FINANCIAL INTELLIGENCE UNIT

GUIDELINES FOR NON-REGULATED SERVICE PROVIDERS (NRSPs)

Table of Contents

CHAPTER 1- INTRODUCTION

1.1 PURPOSE

This Guidance was compiled by the St. Vincent and the Grenadines Financial Intelligence Unit ("FIU") to offer guidelines to the Non-Regulated Service Providers (NRSPs) on the implementation of Anti-Money Laundering and Counter Terrorist Financing (AML/CFT) measures and on how best to comply with the AML/CFT laws and regulations of St. Vincent and the Grenadines.

The AML/CFT policy adopted by each NRSP should be a reflection of its money laundering and terrorist financing risk. Thus, the responsibility rests with each entity to develop and implement its own polices and AML/CFT measures.

1.2 GENERAL APPLICATION

These Guidelines are intended to offer guidance to all NRSPs, which include:

1. Real estate agents
2. Casinos
3. Car dealers
4. Jewelers
5. Lawyers, notaries, other independent legal professionals, accountants and auditors (including sole practitioners, partners or employed professionals within professional firms), when they prepare for, or carry out, transactions for their client concerning the following activities:
   (i) buying and selling of real estate;
   (ii) managing of client money, securities or other assets;
   (iii) management of bank, savings or securities accounts;
   (iv) organisation of contributions for the creation, operation or management of companies;
   (v) creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

1.3 THE FINANCIAL INTELLIGENCE UNIT

The Saint Vincent and the Grenadines Financial Intelligence Unit (FIU) is designated as the supervisory authority of Non-Regulated Service Providers (NRSPs). The objectives of the supervisory authority include:

1. Determining applications for registration and to take appropriate action against NRSPs which carry out relevant business without being registered.
2. Monitoring the compliance of the NRSPs with their AML/CFT obligations under the relevant Laws, Regulations and Code.

3. Taking appropriate enforcement action against the NRSPs for breaches of, or non-compliance with, their AML/CFT obligations.

It is the responsibility of the FIU to supervise the relevant service providers in relation to their AML/CFT obligations, which include:

a. The implementation of a Compliance Programme
b. Appointment of a Compliance/Reporting Officer
c. Effective Reporting and Suspicious Transaction Detection
d. Effective Record Keeping Systems
e. Establishment of Adequate Internal Controls
f. Effective Staffing, Training and Education
g. Establishing Customer Due Diligence Protocols

The supervisory authority, where reasonably required for the discharge of its functions, may by written notice require a NRSP to provide specific information and documents. A search warrant may be issued by the Magistrate's Court if the NRSP fails to comply with the notice.

In addition, the Director of the FIU, where there are reasonable grounds to suspect that a relevant offence has been committed, may require the NRSP to produce such information he/she considers necessary for the purpose of investigating that offence.

1.4 RELEVANT LAWS

a. The Financial Intelligence Unit 2002 Act, as amended by Act No.7 of 2013
b. The Proceeds of Crime Act 2013, as amended by the Proceeds of Crime Amendment Act, No. 18 of 2017 (POCA)
c. The Anti-Money Laundering and Terrorist Financing Regulations 2014, as amended by Act No.25 of 2017 (AMLTFR)
d. The Anti-Terrorist Financing and Proliferation Act 2015, as amended by No.17 of 2017 (ATFPA)
e. Anti-Money Laundering and Terrorist Financing Code 2017
f. Non-Regulated Service Providers Regulations 2019

CHAPTER 2- MONEY LAUNDERING AND TERRORIST FINANCING

2.1 WHAT IS MONEY LAUNDERING

The expression "money laundering" covers all procedures to conceal the origins of criminal proceeds so that they appear to have originated from a legitimate source. This gives rise to three features common to persons engaged in criminal conduct, namely they seek:

- To conceal the true ownership and origin of criminal proceeds;
- To maintain control over them; and
- To change their form.

There are three stages of laundering, which broadly speaking occur in sequence but often overlap. It should be noted however, that all stages may not be present in every situation:

2.1.1 Placement

This is the physical disposal of criminal proceeds. In the case of many serious crimes (such as drug trafficking and robbery) the proceeds take the form of cash, which needs to be placed in the financial system. Techniques such as "structuring" or "smurfing" are used in which, instead of making a large deposit transaction to cause suspicion, illegal receipts are broken up into smaller sums and deposited into single or multiple accounts and using other individuals to make the deposits. Placement 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;

e) purchasing the services of high-value individuals;

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

g) placing cash in the client account of a professional intermediary such as attorneys.

2.1.2 Layering

This occurs after the funds have entered the financial system and involves the separation of criminal proceeds from their source by the creation of layers of transactions designed to disguise the paper trail and provide the appearance of legitimacy. Layering may include:

a) rapid switches of funds between banks and/or jurisdictions;

b) use of cash deposits as collateral security in support of legitimate transactions;

c) switching cash through a network of legitimate businesses and "shell" companies across several jurisdictions; or

d) resale of goods/assets.

2.1.3 Integration

This is the stage in which criminal proceeds are treated as legitimate. After the layering stage, integration places the criminal proceeds back into the economy in such a way that they appear to be legitimate funds or assets. These laundered funds are then used to further criminal activity or to enhance the criminal lifestyle such as real estate investments or the purchasing of luxury assets.

2.2 WHAT IS TERRORIST FINANCING

Terrorist Financing is the process by which funds are provide to an individual or group to fund terrorist activities. Unlike money laundering, funds to finance terrorism can derive from legitimate sources such as personal donations, non-profit organisations, state sponsorship, profits from legitimate commercial businesses or from criminal activity such as drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion. Similar to money laundering, terrorist financiers also move funds to disguise their source, destination and purpose for which the funds are to be used.

2.2.1 Use of Funds

a. To carry out specific terrorist attacks and undertake pre-operational surveillance. This includes travel to and from the target location, the use of vehicles and other machinery and purchase of a range of arms from light assault weapons to improvised explosive devices (IEDs).

b. To recruit new members

c. To spread propaganda through the publishing magazines and newspapers as well as purchasing internet domain names and administer websites. Some terrorist groups have even acquired television and radio outlets to promote their messages and worldview.

d. To enable training of operatives and sympathisers in a number of areas including, weapons training, bomb-making, clandestine communication and ideology.

e. To pay the salaries of their leadership and members, as well as for the families of jailed or deceased members. Providing financial security and incentives to group members can

cement commitment to the organisation's goals and ideology. Terrorist groups may also provide long- term financial support to the families of deceased operatives.

f. To establish or subsidies social institutions that provide health, social, and educational services. This is done to undermine the credibility of the legitimate government by providing services that they say the state is neglecting and to build support within local populations and aid recruitment efforts.

