Customer Due Diligence Guidelines

Saint Vincent and the Grenadines Financial Intelligence Unit

ABSTRACT

This guidance document is intended to provide institutions with necessary guidance in respect of what actions are to be taken when establishing customer relationships.

6th October 2021
FIU Ref: 001/2021

CUSTOMER DUE DILIGENCE GUIDELINES

This guidance document is intended to be a supplemental document that allows institutions to have a summary of the customer due diligence requirements and their application.

1. Categories of Customers- The first thing institutions should consider is what category the customer belongs to because the category will determine what type of procedure is to be applied when starting or even continuing a business relationship. For each category of customer your institution must identify the type of identification and relationship information collected and the procedure used to collect this data. The type of relationship being referred to means the purpose and nature of the business relationship, type and volume of activity, beneficial ownership data amongst other areas highlighted in the guidance sections below. The categories of customer may include but are not limited to:

    a) **Individuals/ Natural Persons**- identification and verification procedures are to be applied on a risk sensitive basis.

    b) **Legal Persons or Arrangements**- these include companies, trusts and other such arrangements. Where this category arises, the institution is required to identify and verify the customer and the beneficial owners. This may often require documents such as the business registration or certificate of incorporation, trust deed, partnership agreement, identity cards for natural persons involved, address of the registered office and any other such document specified within the relevant legislation highlighted below.

    c) **Third Party Representatives**- where third parties are concerned institutions are required to verify that the person purporting to act on behalf of the customer is authroised to do so and should identify and verify the identity of that person.

    d) **Non-Face to Face Customers**- will require identification and verification, however, it may be permissible to have verification completed after the business relationship has been established as a means of preventing disruption of services. It should be noted that the delay of verification is discretionary and should only be applied for low risk customers.

    e) **PEPs**- Politically Exposed Persons (PEPs) are defined as an individual who is or has been entrusted with a prominent public function and their family members and close associates. The categories of PEPs that stem from this definition are Foreign PEPs, Domestic PEPs, International Organisation PEPs, their family members and close associates. It is a well established fact that politically exposed persons (PEPs) are classified as a type of high-risk customer that usually require enhanced due diligence (EDD). However, based on further guidance from the Financial Action Task Force (FATF) in

their discussion of Recommendations 12 and 22, it has been clarified that the different categories of PEPs are to be treated differently in terms of the level of CDD required for them and their categorisation as a PEP should be reviewed accordingly depending on the change in their position and circumstances. For further information in relation to PEP categories and their differentiations please see the Politically Exposed Persons (PEPs) Guidance document.

2. Risk Analysis- For each category of customer highlighted, a proper risk analysis and rating of each must be given to determine the level of CDD to be applied. To determine the level of risk, the factors highlighted in the AML/CFT Compliance Programme Structural Guidelines[1] document under Chapter 4 should be consulted.

3. SDD[2]- it should be clearly highlighted that SDD should only be applied to low risk customers. Possible measures to be applied in this instance would include but are not limited to:
    a) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;

    b) Reducing the frequency of customer identification updates;

    c) Reducing the degree of on-going monitoring and scrutinising transactions, based on reasonable monetary threshold;

    d) Not collecting specified 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.

    Reliance on any of the aforementioned SDD provisions must be clearly outlined in your institution's manual.

4. EDD- should clearly stipulate that EDD is to be applied to higher risk customers and should clearly identify the procedure for starting a business relationship with a customer who falls into the EDD bracket.
    a) The main difference is that with normal CDD there is only the need for 2 pieces of documentation needed for identification and verification at the onboarding stage and then 1 piece for transactions conducted afterwards.

[1] While this document was created specifically for the Non-Regulated Service Provider (NRSP) Sector, it may be used as a reference guide for other institutions due to structure of the document and interchangeable areas covered.

[2] While these procedures are outlined in international best practices regarding AML/CFT procedures it should be noted that the national provisions regarding SDD as highlighted in Regulation 16 do not presently cover all necessary guidance and is presently being amended.

b) Whereas with EDD it requires 3 pieces of documentation at onboarding and two pieces thereafter. This sub-paragraph should also identify common categories of customers that would fall into this category for EDD.

5. Acceptable Forms of Identification & Certification- should clearly identify an accurate list of acceptable types of documents that can be used for Verification and Identification. These can include but will not be limited to:
   a) Multipurpose Identification Card,
   b) National Identification Card,
   c) Passport,
   d) Police Identification Card (with expiry date & signature),
   e) Farmer's Identification Card.

   All primary or best forms of identification must be equipped with a photo and an expiry date and should not be expired at the time of use. Independent sources otherwise known as Secondary forms of identification are those that can be paired with the primary forms for verification purposes and can include but are not limited to:

   a) utility bills,
   b) bank statements,
   c) birth certificate (but should only be used in conjunction with a recent bank statement, utility bill, any other government issued documentation, a letter of introduction from a regulated person or organization)
   d) A letter of introduction from a regulated person or a person of authority within the community such as a justice of the peace, notary, landlord or pastor.
   e) Certificate of incorporation, registration or equivalent;
   f) Partnership agreement;
   g) Any other documents referenced in the relevant legislation.

