



***DESIGNATED NON-FINANCIAL BUSINESSES
AND PROFESSIONS (DNFBPs)***

Issue No. 21

July 2014

- * *Who are DNFBPs?*
- * *Compliance Requirements*
- * *Customer Due Diligence*
- * *Breaches for Non-Compliance*

In view of increased legislative requirements for financial institutions to develop and implement measures to combat money laundering and terrorist financing, money launderers may look at DNFBPs to try and conceal laundered proceeds and revenues of crimes. Thus, there is potentially, significant risks in the services offered by this sector being misused for money laundering and the financing of terrorism.

Who are DNFBPs?

Designated non-financial businesses and professions (DNFBPs) include but is not limited to the following:

- 1) Casinos where roulette or card games are carried on in the establishment or where there is a slot machine — not including video lottery terminals — on the premises.
- 2) Real Estate agents involved in transactions for or on behalf of a client concerning the buying, leasing or selling of real estate in relation to both the purchasers and vendors of property.
- 3) Wholesale dealers or manufacturers in precious metals and precious stones.
- 4) Lawyers, notaries, other independent legal professionals and accountants, including auditing service providers who prepare or carry out transactions for their clients, including but not limited to:
 - a) Buying, leasing or selling of real estate;
 - b) Managing of client money, securities or other assets;
 - c) Management of bank, savings or securities accounts other than as a business that meets the definition of financial institution;
 - d) Organization of contributions for the creation, operation or management of companies;
 - e) Creation, operation or management of legal persons or arrangements, and buying and selling of business entities.
- 5) Trust and Company Service Providers, when they prepare for or carry out transactions for a client including but not limited to:
 - a) Acting as a formation agent of legal persons;
 - b) Acting as (or arranging for another person to act as) director or secretary of a company, a partner of a partnership, or a similar position to other legal persons;
 - c) Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any legal person or arrangement;

- d) Acting (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
 - e) Acting as (or arranging for another person to act as) a nominee shareholder for another person.
- 6) Other DNFBPs, including dealers in vehicles, travel agencies and investment and commodity advisers.

Compliance Requirements

A DNFBP should be aware of its compliance obligations which are contained in Anti-Money Laundering Regulations, 2011 (“**AMLR**”) and the Financial Services (Implementation of Industry Standards) Regulations, 2011 (“**FSISR**”). It is important for a DNFBP to be familiar with relevant legislation.

A DNFBP should:

- 1) Establish, implement, monitor and maintain an effective Compliance Program.
- 2) Devise and implement relevant policies, procedures, processes and controls designed to prevent and detect potential Money Laundering and Terrorist Financing Activities. Such measures should consider the following:

I. Anti-Money Laundering Policies and Procedures: DNFBPs must establish and maintain effective anti-money laundering policies and procedures, systems and controls designed to prevent opportunities for money-laundering in relation to the applicant and its activities.

II. Customer Due Diligence and Enhanced Due Diligence: DNFBPs should properly identify all customers and maintain client identification records. Enhanced due diligence measures should be applied when there is a suspicion or a high risk circumstance is identified.

III. Risk Assessment: DNFBPs should adequately assess its AML/CFT risk in relation to its customers, its business, products, services, geographical exposures and appropriately define and document its risk based approach.

IV. Anti-Money Laundering Training and Awareness: DNFBPs must provide training to all relevant employees at appropriate and regular intervals. This training should be tailored to the level of exposure and AML/CFT risks faced by the DNFBPs.

V. Reporting to the FSRC: A DNFBP is required to submit its audited financial statements to the FSRC, within three (3) months of the end of its financial year.

VI. Record Keeping Procedures: DNFBPs are required to keep

records for a period of at least five (5) years commencing with the date on which the business relationship ends.

VII. Detection and Reporting of Unusual and/or Suspicious Transactions/Customers: The Compliance Officer should be well versed in the different types of transactions which the DNFBP handles and which may give rise to opportunities for money laundering and terrorist financing. If the Compliance Officer decides that a disclosure should be made, a report, preferably in standard form should be sent to the Financial Intelligence Unit (FIU).

VIII. Appoint a Compliance Officer: A DNFBP should appoint a Compliance Officer who will be responsible for the day-to-day oversight of relevant policies, procedures and controls to detect and prevent money laundering and terrorist financing.

IX. Independent Audit: DNFBPs should ensure that an independent review system that will test and assess the effectiveness of their AML/CFT Compliance Program on a risk-sensitive basis is completed, this review should have a defined minimum frequency (at least once per year).

Customer Due Diligence (CDD)

A DNFBP should:

- a) Properly identify its customers and maintain client identification records including reliable documentation. Such customer identification records should be made available to the FSRC or to any Competent Authority promptly upon request.
- b) Adopt a risk based approach to determine the extent of additional CDD measures commensurate with the level of risk posed by the customer type, business relationship, transaction, product/service or geographical location.
- c) Conduct Enhanced Due Diligence (EDD) measure when there is a suspicion of Money Laundering or Terrorist Financing or where high risk circumstances are identified.

A DNFBP shall implement the following standards of CDD measures:

- 1) Identify and verify the identity of a customer that is natural person, using relevant and reliable independent source documents, data or information;
 - a) The relevance and usefulness in this context of the following personal information shall be considered:
 - ◆ Full name(s) used
 - ◆ Date and place of birth
 - ◆ Nationality
 - ◆ Current permanent address, including post code
 - ◆ Telephone and fax number
 - ◆ Occupation and name of employer
 - ◆ Specimen signature of the customer
 - b) To establish identity, the following documents shall be used in descending order of acceptability:
 - ◆ Current valid passport
 - ◆ National identity card

- ◆ Armed forces identity card; and
- ◆ Driver's licence which bears a photograph

- 2) If a customer is not a natural person, the DNFBP shall:
 - a) Identify and verify the name, address and legal status of the customer by obtaining proof of incorporation issued by the relevant authority or similar formal evidence of establishment and existence;
 - b) Verify that any person purporting to act on behalf of the customer is authorized to do so and that such person's identity is properly verified;
 - c) Identify the beneficial owner, taking reasonable measures to verify the identity of the beneficial owner using identification data obtained such that the DNFBP is satisfied that it recognizes who the beneficial owner(s) are;
 - d) Understand the ownership and control structure of the customer; and
 - e) Identify the natural persons that may ultimately own and control the customer.
- 3) Establish and record the purpose and intended nature of the business relationship;
- 4) Conduct ongoing due diligence on the business relationship and apply scrutiny to transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the DNFBP's knowledge of the particular clients, their business and risk profile; including, where necessary the source of funds;
- 5) Establish measures for customers who conduct large cash transactions;
- 6) In addition to as stated above, in the case of casinos, specific measures to identify a customer whom the casino pays a casino disbursement.

Breaches for Non-Compliance

The statement of standard expected of DNFBPs in the Federation is contained in the Proceeds of Crime Act CAP 4.28; the Anti-Terrorism Act CAP 4.02 and the Financial Services Regulatory Commission Act, 2009.

DNFBPs are strongly encouraged to develop and maintain effective and up to date policies, systems of procedures and controls to guard against money laundering and terrorist financing. Failure to act in a manner which is consistent with statutory requirements constitute an offence and the DNFBP shall be liable on conviction to fines as imposed by Regulations 3(7); 5(6); 8(10); 11(4) and 14 of the AMLR and the Anti-Terrorism (Prevention of Terrorist Financing) Regulations, 2011.

Source

<http://www.nevisfsrc.com/regulatory-framework/supervision>

FATF Recommendations