2.2.2 Movement of Funds

a. Hawala System

This informal value system involving the international transfer of value outside the legitimate banking system and based on a trusted network of individuals, has also played a role in moving terrorist-related funds. Individuals from various parts of the world use their accounts to move money internationally for third parties. In this way, deposits and withdrawals are made through hawala bankers rather than traditional financial institutions. The third parties are normally immigrants or visiting workers who send small sums to their homelands to avoid bank fees for wire transfers. There is usually no physical movement of currency and a lack of formality with regard to verification and record-keeping. The transfer takes place by coded information that is passed through chits, couriers, letters, faxes, emails, text messages, or online chat systems, followed by some form of telecommunications confirmations. Almost any document that carries an identifiable number can be used by the receiver to pick up the values in the other country.

Unlike formal institutions, hawalas are not consistently subject to formal government oversight and are not required to keep detailed records in standard form. This make it more appealing to money launders and terrorists.

b. Non-Profit Organisations

Knowingly or not, charitable organizations have served as vehicles for raising and laundering funds destined for terrorism. Charities or non-profit organizations have the following characteristics that are particularly vulnerable to misuse for terrorist financing:

i. Enjoying the public trust
ii. Having access to considerable sources of funds
iii. Being cash-intensive
iv. Frequently having global presence, often in or next to areas exposed to terrorist activity
v. Often being subject to little or no regulation and/or having few obstacles to their creation

c. Funds transferred through banks

The banking sector continues to be the most reliable and efficient way to move funds internationally, and remains vulnerable to TF. The banking sector is an attractive means

for terrorist groups seeking to move funds globally because of the speed and ease at which they can move funds within the international financial system.

d. Money Value Transfer Systems

Along with the banking sector, the remittance sector has been exploited to move illicit funds and is also vulnerable to TF. In conflict-prone countries where access to banking services is limited and terrorist groups operate, remittance providers may be the primary financial institution through which consumers can engage in cross-border funds transfer activity. Remittance providers are especially vulnerable to abuse for TF where they are unregulated, not subject to appropriate AML/CFT supervision or where they operate without a license (thus operating without any AML/CFT controls). The biggest TF threat involves agents or employees who knowingly facilitate funds transfers on behalf of terrorist groups, including the falsification of transaction reporting to obfuscate or anonymise details. Migrant communities and families rely heavily on MVTS to remit funds home; this provides a channel for commingling TF with legitimate family transfers. It also makes it difficult to detect TF from normal family and community remittances.

e. Physical transportation of cash

Cash continues to be a prevalent aspect of terrorist operations. While funds may be raised in a number of ways, often they are converted into cash to be taken to conflict zones. This is assisted by porous national borders, difficulty in detecting cash smuggling (particularly in the small amounts that are sometimes smuggled for TF purposes), and the existence of informal and unregulated economies.

2.2.3 Emerging risks for terrorist financing

a. The use of employment income, social assistance, family support and bank loans by foreign terrorist fighters (FTFs) to fund their terrorist activities. This makes detection nearly impossible without the association of other aggravating terrorist financing indicators.

b. The use of social media by terrorist organisations to communicate and raise money for their causes.

c. The use of new payment products and services such as virtual currencies, prepaid cards and PayPal to facilitate the funding of terrorist activities

d. The use of natural resources such as gas, oil, timber, diamonds, gold (and other precious metals), wildlife (e.g. ivory trading) and historical artifacts to both fund terrorist acts and support day to day activities. These resources themselves may be sold on the black market or to complicit companies where they can then be integrated into the global trade sector

2.2.4 Terrorist Financing Indicators

To avoid becoming conduits for terrorist financing, institutions must look at, among other things, the following factors:

a. Use of an account as a front for a person with suspected terrorist links.
b. Appearance of an accountholder's name on a list of suspected terrorists.
c. Frequent large cash deposits in accounts of non-profit organisations.
d. High volume of transactions in the account.
e. Lack of a clear relationship between the banking activity and the nature of the accountholder's business.
f. Dormant, low-sum accounts that suddenly receive wire transfer deposits followed by daily cash withdrawals that continue until the transferred sum is removed.
g. Lack of cooperation by client in providing required information.

CHAPTER 3- ANTI-MONEY LAUNDERING AND COUNTER TERRORIST FINANCING OBLIGATIONS

3.1 AML/CFT OBLIGATIONS

There is 9 step process recommended to ensure compliance with the anti-money laundering and counter terrorist financing obligations, they are as follows:

3.1.1 STEP 1: Registration of The NRSPs

All NRSPs **must** register with the FIU before conducting any type of relevant business.

a. Registration Process

The NRSP **must** complete and submit to the FIU:

i. Registration Form; and
ii. Compliance / Reporting Officer Fit and Proper Questionnaire Form

These forms are available for download on the FIU's website.

3.1.2 STEP 2: Appointment of A Compliance / Reporting Officer

The NRSP shall nominate an individual with sufficient seniority in the organization as Compliance /Reporting Officer. The individual **must** complete and submit the **Compliance / Reporting Officer Fit and Proper Questionnaire Form** to the FIU for approval. Upon written approval from the FIU, the appointed Compliance / Reporting Officer shall be responsible for:

i. Implementing the Compliance Programme by establishing and maintaining policies, procedures, processes and controls consistent with St. Vincent and the Grenadines' AML/CFT legislation and exercising day –to-day operational oversight of the NRSP's compliance functions
ii. Receiving and considering internal money laundering disclosures submitted by employees and whether a Suspicious Activity Report (SAR) should be made to the Financial Intelligence Unit
iii. Acting as the point of contact to the FIU and responding promptly to any request for information made by the FIU.
iv. Submitting an annual compliance report to the FIU stating the level of compliance adherence to relevant policies, procedures, processes and controls with respect to regulatory obligations.
v. Submitting quarterly reports specifying the number of Suspicious Activity Reports submitted to the FIU in the quarter.
vi. Accessing relevant information concerning the NRSP's clients, representatives of the clients, business relationships and transactions and the details of such transactions which a NRSP contemplates or actually enters into, with or for a client or third-party.

vii. Ensuring the training of directors and staff in AML/CFT

The appointed compliance / reporting officer should have the authority and the resources necessary to discharge his or her responsibilities effectively. He/she should have the requisite experience and independence to act on his/her own authority, have direct access to senior management, and have sufficient resources including appropriately trained and effective staff. For sole traders, the owner can nominate himself/herself as compliance / reporting officer or can choose to nominate another individual to help implement a compliance programme.

