Standard Commerce Bank, Ltd.[1]

Anti-Money Laundering & Counter Terrorism Compliance Procedures for Compliance Staff

25 Victoria Street (Corner of Bath Road)
Roseau, Commonwealth of Dominica

Implementation Date: May 2016

Version Number: 1.0

Last Updated: May 2016

Approved By: Alex Silver, Compliance Officer

[1] Standard Commerce Bank, Ltd. is referred to as "SCB" or the "Bank" within this document.

Table of Contents

1 Compliance Officer

This document provides procedural guidance for the anti-money laundering (AML) and counter terrorism financing (CTF) Compliance Officer (Compliance Officer) of SCB. Tasks described in this document may be delegated to other staff members who perform tasks on the Compliance Officer's behalf.

2 Staff

For the purposes of this document, references to staff or employees, includes Introducers[2], Affiliates[3] and any other third party companies that perform relevant functions, such as, client interactions, client identification or transaction related functions.

---

[2] **Introducers** are defined as an individual or more often a company which has a relationship with the offshore bank allowing to introduce new customers to that offshore bank. Such relationship between offshore introducer and offshore bank is normally made in written form and an introducer receives substantial amount of responsibility for selecting customers, providing proper due diligence, assisting with paperwork as well as for monitoring customers. *See:* Lexology Definition U.K. SCB has implemented policy to ensure that new clients will only be on-boarded , if referred by an existing client. All existing clients are associates of the directors of the Bank.

[3] **Affiliates** are defined pursuant to 12 USCS § 221a (b) [Title 12. Banks and Banking; Chapter 3. Federal Reserve System; Definitions, Organization, and General Provisions Affecting System], the term affiliate shall include "any corporation, business trust, association, or other similar organization--

(1) Of which a member bank, directly or indirectly, owns or controls either a majority of the voting shares or more than 50 per centum of the number of shares voted for the election of its directors, trustees, or other persons exercising similar functions at the preceding election, or controls in any manner the election of a majority of its directors, trustees, or other persons exercising similar functions; or

(2) Of which control is held, directly or indirectly, through stock ownership or in any other manner, by the shareholders of a member bank who own or control either a majority of the shares of such bank or more than 50 per centum of the number of shares voted for the election of directors of such bank at the preceding election, or by trustees for the benefit of the shareholders of any such bank; or

(3) Of which a majority of its directors, trustees, or other persons exercising similar functions are directors of any one member bank; or

(4) Which owns or controls, directly or indirectly, either a majority of the shares of capital stock of a member bank or more than 50 per centum of the number of shares voted for the election of directors of a member bank at the preceding election, or controls in any manner the election of a majority of the directors of a member bank, or for the benefit of whose shareholders or members all or substantially all the capital stock of a member bank is held by trustees."

3 AML/CTF Compliance Programme Updates

The Compliance Officer will update the AML/CTF Compliance Programme, according to the following schedule:

- Annually, in the second quarter of every calendar year;
- When there are changes to SCB's business model;
- Where there are changes to applicable Commonwealth of Dominic, AML/CTF legislation;
- Following an AML/CTF Compliance Effectiveness Review, which is required at least once, every two years, in order to address any deficiencies identified in the final report provided by the reviewer;
- Following regulatory reviews, in order to address any deficiencies identified in the final report provided by the regulator; or
- In the event of internal process or performance issues, that have been identified by SCB, as requiring remediation.

All programme updates will be logged and tracked by the Compliance Officer, or a delegate and all records related to AML/CTF compliance programme updates will be maintained for a minimum of seven (7) years.

The Compliance Officer, or a delegate, will communicate any relevant changes, to all staff, in a manner that ensures they are aware of the changes, are able to perform their roles effectively and have the ability to clarify any ambiguities with the Compliance Officer.

4 AML/CTF Compliance Training

The Compliance Officer, or a delegate, will ensure that all staff have received sufficient AML/CTF Compliance training, in order to be effective in their roles.[4] Minimum standards for training are set out in the AML/CTF Compliance Policy. In instances where staff are performing specialized roles, or where the Compliance Officer has observed issues or misunderstandings related to compliance tasks, additional training will be provided, at the Compliance Officer's discretion.

The Compliance Officer, or a delegate, will maintain records of all AML/CTF Compliance training sessions conducted, including training sessions outside of new hire and annual employee training, for a minimum of seven (7) years. The information to be recorded and maintained is detailed in the AML/CTF Compliance Policy document, in the AML/CTF Compliance Training section. The Compliance Officer, or a delegate, will also maintain records of all external training sessions attended by the Compliance Officer and/or delegates, for the purpose of maintaining up to date knowledge of AML/CTF legislation and best practices.

[4] 2013 Money Laundering (Prevention) S.R.O. No. 4 Part II Section 6.

5 AML/CTF Compliance Effectiveness Reviews

The Compliance Officer will ensure that an AML/CTF Compliance Effectiveness Review is conducted, at least once, every two years. The final report, resulting from the review, must be signed-off by Senior Management within thirty (30) days of the date it is issued. The minimum standards for what elements must be considered when an AML Compliance Effectiveness Review is conducted, are defined in the AML/CTF Compliance Policy.