   In considering the types of acceptable documents institutions should also be aware of and clearly highlight to customers the acceptable requirements for certified copies by stating who should certify the document and what details it should include.

   The current standard of certification includes documents certified by the following persons:

   a) Notaries
   b) Justices of the Peace

c) Attorneys

d) Senior Clergy members (pastors, priests)

e) Senior Police Officer (rank of Superintendent or above)

The certification should include the following hallmarks:

a) Name and signature of certifier

b) Contact information (address and phone number) of certifier

c) Stamp of certifier

d) Relevant certification phrase "I certify this to be a true copy of the original" or any other relevant variation depending on the document.

e) Date

6. CDD Checklist- when conducting CDD there are three (3) basic categories to classify the information that will need to be collected. While the categories are standard, the information listed under each is not an exhaustive list. Best practices suggest that the categories and their content are as follows:

   A. Relationship Information- the data collected in this category is used to determine what type of relationship the customer is looking to develop with the institution, general questions to ask when collecting data is as follows:

      i. Purpose and intended nature of the business relationship;
      ii. Type of service being sought, estimated volume and value of expected activity or transactions;
      iii. Source of funds and where high risk, the source of wealth of the customer, third party or the beneficial owner;
      iv. Details of any existing relationship with your institution;
      v. If the customer is not a resident, determine the reason for using your institution's services or reason for wanting to start business relationship with your institution;
      vi. Any other information concerning the start of a business relationship that your institution would deem important;
      vii. If the potential customer, third party or beneficial owner is the trustee of a trust or a legal person including companies your institution will need to collect the following relationship information:

         a) The type of trust or legal person;
         b) The nature of activities of the trust or legal person;
         c) The place or places where the trust or legal person conducts its activities;

d) If the trust is a part of a more complex structure and if yes, the details of the structure including the existence of any underlying companies or other legal persons;
e) For trusts, the classes or categories of beneficiaries;
f) For legal persons your institution would need to determine its ownership, details of any groups the company or legal person is a part of and ownership of any such group;
g) Whether any trust or legal person is subject to supervision in any jurisdiction outside of SVG and who the supervisory authority is.

B. Identification Information- the following information is the best practices approach applied to initially identify a potential customer, it should be noted that this is not an exhaustive list:
   i. Full legal name, former names and any other names used by the individual;
   ii. Gender;
   iii. Principal residential address;
   iv. Date of birth;
   v. If the person is deemed to be high risk, the following additional information for identification should be sought:
      a) Place of birth;
      b) Nationality;
      c) Official government identity number or other government identifier.
   vi. Where the customer is a legal person the following identification information is necessary:
      a) Full name of the legal person and any trading name it uses;
      b) The date of incorporation, registration or formation;
      c) Any official identity number unique to the legal person;
      d) Address of the registered office or head office;
      e) Name and address of registered agent (if applicable);
      f) Mailing address (if different to registered address);
      g) Principal place of business;
      h) Names of the Directors;
      i) Identification information for all Directors who holds authority to instruct the institution concerning business relationships or occasional transactions;
      j) Identification information for all individuals who are ultimate holders of 15% or more of the legal person.

vii. Where the customer is a trust the following identification information is necessary:

a) The name of the trust;
b) The date of establishment of the trust;
c) Any official identifying number of the trust;
d) Identification information for each trustee of the trust;
e) The mailing address of the trustees;
f) Identification information on each settlor of the trust;
g) Identification information of each beneficiary or each category of beneficiary;
h) Identification information for each enforcer of protector of the trust;
i) Identification for any other natural person exercising ultimate control over the trust;
j) Confirmation from trustees that all information requested has bene provided and that updates will be provided in the event of any changes;
k) If the trust has more than one type of beneficiary (discretionary trust), your institution will need to gather information to enable identification of the beneficiary at the time of receipt or collection of any property under the trust;
l) If the trust is charitable, your institution will need to collect information in respect of the objects of the trust.

viii. Where the customer is a foundation the following identification information is necessary:

