of Other) | |
| 3. Address (of Regulated Institution or Other) | |
| 4. Telephone number | 5. Fax Number |
| **PARTICULARS OF SUSPECT** | |
| 7. Name (full name of person, business or company) | |
| 8. Address | |
| 9. Date of Birth (DD/MM/YY) | |
| 10. Occupation | |
| 11. Employer | |
| 12. Telephone number - business | 13. Telephone number - residence |
| 14. Form(s) of identification produced by suspect | |
| 15. Suspect's relationship with Reporting Entity | |
| 16. Is suspect employed by Reporting Entity? (YES/NO (If "Yes" give details) | |
| 17. Other relevant information (please include details of identification and/or references taken, associated parties, addresses, telephone numbers etc.)<br>18. 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 ACTIVITY REPORT**

| **19. Reasons for Suspicio** |
|---|
| |

| **20. Signed by (name of person** compiling report) | 21. Contact Name (Reporting Officer/Compliance Officer where applicable) |
|---|---|
| 22. Telephone Number | 23. Fax Number |
| 24. Telephone number | 25. Fax number |

Financial Intelligence Authority
P.O. Box GM 959
Gablewoods 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.**

## APPENDIX G

## SPECIMEN RESPONSE OF THE FINANCIAL INTELLIGENCE AUTHORITY

It is essential that this letter remains confidential. It should be retained within files kept by the Reporting Officer

Dear Sir/Madam

**Acknowledgement of Suspicious Activity Report**

I acknowledge receipt of the information supplied by you to the Financial Intelligence Authority under the provision of the Money Laundering Prevention Act concerning *[name of individual(s) and/or entity (ies)]*

As this matter proceeds contact will be maintained on the progress of our entities.

Yours faithfully
FINANCIAL INTELLIGENCE AUTHORITY

**Administrative Secretary**

Dear Sir/Madam

**Financial Intelligence Authority Feedback Report**

I enclose for your information a summary of the present position of the case concerning *[name of individual]* as reported to the Financial Intelligence Authority.

*[place summary here]*

The current status shown, whilst accurate at the time of making this report, should not be treated as a basis for any subsequent decision without reviewing the up-to-date position.

Please do not hesitate to contact the Financial Intelligence Authority if you require any further assistance.

Yours faithfully

**Financial Intelligence Authority**

## APPENDIX H

## GLOSSARY

*Applicant for business:* the party to a Saint Lucia institution that they enter into a business relationship or one-off transaction. The party may be an individual or an institution. In the former case, therefore, the applicant for business (if the case is not exempt from the need for verification) will be synonymous with the verification subject; if the applicant for business is an institution however, it is likely to comprise a number of verification subjects.

*Business relationship:* (As opposed to a one-off transaction) A continuing arrangement between two or more parties one of whom is acting in the course of business (typically the institution and the customer/client) to facilitate the carrying out of transactions:

(1) on a frequent, habitual or regular basis, and

(2) where the monetary value of dealings in the course of the arrangement is not known or capable of being known at entry.

*Entry:* The beginning of either a one-off transaction or a business relationship. I triggers the requirement of verification of the verification subject (except in exempt cases). Typically, this will be:

(1) the opening of an account, and/or

(2) the signing of a terms of business agreement.

*Key staff* Any employees of an institution who deal with customers/clients and/or their transaction.

*One-off transaction:* Any transaction carried out other than in the course of an established business relationship. It falls into one of two types:

(1) the significant suspicious one-off transaction

(2) the small one-off transaction

A business relationship is an established business relationship where an institution has obtained, under procedures maintained in accordance with these Guidelines, satisfactory evidence of identity of the person who, in relation to the formation of that business relationship, was the applicant for business.

*Compliance Officer:* A senior manager or director appointed by an institution to have or vigilance policy and vigilance systems, to decide whether suspicious transactions should be reported, and to report to the FIA if he/she so decides.

*Significant one-off Transaction:* A one-off transaction exceeding whether a single transaction or consisting of a series of linked one-off transactions, or, in the case of an insurance contract, consisting of a series of premiums in any one year.

Made this 22nd day of April, 2010.

NICHOLAS O. FREDERICK,
***Attorney General.***

**SAINT LUCIA**
**PRINTED BY THE NATIONAL PRINTING CORPORATION**
**CASTRIES**
**2010**