In addition to ensuring that these standards are met, the Compliance Officer will certify that any reviewers contracted are sufficiently qualified, by requesting a copy of their curriculum vitae (CV), prior to engaging with the reviewer.

In order for a reviewer to be considered sufficiently qualified, they must:

- Demonstrate sufficient understanding of the Commonwealth of Dominica regulatory landscape;
- Have sufficient experience in conducting AML/CTF Compliance Effectiveness Reviews in the Commonwealth of Dominica or CFATF jurisdictions.; and
- Have maintained professional qualifications/designations and received up to date training; including, but not limited to, the Certified Anti-Money Laundering Specialist (CAMS) or Certified Fraud Examiner (CFE) designations.

Records, related to any AML/CTF Compliance Effectiveness Reviews conducted, will be maintained by the Compliance Officer, which include:

- A copy of the final report;
- A record of Senior Management's sign-off on the final report within 30 days of the date it was issued;
- A copy of the agreement between SCB and the reviewer;
- Copies of the CVs for all reviewers to ensure that each reviewer is sufficiently qualified to perform the review; and
- A record of any updates made to SCB's AML/CTF Compliance Programme to address any deficiencies identified by the reviewer in the final report[5].

The Compliance Officer will ensure that all records relating to AML/CTF Compliance Effectiveness Reviews are maintained for a minimum of seven (7) years.

6 Financial Supervision Unit (FSU) Communication

SCB holds a banking license issued by the Ministry of Finance of the Commonwealth of Dominica and is regulated by the Commonwealth's FSU. The Compliance Officer, or a delegate, will maintain SCB's Banking License in good standing with the FSU by:

[5] A sample of the log to be maintained related to AML/CTF compliance programme updates is included in Appendix 2 of this document.

- Maintaining current registration information;
- Responding to requests for, or to clarify, information, in the prescribed form and manner, within 30 days of the request; and
- Advising the FSU if the Bank stops offering banking services to the public, within 30 days of the cessation.

In all cases, the Compliance Officer, or a delegate, will act as the liaison with the FSU. Records of all FSU communication, including SCB's responses, will be maintained for a minimum of seven (7) years.

Specific to AML/CTF, the Financial Intelligence Unit (FIU) may communicate with the Bank regarding examinations, compliance assessment reports, or other information requests. In all cases, the Compliance Officer, or a delegate, will act as the liaison with FIU. Records of all FIU communication, including SCB's responses, will be maintained for a minimum of seven (7) years.

The Compliance Officer will ensure that records that may be requested by either the FSU or FIU, are stored in a manner that they can be retrieved, and communicated to the Bank's regulator, in a timely manner. Generally, the allotted response time will be 30 days, from the date that a request is sent, to assemble and submit the information that is requested. When SCB receives a confirmation from a regulator that information has been received, this confirmation will be maintained as part of SCB's records of correspondence with the Commonwealth of Dominica's regulatory authorities.

7 Reporting[6]

Certain types of transactions must be reported to the FIU. Reporting to the FIU should always be completed by the Compliance Officer, or a delegate, who must be a person that has been specifically trained to submit reports in the Compliance Officer's absence. All other employees should use the internal forms included in this programme to submit reports to the Compliance Officer. All reports have specific timelines in which they must be submitted to the FIU. All internal reports should be submitted to the Compliance Officer, or a delegate, on the same day that the activity takes place. The reason for this is to ensure there is sufficient time to complete the reporting, as well as any prerequisite processes, such as investigations, that must be conducted.

Reportable transactions are detected by:

- SCB's electronic IT systems; and
- SCB's employees.

[6] The FSU is the authority regulating the SCB's compliance programme, the FIU is the "Unit" to whom the Bank submits all AML/CTR required reporting. FSU - http://fsu.gov.dm/ and FIU - http://fiu.gov.dm/

Reports may be submitted to the FIU either via courier or electronically, using Dominica's new E-Filing System. In all reports where a field is labelled as 'optional', and SCB possesses the information being requested, these fields will be considered mandatory.

7.1 No Currency Transactions

SCB does not, under any circumstances, accept currency (cash) transactions. Should SCB's business model contemplate accepting currency transactions, the Compliance Officer will implement appropriate control processes, including the filing of Currency Reports (CRs).

7.2 Suspicious Transaction Reporting

Suspicious Activity Reports (STRs) are submitted to the FIU when there is 'reasonable grounds' to suspect that an activity is related to money laundering or terrorist financing. STRs must be submitted whether or not the transaction or activity is completed (it does not depend on whether the transaction is declined by the company or cancelled by the client). These reports must be submitted to the FIU within five (5) days of the date that the Compliance Officer deems the transaction/activity, or attempted transaction/activity, to be suspicious.

Employees should report any instances of suspicious transaction/activity to the Compliance Officer, using the Unusual Transaction Form (Internal), which must be submitted on the same day that the transaction/activity takes place.