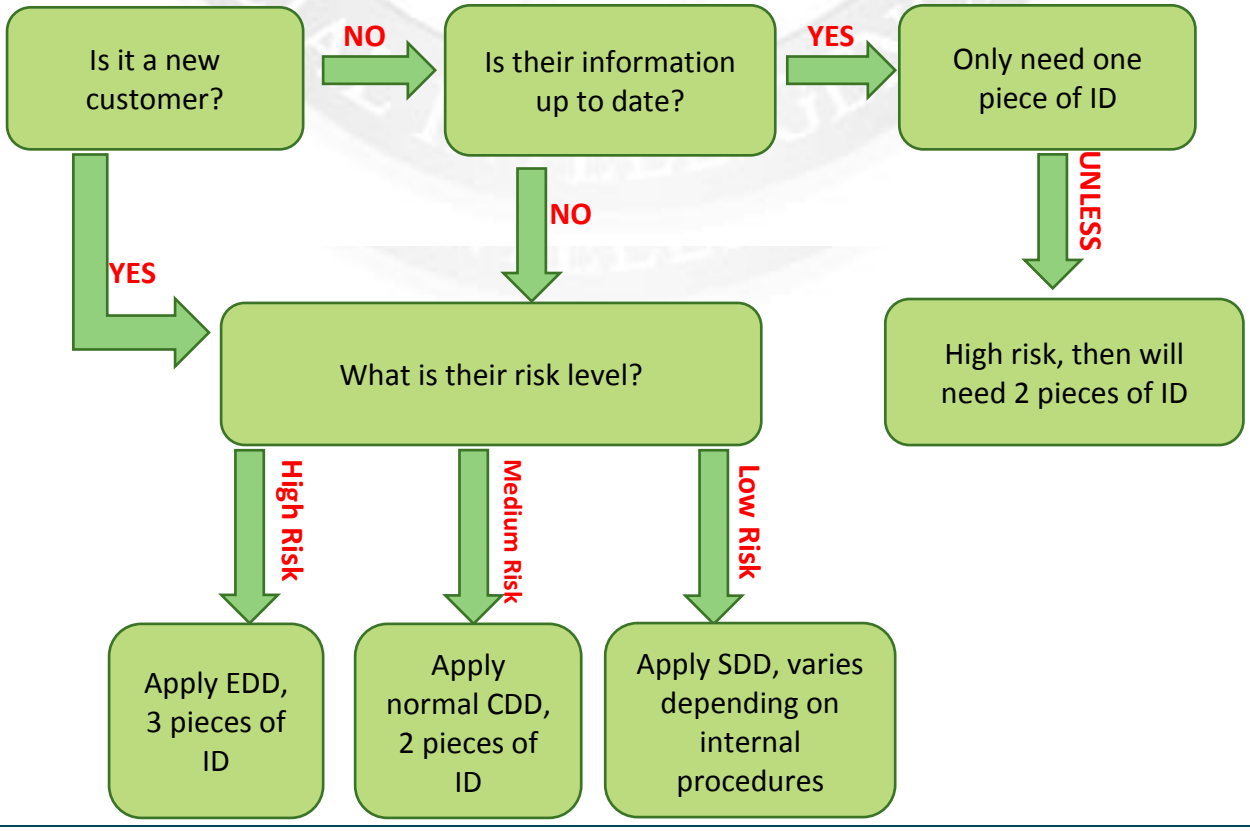
a) The full name of the foundation;
b) Date and country of establishment, registration, formation or incorporation;
c) Any official identifying number;
d) Registered address of head office address;
e) Mailing address if different from registered address;
f) Principal place of business if different from registered address;
g) Name and address of registered agent (if applicable);
h) Name and address of the secretary;
i) Name and identification information (as identified in A.i-vi above) of any foundation member who have authority to give instructions or decision-making powers;
j) Identification information (as identified in A.i-vi above) for any guardians of the foundation (if applicable);

k) Names and other identification information for all founders and Directors of the foundation;
l) Names and other identification information of the beneficiaries of the foundation if the foundation is deemed to be high risk;
m) Any further information deemed appropriate by the institution.

C. Verification Information- Institutions are required to verify the identity information collected that is mentioned in **subparagraphs B.i-vi** above. Verification is done by examining the information provided against a government issued source of identification document or an independent source of information. Verification will also vary depending on the risk posed by the customer. For the acceptable sources used for verification and the risk appropriate application please see **paragraphs 3,4 and 5** above.

7. **Virtual Identification & Covid-19 Implications on CDD**- due to the impacts of Covid-19 many financial institutions and other service providers have reduced opening hours and restricted in-person services that are offered, thereby increasing online banking and other activities. These activities have now been amplified to include customer on-boarding and identity verification remotely/virtually. Please see the document labelled **Digital CDD Guidance** document for information concerning new protocols.

8. **Application Chart**- below is a general application chart of how the different types of CDD are to be applied.



GUIDANCE

1. Anti-Money Laundering and Terrorist Financing Regulations No.20 of 2014 and No.25 of 2017 Amendment (the Regulations) - Regulations 12,16,17,18,19 (https://www.svgfiu.com/index.php/resources/law-regulations)

2. Anti-Money Laundering and Terrorist Financing Code No. 24 of 2017 (the Code)- paragraphs 4-21(pages 95-102, 105-146) (https://www.svgfiu.com/index.php/resources/law-regulations)

3. Anti-Terrorist Financing and Proliferation Act No.14 of 2015 and No.17 of 2017 Amendment (ATFPA)- sections 63-67 (https://www.svgfiu.com/index.php/resources/law-regulations)

4. AML/CFT Guidelines- pages 13-18 (https://www.svgfiu.com/index.php/nrsp-dnfbp/nrsp-guidance/guidelines)

5. AML/CFT Compliance Programme Structural Guidelines- Chapter 4 and 5 pages 5-9

6. Digital Customer Due Diligence (CDD) Guidance

7. Politically Exposed Persons (PEPs) Guidance

8. FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence (https://www.fatf-gafi.org/media/fatf/Updated-2017-FATF-2013-Guidance.pdf)

9. FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22) (https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf)

10. FATF Digital Identity Guidance (https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf)