FINANCIAL SERVICES AUTHORITY

SAINT VINCENT & THE GRENADINES

GUIDELINES:

SIMPLIFIED DUE DILIGENCE GUIDELINES

Issued: January 12, 2023

TABLE OF ACRONYMS

AML	Anti- Money Laundering
BO	Beneficial Owner
CDD	Customer Due Diligence
CFT	Counter-Financing of Terrorism
DNFBPs	Designated Non-Financial Business and Professions
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FI	Financial Institution
ML	Money Laundering
PEP	Politically Exposed Person
PF	Proliferation Financing
RBA	Risk Based Assessment/ Approach
SARs	Suspicious Activity Reports
SDD	Simplified Due Diligence
TF	Terrorist Financing

1.0 INTRODUCTION

Non-Bank Financial Services entities in St. Vincent and the Grenadines are regulated and supervised pursuant to the Financial Services Authority Act No. 33 of 2011. These entities are also deemed to be "service providers" in accordance with Schedule 1 of the Anti-Money Laundering and Terrorist Financing (AML&TF) Regulations, which means that they must comply with the various Anti-Money Laundering /Counter Financing of Terrorism (AML/CFT) requirements outlined in AML/CFT legislation.

The following Guidelines are issued pursuant to section 10 of the Financial Services Authority Act. The guidance herein specifically addresses the simplified customer due diligence[1] (SDD) approach to be applied by regulated entities and clarifies areas of ambiguity within the substantive legislative framework relating to the application of simplified due diligence.

2.0 PURPOSE AND OBJECTIVES

To provide guidance for the application of SDD procedures and to allow for consistent application of regulations 10, 11, 12, and 16 of the Anti-Money Laundering and Terrorist Financing Regulations of 2014 and Part II of the Anti-Money Laundering and Terrorist Financing Code of 2017.

3.0 SCOPE OF APPLICATION

These Guidelines apply to all registered non-banking financial entities in St. Vincent and the Grenadines under the supervisory framework of the Financial Services Authority.

4.0 PROVISO STATEMENT

These Guidelines are designed to guide non-banking financial institutions in conducting appropriate customer due diligence (CDD) measures which will aid in the detection, reporting, and investigation of suspicious transactions, thereby reducing overall money laundering (ML) and terrorist financing (TF) risks.

The provisions herein, are only applicable where financial entities are satisfied that their customers' transaction pattern/activities fall into the simplified due diligence criteria as defined below. More specifically, it highlights a risk-based approach to the adoption of CDD, at various stages of the business relationship.[2] Nevertheless, the financial entity **should** be able to reasonably justify the risk classification attached to each customer, be it at onboarding or throughout the relationship with the customer. Despite the option for the application of SDD measures, financial entities should continually monitor business relationships for trigger events, which may increase risk profiles and create a requirement for further due diligence in the future.

[1] While these procedures are outlined in the FATF Recommendations and international best practices, there are current gaps in national AML/CFT laws which will be addressed by amendments.

[2] If during the relationship with the customer, other information becomes available that suggests that the member may pose a higher risk than originally assessed, a higher level of due diligence should be applied to that customer.

5.0 RISK-BASED APPROACH

All Financial Institutions (FIs) are required to adopt a risk-sensitive approach when conducting due diligence assessments for all customers and transactions. Each customer should be given a risk rating based on predetermined and approved parameters which are sufficiently robust but flexible, thereby avoiding acts of financial exclusion. For the purposes of this guidance, the emphasis would be placed on customers and transactions which are rated as low risk and there is no suspicion of money laundering or terrorist financing

When assessing the ML/TF risks at the institutional level consideration should be given to factors such as the type of customer, their geographic location, delivery channels, and the general product/services being accessed by each customer. These variables, singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD applied. Examples of some variables which should form part of an entity's ongoing monitoring activities:

i. The identified purpose for an account or relationship;
ii. The customer involved (for example, Foreign PEPs must be subject to EDD in all instances);
iii. Transaction size and pattern (assets being deposited);
iv. The source and intended purpose of the funds; and
v. The duration of the business relationship.

6.0 CUSTOMER DUE DILIGENCE

General Requirements

Recommendation 10[3] of the Financial Action Task Force (FATF) Recommendations requires, inter alia, FIs to conduct CDD assessments on all customers to ensure that sufficient information is obtained and maintained vis a vis the customers of the institution.