The Compliance Officer, or a delegate, will emphasize the importance of the following to all staff, in order to provide comfort and understanding related to the limitations and legal requirements of escalating transactions/activities they feel are unusual, specifically:

- Not to letting the client know that they are suspicious. It is against the law to deliberately "tip off" a client about a potential investigation. All staff are, however, protected under the Commonwealth of Dominica law from any action when they submit a report "in good faith." In most cases, even if a case goes to court, the subject of the report will not know that this report has been filed, and more importantly, by whom; and
- When striving to identify clients that conduct or attempt suspicious activity/transactions, the client may ask why the Bank needs their identification information. In such cases, the simplest route is to let the client know that it is SCB's policy to collect this information. If this information is not used for additional marketing activities, let the client know that as well (often clients are more concerned about privacy and security issues, and reassuring them may be helpful).

The Compliance Officer, or a delegate, will maintain records of:

- All STRs filed with the FIU;

- All internal Unusual Transaction Forms, including those submitted for transactions/activities that were not reported to the FIU;
- All technology-based transaction monitoring alerts related to unusual transactions/activity;
- A record of the reason that transactions/activities escalated (via staff or via the technology-based transaction monitoring systems), which the Compliance Officer did not report to FIU, including the analysis conducted to form the basis for each decision; and
- Records of any follow-up activity, including, but not limited to, any additional information requested, updates to Client Risk Rating, enhanced transaction monitoring and/or the closing of client accounts.

The records mentioned above are currently maintained in either paper or electronic format (including scanning), which include the original transaction/activity information and the Compliance Officer's decisions related to whether or not a report was submitted to FIU.

All records relating to STRs will be maintained for a minimum of seven (7) years.

1.1. Restrictions on Conducting Banking—Sanctioned Entities and Individuals

Using a risk-based approach, SCB has a responsibility to reasonably ensure the Bank will not knowingly conduct business with the following:

- Individuals or entities subject to the Commonwealth of Dominica, regional or international sanctions;
- Terrorists or terrorist organisations;
- Anonymous Relationships;
- Shell Banks; and
- Holder of Bearer Shares.

Moreover, SCB at the time of establishing a business relationship[7] with a customer, must conduct verification to determine whether or not the potential customer is a Politically Exposed Person (PEP).

Pursuant to Dominica's statutory rules and orders, this has been defined to mean in pertinent part:

[7] For the purpose of this programme and its accompanying Risk Assessment, and procedural documentation, the term "customer" is considered to include "business relationships", unless otherwise specified. A business relationship is defined as "…formed by a person acting in the course of relevant financial business where that person has obtained, by procedures maintained by him in accordance with regulation 5, satisfactory evidence of the identity of the person who, in relation to the formation of that business relationship, was the applicant for business." 2013 Money Laundering (Prevention) S.R.O. No. 4 Part I Section 2.

> …any individual who is or has been entrusted with prominent public functions in Dominica or in any country or territory, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials including family members or close associates of the politically exposed person.[8]

If so, enhanced due diligence will need to be conducted as PEPs are considered high-risk customers. Unlike a match to a terrorist list, a PEP may be approved and may become a customer; however, they will be flagged and treated as higher risk and monitored accordingly.

Additionally, SCB must freeze any funds or other assets held for individuals or organisations listed on the UN list of persons connected to terrorism in line with the United Nations Resolutions on terrorist financing, and communicate with the Financial Intelligence Unit (FIU).

This information should be escalated to the Compliance Officer immediately. The contents of these referrals or reports (or the fact that you are filing a report) should not be disclosed to the customer. These reports are submitted as soon as possible by the Compliance Officer to the FIU.

8 Client Account Opening Process: Organisations

8.1 Organisation Process: Confirming Existence

The Commonwealth of Dominica's compliance regulations, require SCB to collect an "identification record" containing certain information about the Bank's clients, and in some circumstances, verify specific pieces of the information provided. When conducting typical Customer Information Programme (CIP) and Customer Due Diligence (CDD) during the account opening process, the Bank is required to confirm the following information about the organisation or entity applying, specifically:

- That they exist;
- That they have a physical location; and
- Who they 'Key Person(s)' are.

The typical process that is followed for confirming the client's details, is to obtain proof by requesting the documents from the appropriate list below. The type of document that the Bank requires, will depend on the type of organisation being confirmed. Any discrepancies between the original information provided and the additional documentation collected, must be clarified, and deemed acceptable by the Compliance Department.

[8] 2013 Money Laundering (Prevention) S.R.O. No. 4.

8.1.1 Incorporated Company

- Form W-9 or W-8 Series (as appropriate[9]); and:
- Articles of Incorporation[10]; or
- Certificate of Incorporation[11]; and
- Most recent annual return registration (except in respect of International Business Companies)[12], and
- Documentary evidence regarding an officer of the corporation proving "that the person is who the person claims to be[13]," and one of the following:
    - If Non-U.S.:
        - Confirmation of the organisation's 'Active' status from the country's regulatory authority;
        - Foreign EIN certification from the country's tax authority; or
        - Business Permit/License from an issuing authority; or
        - Sales Tax Certificate from the country's tax authority.
    - If U.S.:
        - Confirmation of the organisation's 'Active' status from a Secretary of State; or
        - EIN certification from the IRS; or
        - Business Permit/License from an issuing authority (City, County or State); or
        - Sales Tax Certificate from the IRS.