3.1.3 STEP 3: Conduct A Risk Based Assessment

The NRSPs **must** carry out and document a risk assessment of the money laundering and terrorist financing risk it faces and to develop strategies to mitigate them. A risk assessment is an analysis of potential threats and vulnerabilities to money laundering and terrorist financing to which the business is exposed. When conducting a risk assessment, the NRSP must take into consideration:

a. **The customer risk**
   i. Are they a trust or other legal person?
   ii. Have you identified beneficial ownership?
   iii. Are they specified in the Act / Regulations as requiring EDD?
   iv. Are they involved in occasional or one-off activities/transactions above a certain threshold?
   v. Do they use complex business structures that offer no apparent financial benefits?
   vi. Are they a politically exposed person (PEP)?
   vii. Are they a cash-intensive business?
   viii. Are they involved in businesses associated with high levels of corruption?
   ix. Do they have an unexplained or hard to verify source of wealth and/or source of funds?
   x. Do they conduct business through, or are they introduced by gatekeepers such as accountants, lawyers, or other professionals?
   xi. Are they a non-profit organisation?
   xii. Have they been identified in the National Risk Assessment (NRA), FIU guidance material as presenting a higher ML/TF risk?

b. Product risk
   i. Does the product/service allow for anonymity?
   ii. Does the product/service disguise or conceal the beneficial owner of your customer?
   iii. Does the product/service disguise or conceal the source of wealth or funds of your customer?
   iv. Does the product/service allow payments to third parties?
   v. Does the product/service commonly involve receipt or payment in cash?

vi. Has the product/service been identified in the NRA, FIU guidance material as presenting a higher ML/TF risk?
vii. Does the product/service allow for the movement of funds across borders?

c. Delivery risk

i. Does your business have non-face-to-face customers (via post, telephone, internet or via intermediaries)?
ii. Do you provide your products/services via the internet?
iii. Does your business have indirect relationships with customers (via intermediaries, pooled accounts, etc.)?
iv. Do you provide your products/services via agents or intermediaries?
v. Do you provide your products/services to overseas jurisdictions?

d. Country risk

Whether the country in which the business is conducted has:

i. Ineffective AML/CFT measures
ii. Ineffective rule of law
iii. High levels of organised crime
iv. Prevalence of bribery and corruption
v. Association with TF
vi. Conflict zones
vii. Production and/or transnational shipment of illicit drugs

The complexity of the assessment depends on the size and risk factors of the business. However, the risk assessment has to be appropriate for the specific business needs, which means that it may be more or less detailed than the elements prescribed above. An NRSP can customize the checklists or can use a different method or another tool.

Based on the risks identified and information published by the FIU, International Organizations such as the Financial Action Task Force (FATF) and the NRA findings, the NRSP must allocate a rating for each customer/ client as it relates to their money laundering and terrorist financing risk.

Example:

Very unlikely	**Possible**	**Likely**	**Very Likely**
There is very little chance of ML/TF occurring	There is a small chance of ML/TF occurring	There is a moderate chance of ML/TF	There is a high chance of ML/TF occurring

The NRSP **must:**

a. Seek to **mitigate the risk** through the implementation of controls and measures tailored to the identified risks;
b. Keep **client identification** and beneficial ownership and business relationship information up to date in accordance with the assessed level of risk;

c. Conduct **ongoing monitoring** of transactions and business relationships in accordance with the assessed level of risk.
d. **Re-evaluate** and **update** the Risk-based Assessment findings when the risk factors change.
e. **Provide** the FIU with a copy of the Risk-based Assessment findings, if required.

3.1.4 STEP 4: Development of A Compliance Programme

The NRSP **must** develop a **written** Compliance Programme, which must be submitted to the FIU for approval. The development and implementation of a Compliance Programme is a legislative requirement and a good business practice. A well-designed, applied and monitored regime will provide a solid foundation for compliance with the AML/CFT obligations. As not all individuals and entities operate under the same circumstances, a compliance programme will have to be tailored to fit the entity's individual needs. It should reflect the nature, size and complexity of its operations.

The Risk-based Assessment will inform the Compliance Programme by determining the policies, procedures, systems and controls which are required to mitigate the money laundering and terrorist financing risks identified such as the extent of the customer due diligence measures to be applied to a customer, third party or beneficial owners as well as the extent of ongoing monitoring of the business relationship to be applied.

The Compliance Programme should include these **five (5)** key elements in an effort to have an effective system of internal controls:

i. the appointment of a reporting / compliance officer;
ii. the development and application of written and updated compliance policies and procedures as it pertains to Customer Due Diligence and Enhance Due Diligence protocols, the detection and reporting of suspicious activities/ transactions, ongoing monitoring and record keeping procedures.
iii. an assessment and documentation of risks related to money laundering and terrorist financing, as well as the documentation and implementation of mitigation measures to deal with those risks;
iv. an ongoing compliance training program for employees and staff; and
v. the periodic documented reviews/audits of the effectiveness of implementation of the policies and procedures, training and risk assessment.

The NRSP **must** ensure that relevant policies, processes and controls are communicated to all relevant employees. An effective AML/CFT programme would only work if the employees who are most likely to interact with the money launderers, are aware of the policies. It is therefore required that appropriate training and development sessions in relation to anti-money laundering and counter terrorist financing be provided. Without effective communication of the obligations of the business in relation to money laundering, the NRSP will be blindsided

as it relates to the use of the business as a medium for money laundering and terrorist financing purposes.

3.1.5 STEP 5: Establishment Of Internal Controls

a. CUSTOMER DUE DILIGENCE (CDD)

Effective customer due diligence measures are an essential part of any system designed to prevent money laundering and terrorist financing and are a cornerstone of the AML/CFT Obligations. However, risks must be assessed before the appropriate level of customer due diligence can be applied. Customer due diligence measures should be conducted in the following circumstances:

- when establishing a business relationship,
- when carrying out an occasional transaction,
- where there is a suspicion of money laundering or terrorist financing; and
- where there are doubts concerning the veracity of previous identification information.

i. Individuals / Natural Persons

In respect of individuals or natural persons an NRSP **must**:

- Obtain CDD information (identification and relationship information) of every customer, third party and beneficial owner.
  - ❖ Identification information includes:
    - The full legal name of the individual
    - Gender of the individual
    - Principal residential address of the individual
    - Date of birth of the individual
  - ❖ Relationship information includes:
    - The purpose and intended nature of the business relationship
    - Type, volume and value of the expected activity
    - Source of funds (Any transaction that exceeds the value of EC$10,000 must be documented on the "Declaration of source of Wealth" Form)
- Request **two (2)** forms of identification during the CDD process, one (1) to identify and the other to verify. In high risk situations, **three (3)** forms of identification are necessary, one (1) for identification and two (2) for verification.
  - ❖ The best forms of identification and verification documents are:
    - A current passport
    - A current national government issued identification card
    - A current driver's license

- ❖ Acceptable sources for verifying residential address are:
    - An independent data source such as register of electors, telephone directory, commercially available databases maintained by credit reference agencies, business information services and commercial agencies that provide electronic identity checks.
    - A recent bank statement or utility bill
    - Correspondence from a central or local government department or agency
    - A letter of introduction confirming residential address from a regulated person or foreign regulated person.

- Verify the identity of the customer and any third party and take reasonable measures, on a risk-sensitive basis, to verify the identity of each beneficial owner. Verification of identity may in certain circumstances be conducted after the establishment of a business relationship if this is necessary not to interrupt the normal course of business and there is little risk of money laundering or terrorist financing occurring, provided the verification is completed as soon as practicable after contact is first established.

- Conduct ongoing monitoring of the business relationship. During a business relationship, the NRSP must monitor activity on an ongoing basis. This includes scrutiny of transactions, source of funds and other elements of knowledge collected in the customer due diligence process, to ensure that the new information is consistent with other knowledge of the client and keeping the documentation concerning the client and the relationship updated.

- Ensure customer due diligence procedures are applied to all clients, both new and existing.

- Ensure that the identification data is kept up-to-date and review the records of higher risk customers or business relationships as appropriate.

ii. <u>Legal Person or Entity</u>

In respect of a legal person or entity the NRSP **must**:

- Obtain the following identification information:
    - ❖ The full name of the legal person
    - ❖ The date of incorporation, registration or formation
    - ❖ Official identifying number

- ❖ The registered office or the address of the head office
- ❖ The name and address of the registered agent
- ❖ The mailing address
- ❖ The principal place of business
- ❖ The names of the directors
- ❖ Identification information of the directors
- ❖ Identification information on the individuals who are beneficial owners of 15% of the company/business

- Verify the identity of the directors/ beneficial owners of the company or business

- Conduct ongoing monitoring of the business relationship

- Ensure that the identification data is kept up-to-date and review the records of higher risk customers or business relationships as appropriate

iii. Terminations

In cases where the NRSP is unable to comply with any of the following CDD measures, namely:

- To apply CDD measures before the establishment of a business relationship or before carrying out an occasional transaction;
- To complete the verification of the identity of a customer, third party or beneficial owner after the establishment of a business relationship; or
- To undertake ongoing monitoring with respect to a business relationship

It is advised not to open an account, commence business relations, accept instructions or perform the transaction.

Where CDD obligations for existing business relationships and clients are not met, as a result of the client's refusal to comply or causing unacceptable delays, the NRSP is advised to terminate the business relationship, and consider filing a Suspicious Activity Report (SAR) with the FIU.

Customer due diligence measures are a very critical part of the anti-money laundering and counter terrorist financing requirements. They ensure that the NRSP knows who its clients are, ensure that it does not accept clients unknowingly which are outside its normal risk tolerance, or whose business it will not understand with sufficient clarity to be able to form money laundering or terrorist financing suspicions when appropriate. In cases where the NRSP does not understand a client's regular business pattern of activity it will be very difficult to identify any abnormal business patterns or activities. In addition the NRSP must be in a position to supply the client's identity to the FIU should that client become the subject of a SAR. Continued alertness for

changes in the nature or ownership of the client, its business model, or its susceptibility to money laundering or Terrorist Financing – or actual evidence of the latter - must be maintained.

b. ENHANCED DUE DILIGENCE (EDD)

A risk-based approach to customer due diligence will identify situations which by their nature can present a higher risk of money laundering or terrorist financing which means that the NRSP must obtain additional customer due diligence information about the client.

EDD must be applied:

i. if a client has not been physically present for identification purposes, and if so, one or more additional measures must be taken to enhance due diligence, for example by, inter alia, gathering additional documents, data or information, or taking additional steps to verify documents; or

ii. if a business relationship or occasional transaction is to be undertaken with a:

- politically exposed person (PEP),
- family member or close associate of a PEP;
- a beneficial owner of a customer, third party for whom the customer is acting or a beneficial owner of a third party for whom the customer is acting is a PEP or family member or close associate of the PEP; or
- person who is or has been entrusted with a prominent function by an international organization, i.e. Director, Deputy Director and Member of the Board or equivalent functions.

In which case the business must provide for senior management approval for the relationship to be established, must take adequate measures to establish the source of wealth and funds which are involved and must conduct enhanced monitoring of any relationship entered into; and

iii. Where the service provider has, or proposes to have, a business relationship with, or proposes to carry out an occasional transaction with, a person connected with a country that does not apply, or insufficiently applies, the FATF Recommendations.

iv. If any other situation which by its nature can present a higher risk of money laundering and terrorist financing.

As such the NRSP is advised to perform EDD for higher risk categories of customers, business relationships or transactions such as:

i. Taking additional steps to verify the customer due diligence information by requesting two (2) forms of identification document.

ii. Obtaining due diligence reports from independent experts to confirm the veracity of the customer due diligence information.

iii. Requiring board and senior management approval for higher risk customers.

iv. Requiring more frequent reviews of high risk business relationships.
v. Enhanced ongoing monitoring.

In assessing the risks in relation to money laundering and terrorist financing, the NRSP is advised to apply systems and controls that can appropriately identify and manage the enhanced risk associated with clients or transactions in or from countries that are prone to corruption, terrorism or conflicts. The NRSP should make appropriate use of relevant findings issued by the FATF, the CFATF, the FIU and the Financial Services Authority (FSA). Additionally, in conducting its EDD the NRSP **must** ensure that it is aware of new or developing technologies that might favour anonymity and take measures to prevent its use for the purpose of money laundering and terrorist financing.

c. NON FACE TO FACE BUSINESS

When the NRSP is conducting non-face-to-face business with clients that have not been physically present for the purposes of identification and verification, it is advised to have policies, procedures, systems and controls in place to manage specific risks associated with such non-face to face business, relationships or transactions.

Where the NRSP is approached via the internet, post or telephone, it **must** carry out non-face to face verification, either electronically or by reference to documents. The NRSPs **must** apply additional EDD measures and undertake enhanced ongoing monitoring such as**:**

i. Obtaining copies of identification documents which are certified by:
- A member of the judiciary, a senior public servant
- An officer of an embassy, consulate or high commission of the country of issue of documentary evidence of identity
- A lawyer or notary public who is member of a recognized professional body
- An actuary who is member of a recognized professional body
- An accountant who is member of a recognized professional body
- A director, officer or manager of a regulated person, or of a branch or subsidiary of a group headquartered in a well-regulated jurisdiction

ii. Verifying additional aspect of identity or other CDD information from independent sources.

iii. Contacting the customer via telephone on a home or business number which has been verified prior to establishing a relationship, or before transactions are permitted, using the call to verify additional aspects of identification information that were previously provided.

Where the client is a legal person, the NRSP is recommended to require documentary evidence of the continuing existence of the legal person (certificate of good standing) and a certified copy of identification and address documentation to verify the address of any person defined therein. The NRSP is must to ensure that adequate procedures for monitoring the activities of non-face to face businesses are implemented and managed effectively.

3.1.6 STEP 6: <u>Suspicious Activity Reporting (Sars)</u>

The NRSP **<u>must</u>** routinely monitor for and detect suspicious activity, and is recommended to, at a minimum, examine the background and purpose of the following:

- Complex or unusually large transactions, which have no apparent visible economic or lawful purpose. This covers both completed and attempted transactions;
- Transactions outside the usual pattern of the client's activity;
- Transactions that are deemed to be of high risk with regard to a client or business relationship, or as they relate to high risk geography, products or services; and
- Transactions, clients, or business relationships that cause the NRSP to have reasonable grounds to suspect money laundering, terrorist financing or some other predicate offence.

The NRSP is **<u>must</u>** ensure that its directors, officers and employees (permanent and temporary) are advised not to disclose to the subject or any other person, the fact that a SAR or related information has been or will be reported or provided to the Compliance / Reporting Officer or the FIU. This is considered to be tipping off and prejudicing an investigation and is an offence.

a. Internal and external reporting

In light of the obligation to file Suspicious Activity Reports (SARs), the NRSP is required to implement relevant internal policies, procedures, processes and controls for the purposes of detecting money laundering and terrorist financing. This should enable employees to report to the Compliance/ Reporting Officer any suspicion or knowledge of money laundering, terrorist financing or other predicate offence that is identified.

i. The internal procedures should clearly set out what is expected of individuals who form such suspicions or obtain such knowledge. The

reports can take any form the NRSP specifies in its internal procedures. Overall the NRSP should ensure that, whatever form the reporting takes, relevant personnel are aware of the internal procedures to be used and all of the necessary information is captured. Consideration should be given to how to minimize the number of copies of reporting information held within a business. For external reporting to the FIU, SAR forms can be found on the FI's website, which must be used when submitting an external SAR to the FIU. The report must be supplemented by copies of third party documents.

ii. The Compliance / Reporting Officer is responsible to ensure that every employee is aware of his/her role and duty to receive or submit internal suspicious activity reports.

iii. In certain circumstances, where the Compliance/ Reporting Officer is unsure whether the matter amounts to suspicion, they are advised to err on the side of caution and file the SAR. However, it should not be defensive filing and all of relevant supporting documents must be provided. The Compliance/ Reporting Officer is required to assess suspicious activity internally and make an internal report outlining the outcome of his/her assessment, which should include the decision on whether or not to file an external SAR with the FIU. This practice would help in protecting the NRSP from situations where the Supervisory Authority is conducting onsite examinations and where a transaction is later flagged as suspicious either internally or externally.

iv. Where the Compliance/ Reporting Officer concludes that no external report should be made, the justification of such a decision must be recorded.

v. The NRSP **must** inform all employees of their obligation to report any suspicious activity to the Compliance/ Reporting Officer or to the FIU, the failure of which constitutes an offence.

3.1.7 Step 7: Staff Awareness And Training

The NRSP **must:**

a. Undertake measures to ensure that all 'relevant' employees are 'made aware' of the laws relating to money laundering and terrorist financing within St. Vincent and the Grenadines and regularly provide training on how to recognise and deal with transactions which may be related to money laundering or terrorist financing. Training should also be made available to all partners in firms, managers, sole practitioners and it is necessary to train all client-facing staff.

b. Develop a training plan, in which the objective is to create an environment effective in preventing money laundering and terrorist financing and which thereby helps protect individuals and the business.

c. Consider not only staff who have involvement in client work or are interacting with customers, but also, where appropriate, those who deal with the business finances, and those who deal with procuring services on behalf of the business and who manage those services.

d. Provide comprehensive training to all relevant staff members, or choose to tailor its provision to match more closely the role of the employees concerned. The NRSP must take into consideration the anti-money laundering and counter-terrorist financing laws of Saint Vincent and the Grenadines, as set out below:

   i. The Anti-Money Laundering and Terrorist Financing Regulations, No. 20 of 2014 as amended by No.25 of 2017
   ii. The Proceeds of Crime Act, No. 38 of 2013 as amended by No.18 of 2017
   iii. The Anti-Terrorist Financing and Proliferation Act, No. 14 of 2015 as amended by No.17 of 2017
   iv. The Financial Intelligence Unit Act, Cap 174 as amended by No.7 of 2013
   v. Anti-Money Laundering and Terrorist Financing Code 2017
   vi. Non-Regulated Service Providers Regulations, 2019

e. Provide training on the internal consultation and advisory systems (to assist individuals in assessing whether they have a valid suspicion), internal reporting systems and expectations for confidentiality and the avoidance of tipping off and alerting a money launderer.

f. Provide training on an annual basis or based on new trends and typologies in money laundering and terrorist financing, using new case law or national/international findings, or by a change in the profile and perceived risks of the business. The NRSP must document its assessment as to whether the current training and state of awareness of employees is sufficient, or whether a supplement is needed.

g. Keep records of training provided. Training methods may be selected to suit the size, complexity and culture of the business, and may be delivered in a variety of ways including face to face, self-study, e-learning and video, or a combination of methods

h. Make arrangements to ensure new staff are trained as soon as possible after they join the business.

3.1.8 STEP 8: Internal and External Audit

The FIU shall conduct On-site Examinations to determine the effectiveness of implementation of the measures outlined in the Compliance Programme. However, the NRSP **must** maintain adequate procedures such as internal and external audits for monitoring and testing the effectiveness of:

- **i.** The policies and procedures of the compliance regime
- **ii.** The training provided

a. Internal Audit

The scope of the Internal Audit Examination shall cover the accuracy of customer identification information, suspicious transaction reports, and all other records and internal controls pertaining to compliance with AML/CFT obligations. Internal audits shall be conducted at least **once** (1) every year or at such frequency as necessary, consistent with the risk assessment of the NRSPs.

b. External Audit

The Independent External Audit Examination must be conducted once every two (2) years or at such frequency as necessary, consistent with the risk assessment of the NRSPs. This **must** be conducted by an independent third-party auditor approved by the FIU.

