Standard Commerce Bank, Ltd.[1]

Anti-Money Laundering & Counter Terrorism Compliance Procedures for All 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.

1 Table of Contents

2 SCB Staff

For the purposes of this document, references to staff and 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.

All procedures listed in this document are mandatory. In addition to reading this document, all employees (including Introducers and Affiliates) are required to complete Anti-Money Laundering (AML) Compliance training, at least, annually.

---

[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 introduced/referred by an existing client.

[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 Staff Procedure

SCB holds a banking license issued by the Ministry of Finance of the Commonwealth of Dominica and is regulated by the Commonwealth's Financial Supervision Unit. As such, SCB is required under Dominica's statutory authorities to develop and maintain an AML/CTF Compliance Program. The following procedure document, should be read in conjunction with SCB's AML/CTF Compliance Policy and Risk Assessment. Additional procedures, specific to compliance staff, are documented in a separate procedure document.

This procedure has been specifically designed to assist SCB's staff and Introducers/Affiliates who deal directly with the Bank's clients and/or transactions. SCB is required to verify, collect, and record information about the Bank's clients and their transactions. Violations of this procedure can have severe negative consequences for SCB, and potentially the employee, Introducer or Affiliate, depending on the violation. Any questions or concerns about this procedure can be directed to the Compliance Officer.

4 Money Laundering and Terrorist Financing

Money laundering[4] is the process of taking money obtained by committing a crime and disguising the source to make it appear legitimate. Specifically, under the Commonwealth of Dominica's 2011 Money Laundering (Prevention) Act, a person who engages in such a behaviour that "disposes of, brings into or takes out of Dominica" has committed an offence in violation of the Act.[5]

it is illegal to launder money or to knowingly assist in laundering money.[6] SCB must take steps to be sure that the Bank's business is not used to launder money and if the Bank suspects that money laundering may be taking place, SCB must report it.[7]

---

[4] FATF (2012), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, updated October 2015, FATF, Paris, France, www.fatf-gafi.org/recommendations.html

[5] "Money laundering" denotes conduct which constitutes an offence under section 3(1);

"(1) A person who -

> (a) receives, possesses, manages or invests; (b) conceals or disguises;
> (c) converts or transfers; (d) disposes of, brings into or takes out of Dominica; or (e) engages in a transaction which involves, property that is the proceeds of crime, knowing or believing the property to be the proceeds of crime commits an offence. As amended by the Commonwealth of Dominica's 2013 Money Laundering (Prevention) Act 5." *See also*: 2013 Money Laundering (Prevention) S.R.O. 4 Commonwealth of Dominica.

[6] Dominica Risk & Compliance Report December 2014 pg. 7.

Terrorist financing[8] is the process of moving funds in order to pay for terrorist activities. Unlike money laundering, the source of the funds is not always criminal but the intended use of the funds is criminal. Under the statutory authority of the Commonwealth of Dominica, it is illegal to knowingly assist in the financing of terrorism, including the possession of terrorist funds or property. If SCB knows or suspects that the Bank has terrorist property in the Bank's possession, it must be reported immediately.[9]

4.1 How Money Laundering Works

Money laundering is described as having three phases by the Financial Action Task Force (FATF). These are Placement, Layering and Integration[10]. These phases are described in detail below.

Placement: In the initial – or Placement – stage of money laundering, the launderer introduces illegal profits into the financial system. An example of how this might be done, is by breaking up large amounts of cash into less conspicuous, smaller sums that are then deposited into a bank account, or used in purchasing a series of monetary instruments (checks, money orders, etc.), that are then deposited into accounts at other locations.

Layering: After the funds have entered the financial system, the second – or Layering – stage takes place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their criminal source.

---

[7] *See*: Section 11.

[8] FATF (2012), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, updated October 2015, FATF, Paris, France, www.fatf-gafi.org/recommendations.html

[9] The Anti-Money Laundering and Suppression of Terrorist Financing Code of Practice 2014 became law on May 1st, 2014 and affects several of the 'other' CFATF Dominica AML/CTR Recommendations. There are several objectives which the Code is intended to achieve including, outlining and providing guidance on the relevant requirements of the Drug (Prevention of Misuse) Act, the FIU Act, the MLPA and its regulations and the SFTA and to ensuring that financial institutions and persons carrying on a relevant business put appropriate systems and controls in place so as to enable them to detect and prevent money laundering and terrorist financing. The mandatory language used in the Code clearly sets out provisions which relevant entities are bound to comply with. The mandatory language is bolstered by s.59 (1) which has created offences and penalties for contravention or failure to comply with specified provisions detailed at Schedule 3 of the said Code. The Code is enforced by the FSU which can impose administrative sanctions for non-compliance and breaches of the provisions set out at Schedule 3.

[10] http://www.fatf-gafi.org/pages/faq/moneylaundering/

The funds might be channelled through different types of currencies, or the launderer might simply wire the funds through a series of accounts across the globe. This use of widely scattered accounts, for money laundering purposes, is especially prevalent in those jurisdictions that do not co-operate in, or are listed as having insufficient, anti-money laundering controls by FATF. In some instances, the launderer might disguise the transfers as payments for goods or services, in an attempt to give them a legitimate appearance.

Integration: Having successfully processed funds through the first two phases, the launderer then moves them to the third – or Integration – stage, in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures, to further add to the air of legitimacy.

4.2 How Terrorist Financing Works

Terrorist financing, as opposed to money laundering, can occur with legitimate funds, rather than proceeds of criminal activities. Legitimate funds can be easily transferred, then used by those who commit terrorist activities. In this respect, it can be assumed that terrorist financing most often acts in the 'Layering' and 'Integration' phases described above. However, rather than luxury items, the funds are used for the commission or support of terrorist activities and/or organisations.