8.1.2 Partnership

- Form W-9 or W-8 Series (as appropriate); and
- Partnership Agreement; and one of the following:
    - If Non-U.S.:
        - Certificate of Existence from the country's regulatory authority;
        - Foreign EIN certification from the country's tax authority; or
        - Business Permit/License from an issuing authority; or
        - Sales Tax Certificate from the country's tax authority.
    - If U.S.:
        - Certificate of Existence from a Secretary of State; or
        - EIN certification from the IRS; or
        - Business Permit/License from an issuing authority (City, County or State); or
        - Sales Tax Certificate from the IRS.

---

[9] Providing tax advice to clients is not permitted or advised.

[10] To be notarized where the corporate body is incorporated outside Dominica.
2013 Money Laundering (Prevention) S.R.O. 4 Part 1.2.

[11] Id.

[12] Id.

[13] 2013 Money Laundering (Prevention) S.R.O. 4 Part 1.2.

8.1.3 Limited Liability Company (LLC) or Limited (Ltd.)

- Form W-9 or W-8 Series (as appropriate); and:
- Articles of Organisation; and one of the following:
    - If Non-U.S.:
        - Confirmation of the organisation's 'Active' status from the country's regulatory authority;
        - Foreign EIN certification from the country's tax authority; or
        - Business Permit/License from an issuing authority; or
        - Sales Tax Certificate from the country's tax authority.
    - If U.S.:
        - Confirmation of the organisation's 'Active' status from a Secretary of State; or
        - EIN certification from the IRS; or
        - Business Permit/License from an issuing authority (City, County or State); or
        - Sales Tax Certificate from the IRS.

8.1.4 Cooperative

- Form W-9 or W-8 Series (as appropriate); and:
- Articles of Incorporation; or
- Confirmation of the organisation's 'Active' status from an appropriate regulatory authority; and
- EIN certification from the competent tax authority; or
- Business Permit/License from an issuing authority; or
- Sales Tax Certificate from the country's tax authority.

8.1.5 Not-For-Profit/Charity

- Form W-9 or W-8 Series (as appropriate); and:
- Articles of Association; or
- Certificate of Existence from an appropriate regulatory authority; or
- Certification of Tax Exempt status; or
- Confirmation of official Charity Registration from the competent tax authority, if they solicit donations from the public.

8.1.6 Trust

- Form W-9 or W-8 Series (as appropriate); and:
- Trust Charter/Agreement, which sets out the Trustee, Beneficiary and any other related parties; or
- Trust Ledger, which sets out the Trustee, Beneficiary and any other related parties.

8.1.7 Informal Organisation

- Form W-9 or W-8 Series (as appropriate); and:
- Board resolutions; or
- Meeting minutes; or
- Official attestation from the organisation's leadership.

8.2 Organisation Process: Confirming Physical Address

All address provided by a client, must be a physical address (not a P.O. Box or general delivery address). SCB must obtain a proof of address document. The documents required for the confirmation listed below, are all acceptable, regardless of the type of organisation being confirmed. This may be any **one** of the following items, and the document must be in the organisation's name (not in the name of an individual):

- Any of the documents used to confirm the organisation's existence (where the address is included in the document);
- A utility bill from a recognized provider;
- A bank statement or communication from a recognized bank;
- A tax document, notice or communication from a competent tax authority;
- A statement or communication from a recognized insurance company; or
- Correspondence from a government organisation (federal, state or municipal.

In most cases, the Bank will be able to confirm the client's physical address using the same document that was used to confirm that they exist. If the organisation has recently moved and/or the address in the document collected does not match the address on the corporate application, additional clarification will be required.

8.3 Organisation Manual Process: Confirming Key Persons

A Key Person is typically referred to as any physical person who has ownership or significant control over an organisation. When collecting the details for an organisation's Key Person(s) there are a few different types of individuals that qualify, such as:

- Beneficial Owners;
- Directors; and
- Authorized Representatives.

During the application process, the client provides information about their Key Person(s). SCB does not need to identify all Key Persons, but the Bank is required to identify the person submitting the application on behalf of the organisation. SCB will request an identification document and a proof of address document for the identified Key Person(s) of the organisation.

Documentation that are considered acceptable for this purpose by SCB are as follows:

- A copy of a piece of government issued photo identification (such as a passport or driver's license) that is valid (not expired); and
- A proof of address document (such as a utility bill, communication from a recognized bank or insurance company, communication a competent federal tax authority, or voter registration).

8.4 Beneficial Owners

In addition, we must confirm the beneficial owners of the organisation. Beneficial owners are any individual(s) that own or control 25% or more of the organisation, either directly or indirectly[14]. Who is a beneficial owner will vary, depending on the type of organisation.