The results of the internal and external audit shall be timely and directly communicated to both the NRSP's Board of Directors or senior management, or the partners or the sole proprietor, as the case may be, and the compliance officer. There shall also be a written procedure by which deficiencies in a compliance program are promptly remedied once identified by either the internal or external audit. Moreover, audit results relative to AML/CFT compliance shall promptly be made available to the FIU upon request. NRSPs are required to identify and assess the ML/TF risks that may arise in relation to the development of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products

3.1.9 STEP 9: Record Keeping

The NRSP **must:**

- **a.** Keep records of clients' or customers' identity, the supporting evidence of verification of identity (in each case including the original and any updated records), all account files, its business relationships (including correspondence) with them and details of any occasional transactions and monitoring of the relationship. These records must be kept for **seven years** after the end of the

relevant business relationships or completion of the transactions. The NRSP must ensure the retention of historic, as well as current records.

b. Store securely information relating to both internal and external reports for at least seven years after receipt. This includes copies of the quarterly SARs submitted to the FIU

c. Keep all records following the establishment of the relationship or the completion of the transaction, regardless of whether the account or business relationship is ongoing or has been terminated.

d. Maintain records of the annual compliance report, and any other reports that highlight the level of compliance, deficiencies and actions, including reports submitted to senior management.

e. Make the transaction records and other identification data available to the FIU upon request. Further in cases where there is an ongoing investigation the NRSP must hold the necessary records for the life of the investigation, if not indefinitely.

f. Maintain records including dates of training sessions, a description of training provided and the names of the employees who received training for a period of at least seven (7) years from the date on which training was received

g. Keep records of all correspondence received from the FIU and any other Law Enforcement Agency.

h. Keep records of ALL internal and external audits conducted.

CHAPTER 4- IDENTIFYING SUSPICION

4.1 SPECIFIC SUSPICIOUS INDICATORS

The following guidance is divided into the major categories of NRSPs and identifies specific indicators of suspicious activity which is to be observed by members of the said sectors.

4.1.1 Lawyers

In carrying out their duties lawyers are often required to hold clients' funds, manage said funds, serve as a conduit for the sale and purchase of large properties, manage companies and trusts or carry out executive duties. The level of involvement paired with the frequency of large monetary transactions, the shifting or protection of assets and verifying of information makes this NRSP a prime target for ML/TF transactions or behaviours.

Recommendation 22 of the FATF Standards provides that the customer due diligence and record-keeping requirements of the Recommendations apply to legal professionals when they prepare for and carry out certain specified activities for their clients, namely:

a) Buying and selling of real estate;
b) Managing of client money, securities or other assets;
c) Management of bank, savings or securities accounts;
d) Organisation of contributions for the creation, operation or management of companies; and
e) Creation, operation or management of legal persons or arrangements, and buying and selling of business entities

(i) The purchase and sale of real property

Real estate, both commercial and residential, accounts for a high proportion of confiscated criminal assets, demonstrating that this as a clear area of vulnerability. In many countries, legal professionals are either required by law to undertake the transfer of property or their involvement is a matter of tradition, custom or practice. Lawyers will hold or control (e.g. through a financial institution) and transfer or control the transfer of the relevant funds for the purchase of the real estate assets.

Some criminals may seek to invest the proceeds of their crime in real estate without attempting to obscure their ownership of the real estate. Alternatively, criminals may seek to obscure the ownership of real property by using false identities or title the property in the names of family members, friends or business associates, or purchase property through an entity or a trust. Therefore CDD must be conducted.

(ii) Client funds

Client accounts are accounts held by legal professionals with a financial institution. Legal professionals are required to hold client funds in a separate account with a financial institution and use the funds only in accordance with their client's instructions. The purpose of these accounts is to hold client funds in "trust" for or for a purpose designated by the

client. No funds may pass through a client account without being attached to an underlying legal transaction or purpose, and the legal professional is required to account for these funds.

The use of client accounts has been identified as a potential vulnerability, as it may be perceived by criminals as a means to either integrate tainted funds within the mainstream financial system or a means by which tainted funds may be layered in such a way to obscure their source, with fewer questions being asked by financial institutions because of the perceived respectability and legitimacy added by the involvement of the legal professional. Legal professionals can seek to limit their exposure to this risk by developing and implementing policies on the handling of funds (e.g. currency value limits) as well as restricting access to account details to prevent unsanctioned deposits.

(iii) Formation of companies and trusts

Criminals may seek the opportunity to retain control over criminally derived assets while frustrating the ability of law enforcement to trace the origin and ownership of the assets. Companies and often trust and other similar legal arrangements are seen by criminals as potentially useful vehicles to achieve this outcome. While shell companies, which do not have any ongoing business activities or assets, may be used for legitimate purposes such as serving as a transaction vehicle, they may also be used to conceal beneficial ownership, or enhance the perception of legitimacy. Criminals may also seek to misuse shelf companies formed by legal professionals by seeking access to companies that have been 'sitting on the shelf' for a long time. This may be in an attempt to create the impression that the company is reputable and trading in the ordinary course because it has been in existence for many years. Shelf companies can also add to the overall complexity of entity structures, further concealing the underlying beneficial ownership information.

(iv) Management of companies and trusts

In some cases, criminals will seek to have legal professionals involved in the management of companies and trusts in order to provide greater respectability and legitimacy to the company or trust and its activities. In some countries professional rules preclude a legal professional from acting as a trustee or as a company director, or require a disclosure of directorship positions to ensure independence and transparency is maintained. In countries where this is permitted, there are diverse rules as to whether that legal professional can also provide external legal advice or otherwise act for the company or trust. This will determine whether any funds relating to activities by the company or trust can go through the relevant legal professional's client account. In addition, in some countries, the non-legal counsel of a legal professional acting in a business capacity for formation or management of companies or trusts may not be protected by the legal professional privilege.

(v) Acting as nominee

Individuals may sometimes have legal professionals or other persons hold their shares as nominees, where there are legitimate privacy, safety or commercial concerns. However, criminals may also use nominee shareholders to obscure their ownership of assets. Legal professionals should identify beneficial owners when establishing business relations in these situations. This is important to prevent the unlawful use of legal persons and

arrangements, by gaining a sufficient understanding of the client to be able to properly assess and mitigate the potential ML/TF risks associated with the business relationship. Where legal professionals are asked to act as nominees, they should understand the reason for this request and ensure that they are able to verify the identity of the beneficial owner of the shares and that the purpose is legitimate.