CDD evaluations should be undertaken when:

i. establishing a business relationship;
ii. carrying out occasional transactions, including one-off transactions;
iii. there is a suspicion of ML or TF; or
iv. the FI has doubts about the veracity or adequacy of previously obtained customer identification data.

The CDD Measures to be taken are as follows:

i. Identifying the customer and verifying the customer's identity using reliable, independent source documents, data, and information;
ii. Identifying the beneficial owner (BO) and taking reasonable measures to verify the identity of the BO
iii. Understand, and as appropriate, obtain information on the purpose and intended nature of the business relationship; and

[3] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

iv. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business, and risk profile.

FIs are required to apply each of the CDD measures set out under (i)-(iv) above, but should determine the extent of such measures using the risk-based approach (RBA). The requirement above should apply to all new and existing customers on the basis of risk and materiality. CDD is not a static exercise and should be proportionate to the ML/TF risks posed by the customer. As such, FIs must be cognizant that a customer's risk profile may change and should therefore establish monitoring, reporting, and other procedures to manage these risks. Following this, FIs should consider whether to apply Simplified (SDD) or enhanced due diligence (EDD)[4].

If SDD has been applied, it is important for FIs to periodically check the activities and risk profile of the client to determine that SDD can still be applied. This means that some monitoring of these business relationships is always necessary to assess whether the business relationship is actually being used for the reasons provided. It can also follow from an event-driven review that SDD can no longer apply. When there are facts or circumstances which lead to an increased ML/TF risk or other reasons to re-assess the risk profile of the client, CDD or EDD has to be carried out. The service provider should keep sufficient evidence in the customer file as to the reason why SDD was applied, for example, information on the customer risk profile and reason(s) for the application of SDD.

6.1 Simplified Due Diligence

SDD refers to the minimum level of due diligence that a service provider should conduct on a customer or potential customer. SDD **should not** be interpreted as an exemption from CDD. CDD should be applied in all instances. SDD is considered appropriate where there is a low risk that the services will be exploited for ML or TF. SDD should be applied to these four CDD components:

a) identification/verification of a customer,
b) identification/verification of BO,
c) understanding the purpose and nature of the relationship, and
d) ongoing monitoring of the relationship.

6.1.1 Simplified CDD measures

There are circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, and provided there has been an adequate analysis of the risk by the service provider, it could be reasonable for service providers to apply simplified CDD measures.

[4]EDD and enhanced monitoring are applied in cases where the profile of a customer who was previously risk rated as low-risk changes after the establishment of relation. The financial institution is required to intensify its risk mitigation measures for such customers to match the higher risk posed.

Examples of potentially lower-risk situations include the following:

(a) Customer risk factors:
- Financial institutions and DNFBPs – where they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements.
- Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
- Public administrations or enterprises.

(b) Product, service, transaction, or delivery channel risk factors:
- Life insurance policies where the premium is low (e.g., an annual premium of less than USD/EUR 1,000 or a single premium of less than USD/EUR 2,500).
- Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral.
- A pension, superannuation, or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme.
- Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

(c) Country risk factors:
- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.
- Countries identified by credible sources as having a low level of corruption or other criminal activity.

In making a risk assessment, service providers could when appropriate, also take into account possible variations in money laundering and terrorist financing risk between different regions or areas within a country.

Having a lower money laundering and terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is at lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions.

It should be clearly highlighted that SDD **should only** be applied to low-risk customers. Examples of SDD that can be applied include but are not limited to:

a) Verifying the identity of the customer and the BO after the establishment of the business relationship;
b) Reducing the frequency of customer identification updates;
c) Reducing the degree of ongoing monitoring and scrutinizing of transactions, based on a reasonable monetary threshold;

d) Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but rather, inferring the purpose and nature from the type of transactions or business relationship established.