Organisation Type	Beneficial Owner
Incorporated Company	Each individual with 25% or more of the total vote or value of the organisation.
Partnership	Each individual with 25% or more of the total vote or value of the organisation.
Limited Liability Company (LLC)	Each individual with 25% or more of the total vote or value of the organisation.
Cooperative	Each individual with 25% or more of the total vote or value of the organisation.
Not-For-Profit/Charity	Board of Directors.
Trust	Trustee and all trust beneficiaries.
Informal Organisation	Each individual with 25% or more of the total vote or value of the organisation.

Currently, beneficial owners are confirmed via the information contained in the account agreement, which is signed by the client. It is expected that SCB will be asked to take additional steps to confirm beneficial ownership via documentation in the near future. As with other information about organisations, the Bank will first attempt to confirm the organisation's beneficial ownership electronically. Where additional documentation is required, SCB anticipates that the following documents will be suitable for this purpose:

8.4.1 Incorporated Company:

- Articles of Incorporation and/or Amendment (where shareholders are listed); or
- Shareholder registry.

8.4.2 Partnership:

- Partnership Agreement and/or Amendment (where partners are listed); or
- Partner registry.

8.4.3 Limited Liability Entity (LLC or Ltd):

- Articles of Organisation and/or Amendment (where members are listed); or
- Member registry.

[14] Examples clarifying direct and indirect beneficial ownership are provided at the end of this section. If further clarification is required, please contact the Compliance Officer.

8.4.4 Cooperative:

- Articles of Incorporation and/or Amendment (where shareholders are listed); or
- Shareholder registry.

8.4.5 Not-For Profit/Charity:

- Articles of Association and/or Amendment; or
- Ratified meeting minutes listing all directors.

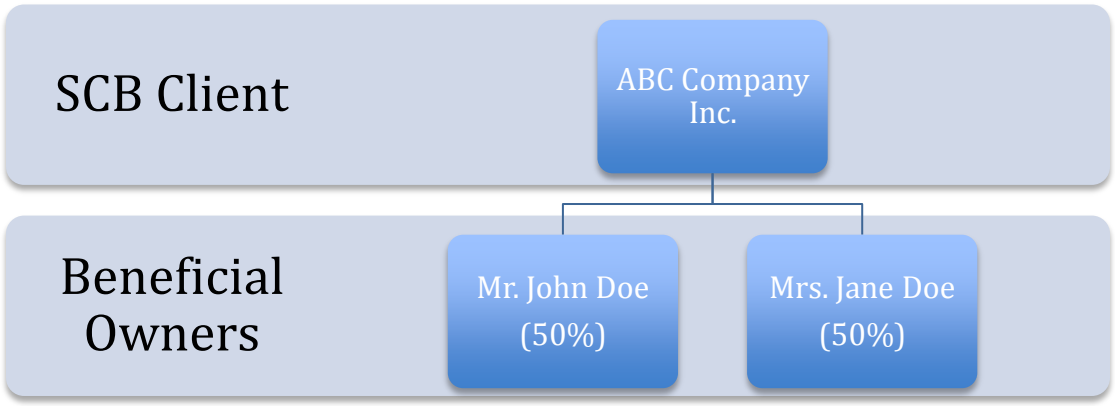
8.4.6 Trust:

- Trust Charter; or
- Trust Ledger.

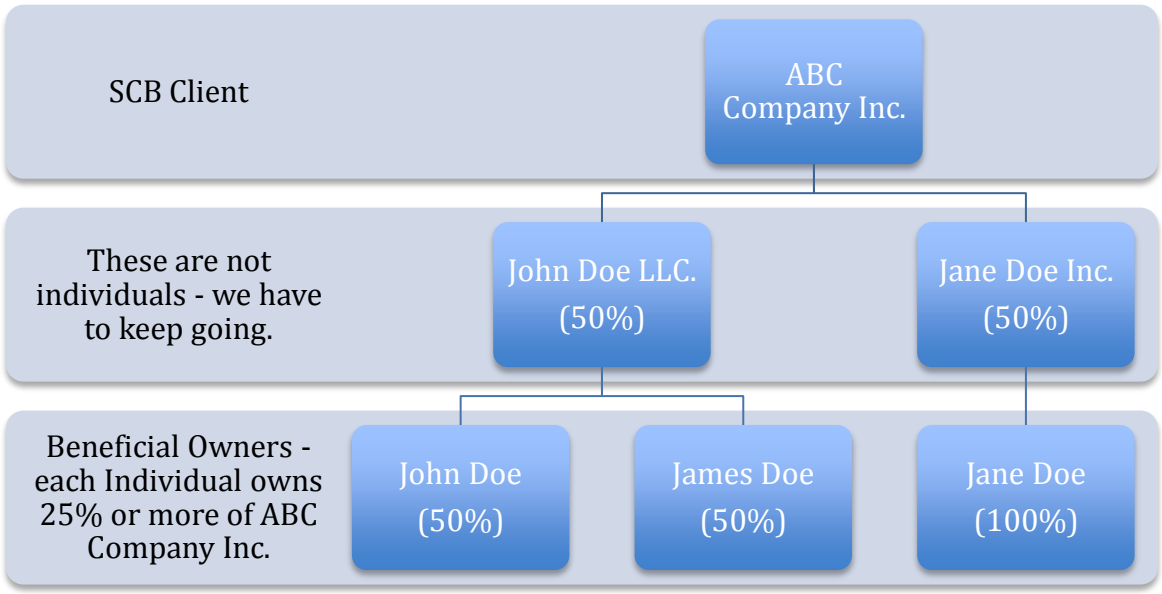
8.4.7 Informal Organisation

- Ratified meeting minutes listing all controlling persons; or
- Signed attestation.