(vi) Other services that might indicate ML/TF activity

Legal professionals possess a range of specialised legal skills that may be of interest to criminals, in order to enable them to transfer value obtained from criminal activity between parties and obscure ownership. These specialised skills include the creation of financial instruments and arrangements, advice on and drafting of contractual arrangements, and the creation of powers of attorney. In other areas of legal specialisation, such as probate (succession) and insolvency or bankruptcy work, the legal professional may simply encounter information giving rise to a suspicion that the deceased or insolvent individual previously engaged in criminal activity or that parties may be hiding assets to avoid payment to legitimate creditors. Where these circumstances involve legal professionals engaging in a specified activity, legal professionals must carefully consider their AML/CFT obligations. Legal professionals should also consider the ML/TF risk in such circumstances.

(vii) Legal professional privilege

In observing the AML/CFT regulations it is often queried whether complying with the regulation will lead to a breach of professional privilege or legal confidentiality held between the attorney and client. Rest assured; compliance does not result in the breach of either as established in the recent Jamaican judgment of *The Bar Association of Jamaica v The Attorney General et al Claim No. 2014 HCV 0772* because the transactions / activities under recommendation 22 are not inclusive of matters which fall under legal professional privilege or professional secrecy such as information lawyers, notaries or other legal professionals receive from or obtain through a client:

a. in the course of ascertaining their legal position; or
b. in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings

Further, a failure to take necessary safeguards, to ignore clear illicit activity or to facilitate illicit transactions will result in the attorney being an accomplice to the crime and would be in contravention of the legal ethical principles that ground the legal profession.

The following indicators serve as a non-exhaustive guide on how to identify illicit activities:

a. Appointing a lawyer in financial or commercial transactions and requesting the concealment of the customer's name in any of these transactions.

b. The customer resorts to lawyers to create companies, particularly international business companies, from outside the country (offshore) in a way that shows that the objective of creating the company is to conceal the illicit source of the funds.

c. The customer resorts to lawyers to invest in the real estate market but the purchase or sale prices are not commensurate with the real estate value.

d. The customer requests, upon hiring a lawyer to incorporate a company, to transfer/deposit the incorporation fees or the capital to/in the bank account of the lawyer through multiple accounts that he has no relation to without a reasonable justification.

e. The lawyer manages investment portfolios, in countries allowing such activity, and receives instructions from the customer to conduct transactions that have no clear economic reason.

f. The sources of funds used for requested transactions are from large financial transactions that cannot be justified by any known business or corporate purpose.

g. Requests made for payments to third parties without clear reason or a valid corresponding transaction.

4.1.2 Notaries

Given the position held by notaries and their ability to facilitate the signing of documentation necessary to create trusts and or business entities, their ability to facilitate sale and purchase agreements as well as share transfers, amongst other such duties it is pertinent that they observe the following non-exhaustive list of suspicious indications as a means to avoid becoming a facilitator to money laundering and terrorist financing:

a. Customers desire to create or buy a company that has a suspicious objective, does not realize profits or does not seem to be connected to his/her usual profession or related activities, without being able to submit sufficient explanations to the notary.

b. When a customer sells assets or real estate properties repeatedly without realizing any profit margin or submitting a reasonable explanation in this respect.

c. The customer who creates or wishes to create different companies in a short timeframe for his/her own interest or the interest of other persons without reasonable financial, legal or commercial grounds.

d. The customer's use of another person as a facade to complete a transaction without any legitimate financial, legal or commercial excuse.

4.1.3 Accountants & Auditors

According to FATF Recommendation 22, Customer Due Diligence and Record-Keeping Requirements are to be applied to Real estate agents accountants when they prepare for or carry out transactions for their clients concerning the following activities:

a) Buying and selling of real estate;
b) Managing of client money, securities or other assets;
c) Management of bank, savings or securities accounts;
d) Organisation of contributions for the creation, operation or management of companies; and
e) Creation, operation or management of legal persons or arrangements, and buying and selling of business entities

The very nature of the work carried out by accountants and auditors places them at the center of the ML/TF realm. This is because they offer financial services and advice to persons in respect of how to handle assets, measures to take in respect of taxes and tax law compliance, advice and procedural guidance on liquidation and insolvency, active money management and bookkeeping etc. An accountant's advice is sometimes sought at least in relation to initial corporate, tax and administrative matters. Additional, criminals may seek to have accountants involved in the management of companies and trusts in order to provide greater respectability and legitimacy to the company or trust and its activities.

Individuals may sometimes have accountants or other persons hold their shares as a nominee, where there are legitimate privacy, safety or commercial concerns. However, criminals may also use nominee shareholders to obscure their ownership of assets. Where accountants are asked to act as a nominee, they should understand the reason for this request and ensure they are able to verify the identity of the beneficial owner of the shares and that the purpose appears to be legitimate.

Criminals may abuse services provided by accountants to provide a sense of legitimacy to falsified accounts in order to conceal the source of funds. For example, accountants may review and sign off such accounts for businesses engaged in criminality, thereby facilitating the laundering of the proceeds. Accountants may also perform high value financial transactions allowing criminals to misuse accountants' client accounts. Insolvency practice, which may be conducted by certain accountancy professionals also pose a risk of criminals concealing the audit trail of money laundered through a company and transferring the proceeds of crime. Accountancy services may also be used to facilitate tax evasion and VAT fraud.

Bear in mind, that due to these activities and the level of involvement, like attorneys, they too are considered protective gatekeepers. As gatekeepers they must be aware of the AML/CFT regulations and seek to be compliant. To assist in compliance endeavours the following indicators are to be used to assist in the prevention and detection of ML/TF activities within this sector:

a. The customer does not express concern in incurring losses or realizing extremely low profits in comparison with persons engaged in the same business. The customer remains persistent in pursuing his/her activities.

b. High volume of foreign transfers from/to the client's accounts or the sudden increase of the revenue and cash amounts he obtains that is not consistent with his/her usual income. This type of activity occurs in a manner without any justification.

c. Customer's receipt of cash or high value cheques, which do not match the volume of his/her work or the nature of his/her activity, particularly if the transactions come from persons who are not clearly or justifiably connected to the client.

d. Unjustified amounts or deposits in the customer's account whose origin or cause is difficult to identify.

e. Disproportionate amounts, frequency and nature of transactions carried out by the customer that are not consistent with the nature of his/her business, profession or known and declared activity, particularly if these transactions are carried out with suspicious countries that are not connected with his/her apparent business domain.

f. Repeated large cash transactions including foreign exchange transactions or cross-border fund movement when such types of transactions are not consistent with the usual commercial activity of the customer.