Where the risks of ML or TF are identified as low, FIs are allowed to perform SDD measures for the designated activity or with specific customers. However, regard must be given to the reason for the lower risk classification. The simplified measures should be commensurate with the lower risk factors (e.g., the simplified measures could relate only to customer onboarding measures or to aspects of ongoing monitoring). These SDD measures may include but are not limited to:

1. Changing the timing of customer due diligence where the product/service or transaction sought has features that limit its use for ML/TF e.g.

    i. Verify the customer's or BO's identity after the establishment of the business relationship or
    ii. Verify the customer's or BO's identity once transactions exceed a defined threshold or after transaction patterns, expectations and limits have been determined. Regulated entities must adopt reasonable measures to ensure that:

        a) The adoption of these measures does not result in a de facto exemption from CDD. That is, steps must be taken by the institution to ensure that the customer or BO's identity will ultimately be verified within 5-7 business days;
        b) The threshold or time limit is set at a reasonably low level (although, with regards to terrorist financing, financial entities should note that a low threshold alone may not be enough to reduce risk);
        c) There are systems in place to detect when the threshold, unusual transaction or time limit has been reached; and
        d) They do not defer CDD or delay obtaining relevant information about the customer where regulations require that this information be obtained at the outset.

2. Modifying the quantity of information obtained for identification, verification, or monitoring purposes, for example by:
3.
    i. Opting to verify identity, based on information obtained from one primary and reliable source of an identification document or data source only (for example, government-issued identification); or
    ii. Basing the due diligence information required on the product/service design (where the product/service is such that it has limited scope for ML/TF/PF to occur) or on the nature and purpose of the business relationship e.g., the payment of death benefit

4. Adjusting the quality or source of information obtained for identification, verification or monitoring purposes;

5. Changing the frequency of CDD updates and review of the business relationship, for example, carrying out these activities only when trigger events occur. It is the

responsibility of financial entities to ensure that this does not result in a de facto exemption for keeping CDD information up-to-date;

6. Altering the frequency and intensity of transaction monitoring, for example, monitoring transactions above threshold only whether it is attained by one truncation or cumulative transaction over a predetermined period.

SDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply. Therefore, all financial entities must document and adopt a flexible and risk-sensitive approach to due diligence for AML/CFT.

6.1.2 Reliance placed on prior identification and verification activities

FIs may rely on the identification and verification steps taken when performing subsequent business unless there are doubts concerning the veracity of that information. In so far as the expected transaction levels and other parameters for customers do not change materially or the purpose for which the account is utilized remains consistent with the customer's business profile. Where material differences become apparent, a reassessment exercise should be performed and, if required, the customer risk should be reclassified immediately.

6.1.3: Resource Material

FIs should pay particular attention to publications from the FATF and other reputable international bodies in the application of the risk-based approach and implementation of CDD measures including SDD. Some resource materials include;

- The FATF Methodology (Updated October 2021)
- The FATF Recommendation (Updated March 2022)
- FATF Guidance Risk-Based Approach for Money or Value Transfer Services (2016)
- FATF Guidance Risk-Based Approach Supervision (2021)
- FATF Guidance- AML/TF Measures and Financial Inclusion- with supplement on CDD

COMMENCEMENT

These Guidelines shall come into effect this 12th day of January, 2023.

Issued by:

Financial Services Authority
P.O. Box 356
Kingstown
St. Vincent & the Grenadines
Tel (784) 456-2577 / (784) 457 2328
Electronic mail: info@svgfsa.com

APPENDIX 1: STEP BY STEP GUIDE IN APPLYING SIMPLIFIED DUE DILIGENCE MEASURES.

Indentify and Assess ML/TF Risks Using Risk-Based Approach

Risk rate customer considering:

- Type
- Business Relationship
- Geographic location
- Delivery channels being utilised
- General product/services accessed

Having established information on the customer based on above factors, the financial institution should be able to determine extent of CDD measures to be applied in respect of a customer.

Conduct Customer Due Diligence Assessment

Obtain information from the customer on:

- a) identification/verification
- b) identification/verification of BO
- c) Purpose and nature of the relationship

Conduct ongoing monitoring of the relationship.

Determine CDD Measures to Apply

- Simplified Due Diligence - appropriate where there is a low risk of ML or TF
- Enhanced Due Diligence - appropriate when there is a higher risk of ML or TF

SDD Application

ONLY applicable to low-risk customers.

- Examples of SDD that can be applied include but are not limited to:
  - a) Verifying the identity of the customer and the BO after the establishment of the business relationship;
  - b) Reducing the frequency of customer identification updates;
  - c) Reducing the degree of ongoing monitoring and scrutinizing of transactions, based on a reasonable monetary threshold;
  - d) Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but rather, inferring the purpose and nature from the type of transactions or business relationship established.

Ongoing Monitoring of Relationship

- Conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship
- Helps to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business, and risk profile.
- Ongoing monitoring should assist in determination as to whether SDD should continuously apply to customer.