8.4.8 Direct Beneficial Ownership Example



8.4.9 Indirect Beneficial Ownership Example



9 Client Account Opening Process: Individuals

9.1 Individual Process: Confirming Identity

The Commonwealth of Dominica compliance regulations, require SCB to collect and record certain information about the Bank's clients, and in some circumstances, verify specific pieces of the information provided. When conducting typical Customer Information Programme (CIP) and Customer Due Diligence (CDD) during the account opening process, we are required to confirm the following information about the individual applying, specifically:

- That they exist;

- That they are who they say they are; and
- That they have a physical location.

SCB must obtain a proof by requesting an additional document that confirms the information in question. Any discrepancies between the original information provided by the client and the additional documentation collected, must be clarified, and deemed acceptable by the Compliance Department.

Documentation that is considered acceptable by SCB, for the purpose of confirming an individual's identification, includes:

- A copy of a piece of government issued photo identification (such as a passport or driver's license) that is valid (not expired); and

Documentation that is considered acceptable by SCB, for the purpose of confirming an individual's physical location, includes:

- A utility bill in the client's name;
- Communication from a recognized bank or insurance company;
- Communication from a competent tax authority; or
- Voter registration.

10 Clients That Cannot Be Identified

If a client is not able, or willing, to be identified, SCB cannot open an account for them. In these cases, the Bank must let the client know that it is against the law in the Dominica to complete certain transactions without identification, and that SCB's internal policy requires complete client identification prior to account opening. This internal policy is meant to help ensure compliance with the Commonwealth Dominica's legislative obligations, as well as protect the Bank's clients and SCB's business.

Some clients may be hesitant to provide their identification for legitimate reasons. Remember, if you are obtaining client identification because you suspect that the client's activities are related to money laundering or terrorist financing, the Bank cannot tell the client about any suspicion. Instead, let the client know that it is the Bank's policy to ask for identification for all clients. Since most objections will be related to privacy or marketing concerns, and not AML or CTF, let the client know that the information will not be used for marketing purposes, if they do not wish to receive marketing messages from the Bank[15].

[15]If the client indicates that they do not wish to receive marketing messages, this should be noted and passed on to the Privacy Officer, in order to be certain that the client is not included in any present or future SCB related marketing lists.

The Bank divides our clients into High, Medium and Low risk rating, which is initially based on the client's information collected/provided, and then updated going forward, according to their transactions and activities. The parameters for Client Risk Rating are described in SCB Risk Assessment document.

10.1 Client Risk Rating Procedure

Client Risk Rating is currently conducted at account opening by the Compliance Department to collect the additional documentation required. All clients and assigned a rating of high, medium or low.

Where a client is deemed to be high risk, enhanced due diligence and enhanced transaction monitoring are performed by the Compliance Officer or a delegate.

11 Client Information Updates

For all active clients (clients that have conducted a transaction within the past year), the information originally collected for CDD, KYC and CIP purposes, is updated on a regular schedule, based on Client Risk Rating and/or triggering events.

11.1 Information Updates

The client information that is to be updated, refers to their:

- Name;
- Address;
- Email address;
- Telephone number; and
- Occupation or principal business.

Clients that are organisations are also required to confirm the organisation's beneficial ownership and director information, and provide any additional information, where changes to the organisation have occurred.

11.2 Inactive Status

Inactive clients (any client that has not completed a transaction within the past year) are required to update their client information in order to return to active status and complete any transactions.

11.3 Low and Medium Risk Clients

Low risk clients are required to update their client information every three (3) years, or at the point that the identification document on file has expired. Where, Medium risk clients are required to update their client information every two (2) years, or at the point that the identification document on file has expired. This ensures that in the case where there is no expiry date for the identification document initially provided, the client information is still updated within a reasonable timeframe.

11.4 High-Risk Clients

High-risk clients are required to update their client information annually, or when the identification document on file becomes expired, if less than two years.

If the reason that a client has been considered High-risk relates to doubts about the veracity of any of the CDD, KYC or CIP information originally provided to SCB, additional documentation or confirmation of the client's identity may be required, at the Compliance Officer's discretion.

12 Transaction Monitoring

Transactions are monitored for activities that indicate suspicious activity may be taking place. Where an alert is generated, either through our IT system or via staff, the Compliance Officer, or a delegate, will conduct an investigation and document the results. These records will be maintained for a minimum of seven (7) years, regardless of whether or not an STR is submitted to the FIU.