4.1.4 Real Estate Agents (may apply to Lawyers)

Like lawyers, real estate agents would deal with the buying and selling or properties and transactions of large sums. The use of real estate transactions is one of the proven and most frequent methods of Money Laundering employed by organised crime. The real estate sector is affected by different types of predicate offences which lead to Money laundering and Terrorist Financing such as forgery, fraud, tax evasion and embezzlement. As such they need to be mindful of the following which depicts ways in which their services may be misused for ML/TF purposes:

a. Buying or selling real estate at a price not consistent with its actual value, whether by increase or decrease, in comparison with the market prices or the prices of similar real estate in the same area.

b. Repeated buying of real estate whose prices do not suit the buyer's usual capacity according to the information available about him/her or expected from him/her (due to the nature of his/her profession or business), which creates suspicion that he/she is carrying out these transactions for other persons.

c. Trying to register the real estate at a price less than actual value or the amount that will be paid and the difference paid "under the table".

d. The customer is not interested in inspecting the real estate to check its structural condition prior to the completion of the purchase.

e. Purchase of a number of properties in a short period of time without expressing any interest in their location, condition, costs of repairs and otherwise.

f. Sale of the real estate directly after buying it at a price less that the price of purchase.

g. The customer is not interested in putting his name on any file that may relate him/her to the property or use of different names when submitting purchase offers.

h. Buying real estate in the name of another person who is not clearly or justifiably connected to the customer.

i. Replacing the buyer's name shortly before the completion of the transaction without sufficient or clear justification.

j. Arranging the financing of purchase transactions, partially or in full, through an unusual source or an offshore bank.

4.1.5 Jewelers

Given the ease at which precious metals such as gold, precious stones and jewels can be transported, bought, sold and repurposed, it has made the jewelry industry a target for ML/TF transactions. The lucrative nature of these tradable goods and the ease of trade will enhance the target appeal of this NRSP sector by criminals. As such the following indicators should be used as a non-exhaustive guide for indicating suspicious activity:

a. Customer's purchase of jewels of high value does not correspond with what is expected from him/her (upon the identification of his profession or the nature of his/her business).

b. Regular purchase of high value commodities or large quantities of a specific commodity in a way that does not match the usual transactions carried out by the customer or the usual pattern of the business for his/her income.

c. Attempts to recover the amount of recent purchases without a satisfactory explanation or when the customer tries to sell what he/she recently bought at a price that is much less than the purchasing price.

d. Attempts to sell high value jewels at a price much less than their actual or market value.

e. Customer's willingness to pay any price to obtain expensive jewels without any attempt to reduce or negotiate the price.

f. Delivers jewels or precious metals purchased with illicit funds to be repurposed and asserts full ownership of the product in question but requests payment be made to another person or entity.

4.1.6 Car Dealers

This particular industry involves the selling, buying and leasing of new and used automobiles. Given the cash intensive nature of these activities, it opens the industry up to potential use by criminals for money laundering. The following indicators depict how this industry is used for money laundering and serves as a guide to assist in the identification of illicit use:

a. Where the purchaser deposits below the reporting threshold or the purchasing of vehicles with sequentially numbered cheques or money orders.

b. Frequent trading in of vehicles and conducting successive transactions of buying and selling vehicles to produces layers of transactions

c. Receiving payment from third parties outside the jurisdiction, in areas with ineffective or relaxed money laundering controls.

d. Large, single payment, cash sums for purchase of vehicle that fall outside the customer's regular payment scheme and cannot be accounted for by their usual line of business or general earnings.

e. Requests for "down-trading"; whereby the customer requests that their vehicle be traded in for a vehicle of lesser value and for the remaining balance to be paid to them by way of cheque drawn from the dealers account and not cash. (This should be of particular interest in instances where the customer has a known criminal history).

4.1.7 Casinos

Due to the nature of this entities' operations it provides a base for a legitimate flow of large sums of cash between the casino and customer. However, the large influx of cash makes it a primary facilitator for ML/TF transactions especially in the placement and layering stages described in Chapter 1. This is because it allows for the laundering of cash to cheques utilizing casino credit to add a layer of transactions before the funds are transferred out.

A prime example of such a scenario arises where a launderer purchases casino chips or credit with cash that has been generated from criminal activity and then requests repayment by way of cheque drawn from the Casino's account. For a further evasion, the launderer will often request that the cheque be made available at another branch of the casino, often in another country, under the guise of travel.

Therefore, it is pertinent that casino operators be aware of the following indicators of suspicious activity. It should be noted that this list is not exhaustive but should be utilised as a guide:

a. The value used is disproportionate to the customer's resources in light of his/her declared profession.

b. Changes in the gambling routines for a certain customer in disproportion with his/her income that was declared beforehand, e.g. if he/she purchases chips for a game that he/she does not usually play or if it is observed from the objective circumstances that he/she does not seek profit or is not concerned about losing.

c. Buying gambling chips in cash, then requesting to exchange them for a cheque from the casino.

d. Two or more customers purchasing chips in small amounts, utilizing minimal gaming opportunities and then combining the funds to request a single cheque payout from the casino.

e. Avoiding proof of identification by reducing the chips during cash-out or ensure the sum paid out is under the reportable amount.

f. Requesting the issuance of the casino cheque in the name of a third party or to no specified payee.

g. Withdrawing large sums from a deposit account and requesting multiple casino cheques to be issued with each cheque being less than a reportable amount ($10,000).

4.2 GENERAL SUSPICIOUS ACTIVITY/ INDICATORS

The following serves as general guidance to be observed by **ALL** NRSPS in respect of identifying suspicious activity:

a. The customer has an unusually comprehensive knowledge of money laundering issues and the AML Law without justification. For instance, if the customer points out he/she wishes to avoid being reported.

b. Attempts to divide the amounts of any operations below the applicable designated threshold of reporting to the competent authorities regarding money laundering or terrorist financing suspicion.

c. The customer has an unusual interest in the internal policies, controls, regulations and supervisory procedures and unnecessarily elaborates on justifying a transaction.

d. When a customer has accounts with several international banks or has lately established relationships with different financial institutions in a specific country without clear grounds, particularly if this country does not apply an acceptable AML/CFT regime.

e. The customer is reserved, anxious or reluctant to have a personal meeting.

f. The customer uses different names and addresses.

g. The customer requests or seeks to carry out the transactions without disclosing his identity.

h. The customer refuses to submit original documentation, including those related to his identification.

i. The customer intentionally conceals certain important information like his address (actual place of residence), telephone number or gives a non-existent or disconnected telephone number.

j. The customer uses a credit card issued by a foreign bank that has no branch/headquarters in the country of residence of the client while he/she does not reside or work in the country that issued said card.

k. Unusual transactions in comparison with the volume of the previous transactions or the activity pursued by the customer

l. Unnecessarily complex transactions or those that do not seem to have an economic feasibility.

m. Transactions that involve a country that does not have an efficient AML/CFT regime, that is suspected to facilitate money laundering operations or where drug manufacturing or trafficking are widespread.