SAINT LUCIA

STATUTORY INSTRUMENT, 2012, No. 82

[10th August, 2012]

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)(Amendment) Regulations 2012.

Interpretation

2. In these Regulations "principal Regulations" means the Money Laundering (Prevention)(Guidance Notes) Regulations No. 55 of 2010.

Amendment of Schedule

3. The Schedule to the principal Regulations is amended —

(a) by inserting after paragraph 31, the following:

"31A. Where a transaction is inconsistent in amount, origin, destination or type with a client's known, legitimate business or personal activities or has no apparent economic or visible lawful purpose, the transaction must be considered unusual and the institution is to be put on enquiry as to whether the business relationship is being used for money laundering.

31B. Where a financial institution observes unusual or complex activity in relation to a client's account, the financial institution is to make inquiries as to the nature of the activity or transaction and make a written record of its analysis or findings in relation to the unusual or complex activities and the written record is to be made available to the FIA on request.";

(b) by deleting paragraph 88 and substituting the following:

"88. (a) In addition to performing normal due diligence, financial institutions should be utilizing a risk analysis approach which includes-

(i) having appropriate risk management systems to determine whether the customer or potential customer is a PEP or whether he or she is acting on behalf of another person who is a PEP;

(ii) developing a clear policy and internal guidelines, procedures and controls regarding such business relationships;

(iii) obtaining senior management approval for the commencement of business relationships with such customers or to continue business relationships with those who are found to be or subsequently become PEPs.

(iv) taking reasonable measures to establish source of wealth and source of funds; and

(v) ensuring the proactive monitoring of activity on such accounts, so that changes can be detected and consideration as to whether the changes suggest corruption or the misuse of public assets.

(b) In the context of this risk analysis, financial institutions should focus resources on products and transactions that are characterized by a high risk of money laundering.

(c) Financial institutions should ensure that timely reports are made to the FIA where proposed or existing business relationships with PEPs provide grounds for suspicion.

(d) To address PEP risk, financial institutions should develop and maintain enhanced security practices which may include the following:

(i) assessing risks in countries where the financial institutions have financial relationships by evaluating amongst other things, the potential risk for corruption in political and governmental organizations. Financial institutions which are part of an international group may also use the group network as another source of information;

(ii) if financial institutions maintain business relations with nationals and entities of countries that are vulnerable to corruption, establishing who the senior political figures in countries which are vulnerable to corruption are and determining whether their

customer has close links with such individuals (e.g. immediate family or close associates). Financial institutions should consider the risk that a customer may be susceptible to acquiring connections with such political figures after the business relationship has been established;

(iii) exercising vigilance where their customers are involved in the type of business which appears to be most vulnerable to corruption, including trading or dealing in precious stones or precious metals.

(e) Financial institutions should adopt detailed due diligence methods which should include-

(i) scrutinizing complex structures (those utilizing legal structures such as multiple corporate entities, trusts, foundations and multiple jurisdictions);

(ii) establishing the source of wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship, both at the onset of the relationship and on an ongoing basis;

(iii) developing a profile of usual and expected activity of the business in order to provide a basis for regular monitoring. The profile should be regularly reviewed and updated;

(iv) reviewing the decision to commence the business relationship at a senior management or at a Board level and reviewing the development of the relationship annually;

(v) scrutinizing unusual features including very large transactions, the use of government or central bank accounts, expressed demands for secrecy, the use of cash, bearer bonds or other instruments which severs an audit an audit trail, the use of unknown financial institutions and repeated transactions involving sums just below a typical reporting level.

(f) The information collected in accordance with the policies to be adopted by a financial institution should be fully documented

and may constitute the basis upon which the financial institution avoids or terminates a business relationship with PEPs.";

(c) by inserting after paragraph 101, the following:

"Emerging Technologies

101.A (a) In addition to the measures identified in paragraph 96, financial institutions should apply enhanced due diligence when dealing with the use of emerging technologies to access its products and services.

(b) Financial institutions should have policies in place and take measures to prevent the misuse of technology for money laundering. The level of verification used should be appropriate to the risk associated with the particular product or service.

(c) Financial institutions should undertake a risk assessment to identify the type of risk and the levels of risk associated with their product applications and wherever appropriate, implement multi-factor verification measures. Layered scrutiny or other controls reasonably calculated to mitigate those risks.

(d) Financial institutions are to carry out ongoing monitoring of the use of emerging technologies in business relationships that they are engaged in.";

(d) by deleting paragraph 135 (h) and substituting the following:

"(h) Copies of identification documents and authorized signatures should be obtained from all directors in accordance with the general procedure for the verification of the identity of individuals;";

(e) in paragraph 141, by inserting "or domestic" after foreign wherever it appears;

(f) by deleting paragraph 147(e) and substituting the following:

"(e) Transactions from countries or jurisdictions which have inadequate AML systems. The following websites contain sources of relevant information for financial institutions:

(i) Office of Foreign Assets Control (OFAC) for information pertaining to USA foreign policy and national security: www.treas.gov.ofac;

(ii) Transparency International for information on countries vulnerable to corruption: www.transparency.org;

(iii) The Financial Crimes Enforcement Network (FINCEN) for country advisories: www.fincen.gov"; and

(g) by deleting paragraph 179 and substituting the following:

"179. In the case of electronic transfer, where such transfers do not give complete originator information, institutions are required to apply enhanced scrutiny to these. In addition and without obviating the obligation to report suspicious transactions in accordance with normal procedures –

(a) the financial institution of the ultimate recipient should have effective risk based procedures in place to detect missing or incomplete information from messaging or payment and settlement systems used to effect the transfer of funds;

(b) the financial institution of the ultimate recipient should consider missing or incomplete information on the originator as a risk factor in assessing whether the transfer of funds or any related transaction is suspicious and whether it should be reported to the FIA;

(c) where the financial institution of the ultimate recipient detects upon a transfer of funds, that the required originator information is either incomplete or missing, the financial institution should either reject the transfer or seek complete information on the originator. The financial institution may acquire the information from a source other than the institution of the originator;

(d) a financial institution should subject incoming electronic transfers to an appropriate level of post-event random sampling that is risk based. The sampling may be weighed towards transfer from –

(i) countries deemed to be high-risk for money laundering, terrorist financing or both;

(ii) financial institutions of originators who are identified from such sampling as having previously failed to comply with the relevant information requirements;

(e) where a financial institution regularly fails to supply the required originator information and the financial institution of the ultimate recipient has taken reasonable measures to have the institution of the originator correct the failures, the financial institution of the ultimate recipient should –

(i) reject any future transfer of funds from that institution;

(ii) restrict its business relationship with that financial institution;

(iii) terminate its business relationship with that financial institution,

and report a decision to restrict or terminate a relationship to the FIA.".

Made this 8th day of August, 2012.

KIM CAMILLE ST.ROSE,
Attorney General.

SAINT LUCIA
PRINTED BY THE NATIONAL PRINTING CORPORATION
CASTRIES
2012 **[Price: $3.00]**