Transaction monitoring is currently conducted by SCB's staff members that are responsible for quality assurance (QA), who input transaction details. Any concerns related to a client's activities are escalated to the Compliance Officer, or a delegate, for investigation via the Unusual Transaction Form. The same form is used to document the Compliance Officer, or a delegate's, investigations and the decision of whether or not a report is filed with FIU.

Transaction monitoring alerts are resolved by the Compliance Officer, or a delegate, on a daily basis. Where there is insufficient information present to determine whether or not a transaction/activity is suspicious, additional investigations are conducted and/or additional information may be requested, at the Compliance Officer's request. These may include follow-up with SCB's clients via phone, email or social media. All investigations are logged electronically and are maintained by the Compliance Officer and detailed notes are used to ensure that all process steps are clear. Notes on the investigation results are completed for each alert, whether or not the transaction/activity is deemed to be suspicious, triggering STR reporting requirements.

Where alerts, related to transactions/activities, are deemed to be suspicious, the Compliance Officer, or a delegate, must file a report with the FIU within 5 days of the determination. Adjustments will also be made to the Client's risk rating, where required (if the client has not already been designated as a High-risk client).

In some cases, the transaction may be suspended while SCB contacts the client to obtain additional information, in order to make a determination of whether the transaction/activity is, in fact, suspicious. Where the transaction is considered to be outside of SCB's risk tolerance (as defined by the Compliance Officer) and mitigating documents or information cannot be obtained or do not sufficiently mitigate the risk, the transaction may be rejected by SCB.

13 Enhanced Due Diligence and Enhanced Transaction Monitoring

In relation to our High-risk clients, the Compliance Officer, or a delegate, will conduct a full review of the client's activities and information on file. Where there is activity that is deemed to be inconsistent with the information on file about the client, SCB may request additional information.

Internet-based searches are also performed at the time that Enhanced Due Diligence is conducted. Specifically, the Compliance Officer, or a delegate, will make note of any findings related to:

- Money laundering or terrorist financing;
- Financial crime (such as, fraud or tax evasion) or serious/violent crime;
- Any negative news results or potential List Screening matches;
- Discrepancies between publicly available information and information listed in the client's profile; and/or
- Any other information that could affect the Client's Risk Rating

The enhanced due diligence (EDD) activities conducted will be logged by the Compliance Officer, and reflect the reason that the customer is considered to be high risk. The following are example of enhanced due diligence activities that may be conducted, however, the Compliance Officer may conduct other or different activities, at their discretion.

Risk Factor	EDD Activity
The documentation submitted appears to be false, contradictory or altered.	Additional documentation that resolves the conflict, including but not limited to clear copies of documents (where the integrity of a document is in question) certified true copies or notarized copies of documents, and attestations to the veracity of documents by reliable third parties.
The client high-risk organisation that is regulated under the FSU, such as: • Banks; • Financial services companies, including credit unions and financial advisors or planners; • Venture risk capital companies; • Money transmission services; • Money lending and pawning; • Mutual Funds; • Trust businesses; • Insurance businesses;	A copy of the organisation's external compliance review and/or regulatory examination results.

Risk Factor	EDD Activity
• Investment bankers; • Real estate brokers or agents; • Dealers in precious metals, stones, or jewels; and • Registered agents.	
The client is a high risk organisation that is not regulated under the FSU, such as: • Immigration consultants; • Lawyers; and • Accountants.	A copy of the client's professional certification or industry association membership.
Cash Intensive businesses, such as: • Restaurants; • Convenience Stores; • Privately owned Automated Teller Machines (ATMs); • Vending machine operators; and • Privately owned parking garages.	A copy of the organisation's most recent financial statement and/or tax filing.
Organisations dealing with high value goods, such as: • Planes; • Boats; and • Vehicles[16].	A copy of the organisation's business plan or business model.
Organisations with no retail or commercial locations in the U.S., such as: • Online retailers; and • Computer software providers.	A copy of the organisation's most recent financial statement and/or tax filing.
The client is a charity that deals with high-risk jurisdictions.	Additional information about the organisation's charitable initiatives and the controls in place to ensure that funds are not being used to fund terrorism or terrorist groups.
The client has been associated with money laundering or terrorist financing related activities due to lax controls and/or negligence.	Information about the remedial controls in place to ensure that the organisation is not being used to facilitate money laundering or terrorist financing activities.

[16] Car dealerships are regulated by the FSU and are subject to the 2011 Money Laundering (Prevention) Act. No. 8 and all subsequent amendments.

SCB may request additional clarification, documentation or information from a client, where there are discrepancies between the client profile and publicly available information, or where the original high-risk factors have not been sufficiently mitigated. All follow-up activities must be recorded, including the client's response for additional information and the Compliance Officer's determination. All related records are maintained for a minimum of seven (7) years.

14 Co-Contracting Parties

Co-contracting parties are any individual, or organisations, with whom the Bank has entered into binding legal agreements - including Introducers and Affiliates. SCB is required to identify all co-contracting parties in the same way that the bank identifies clients. Introducer and Affiliate identification is completed at the point that they enter into a contractual agreement with SCB.

15 Record Keeping

SCB must maintain specific records in order to meet the Commonwealth of Dominica's legislative obligations related to record keeping. These records will be maintained electronically[17] in our IT systems. The Compliance Officer will ensure that SCB's records retention policies and processes are sufficient, in regards to:

- Maintaining the appropriate official records required under the Commonwealth of Dominica's AML/CTF enactments and other applicable Dominican legislation, for at least seven (7) years; and
- Storing all official records in a form and manner that allows them to be retrieved in a timely fashion, which is generally perceived as 30 days.

The SCB AML/CTF Compliance Policy includes a listing of all official records that must be maintained.

[17] All required records will be scanned and readily retrievable.

16 Appendix 1: Compliance Officer Tracking Sheet

This chart has been developed to assist the Compliance Officer in meeting time sensitive requirements. It is not intended to be a full listing of all AML/CTF Compliance Programme responsibilities.

16.1 AML/CTF Compliance Programme Maintenance

The AML/CTF Compliance Programme must be updated at regular intervals. This chart can be used to help the Compliance Officer, or a delegate, keep track of upcoming deadlines.

What?	When?	Last Completed	Next Due Date
SCB Anti-Money Laundering & Counter Terrorism Policy	Annual	May, 2016	May, 2017
SCB Anti-Money Laundering & Counter Terrorism Procedures for Compliance Staff	Annual	May, 2016	May, 2017
SCB Anti-Money Laundering & Counter Terrorism Procedures for All Staff	Annual	May, 2016	May2017
SCB Anti-Money Laundering & Counter Terrorism Risk Assessment	Annual	May, 2016	May, 2017
Anti-Money Laundering and Counter Terrorism Compliance Training Programme	Annual	May, 2016[18]	May, 2017
AML/CTF Compliance Effectiveness Review	Every Two Years		
Senior Management Sign Off on AML/CTF Compliance Effectiveness Review Final Report	Within thirty (30) days of the review's issue		Thirty (30) days after the completion of the next review

[18] Currently, SCB will rely on their Procedural Documents for Training Purposes.

16.2 Training

The Compliance Officer, or a delegate, must keep a log of all AML/CTF Compliance training (including training sessions attended by the Compliance Officer or compliance staff, to keep their knowledge sharp). This format is used to keep track of the AML/CTF Compliance training that took place within the Bank. The content section should include how the training was delivered and what topics were covered. This can be a brief, bullet point summary.

The category section should include the type of training (annual staff training, new hire training, compliance staff training, etc.) that was provided or attended.

These records may be shared with reviewers, financial service partners or SCB's regulators. They must be kept up to date at all times and go back at least seven (7) years.

Content	Date	Persons Trained	Category
Delivered via (delivery method) by (person): What is money laundering? What is terrorist financing? Who is the FSU? Who is the FIU? What is an offshore bank? What are our responsibilities under the Commonwealth of Dominica law? Compliance Officer AML/CTF Compliance Programme Risk Assessment AML/CTF Compliance Effectiveness Review Training Reporting Recordkeeping Client Identification Programme (CIP), Client Due Diligence (CDD) and Know Your Client (KYC) Client Risk Rating Transaction Monitoring (both regular and enhanced) Who is our Compliance Officer? What do I do if I believe that money laundering or terrorist financing is taking place? What indicators should I look for in our client's transactions and activities?			Annual Staff Training

16.3 Reporting

The reports that are sent to the FIU, as well as any other government agencies, must be submitted within certain timeframes, which are provided in the chart below. The STR may be submitted to the FIU via their new E-Filing System[19]. [20]

Report Type	Timing	Reported To
Suspicious Activity Report (STR)	Initial STR filing within 5 calendar days.	FIU
Currency Report (CR)	Initial CR filing must be completed at the point that currency and/or negotiable instruments valued in excess of $10,000 enter and/or leave Dominica	FIU

If reports are submitted to the FIU via the Dominica E-Filing System, screen prints should be taken although the Bank will receive an electronic confirmation that the report has been received and the Bank must maintain a copy for SCB's records.

[19] www.fiu.gov.dm

[20] Best practice given that the system is new.

17 Appendix 2: Sample Compliance Remediation Log

This sample log format can be used to track the remediation of any AML/CTF Compliance related issues. Issues are generally discovered in three ways:

1) Self-discovery;
2) AML/CTF Compliance Effectiveness Review; or
3) Regulatory Audit.

The issues that pose the greatest risk to the Bank will be considered the highest priority for remediation. Any issues that form part of a formal findings letter from a regulator, will also be considered the highest priority.

The official log is maintained by the Compliance Officer, or a delegate, and can be used to provide updates to Senior Management and the Board of Directors.

What is the Issue?	How was it discovered?	What are we doing to fix it?	Priority	When will it be fixed?	Completed and Signed Off By

The content in this log may be in point form, but should be detailed enough that the issue and the steps taken to resolve it, are clear to someone that was not involved in the remediation process, such as a regulator. The cause and source of discovery related to the issue should be included in the description, when they are known.