5 Clients

When SCB's clients want to setup an account, in order to facilitate transactions through the Bank, the Bank must confirm certain information before any transactions are conducted. To setup an account with SCB, the Bank must collect Client Identification Program (CIP) information, as well as Client Due Diligence (CDD)/Know Your Client (KYC) information. The specifics of the information to be collected depends on whether the client is an individual or organisation.

SCB serves its clients electronically, via the phone or email, so the Bank's clients do not visit SCB's physical location. Due to this SCB must incorporate non face-to-face identification methods. However, once a client is approved so there is an existing client record, the Bank does not need to re-identify the client at the time of a transaction, provided the SCB staff member recognizes the client, whether visually or by voice. SCB staff must be ensure the client information on file is correct and up to date. For example, if the identification document on file that was used for CIP purposes has expired, the client must be re-identified (described below). If you are not certain whether the information that we have on file is up to date, you are required to re-identify the client, even if you recognize them.

6 Client Identification Program

In all cases, SCB identifies the Bank's clients using SCB's Client Identification Program (CIP), as well as records specific information about the client, which composes SCB's Client Due Diligence (CDD) and Know Your Client (KYC) processes. This is not negotiable, due to the legislative obligations on SCB holding a banking license issued by the Ministry of Finance of the Commonwealth of Dominica and regulated by the Commonwealth's Financial Supervision Unit. If the Bank is not able to identify the client, SCB must decline the relationship, until such time that fulsome CIP, CDD and KYC requirements have been met.

In other cases, we must attempt to identify the client, if it is possible to do so, without letting the client know that we may have suspicions about their activities or behaviour. These include:

- Suspected money laundering or terrorist financing activity, where we are required to fill out the internal Unusual Activity Form (UAF), which is described later in this document.

In cases where SCB cannot identify a client, the Bank must document the reasons that the client could not be identified and the efforts made to identify them. These clients will be considered higher risk and Enhanced Due Diligence (EDD) measures will be applied by the Compliance Officer. In some cases, the Compliance Officer may ask a staff member to contact the client to request additional information/documentation.

6.1 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 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:

> …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.[11]

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 submit a report to 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.[12]

6.2 Client Risk Factors and Enhanced Due Diligence (EDD) Activity

These are sample EDD activities. Additional risk factors and EDD activities may be considered at the Compliance Officer's 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;	A copy of the organisation's external compliance review and/or regulatory examination results.

[11] 2013 Money Laundering (Prevention) S.R.O. No. 4.
[12] The FSU is the authority regulating the SCB's compliance program, 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/

Risk Factor	EDD Activity
• Venture risk capital companies; • Money transmission services; • Money lending and pawning; • Mutual Funds; • Trust businesses; • Insurance businesses; • 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 <u>not</u> 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[13].	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

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

Risk Factor	EDD Activity
	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.

7 Client Account Opening Process: Organisations

7.1 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 Program (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.

7.1.1 Incorporated Company

- Form W-9 or W-8 Series (as appropriate[14]); and:
- Articles of Incorporation[15]; or
- Certificate of Incorporation[16]; and
- Most recent annual return registration (except in respect of International Business Companies)[17], and
- Documentary evidence regarding an officer of the corporation proving "that the person is who the person claims to be[18]," and one of the following:

---

[14] Providing tax advice to clients is not permitted or advised.
[15] To be notarized where the corporate body is incorporated outside Dominica.
2013 Money Laundering (Prevention) S.R.O. 4 Part 1.2.
[16] Id.
[17] Id.

- 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.

7.1.2 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.

7.1.3 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

---

[18] 2013 Money Laundering (Prevention) S.R.O. 4 Part 1.2.

- Business Permit/License from an issuing authority (City, County or State); or
- Sales Tax Certificate from the IRS.

7.1.4 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.

7.1.5 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.

7.1.6 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.

7.1.7 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.

7.2 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.

7.3 Organisation 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).

7.4 Beneficial Owners

In addition, SCB 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[19]. 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 application, 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:

7.4.1 Incorporated Company:

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

7.4.2 Partnership:

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

7.4.3 Limited Liability Entity (LLC or Ltd):

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

[19] 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.

7.4.4 Cooperative:

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

7.4.5 Not-For Profit/Charity:

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

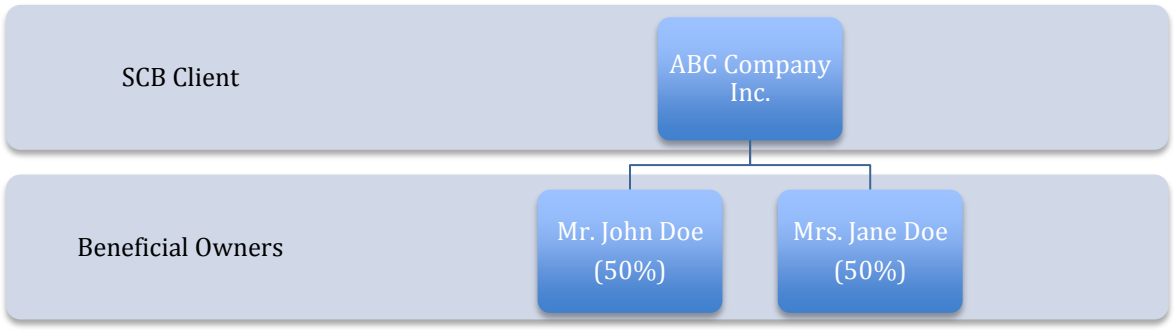
7.4.6 Trust:

- Trust Charter; or
- Trust Ledger.

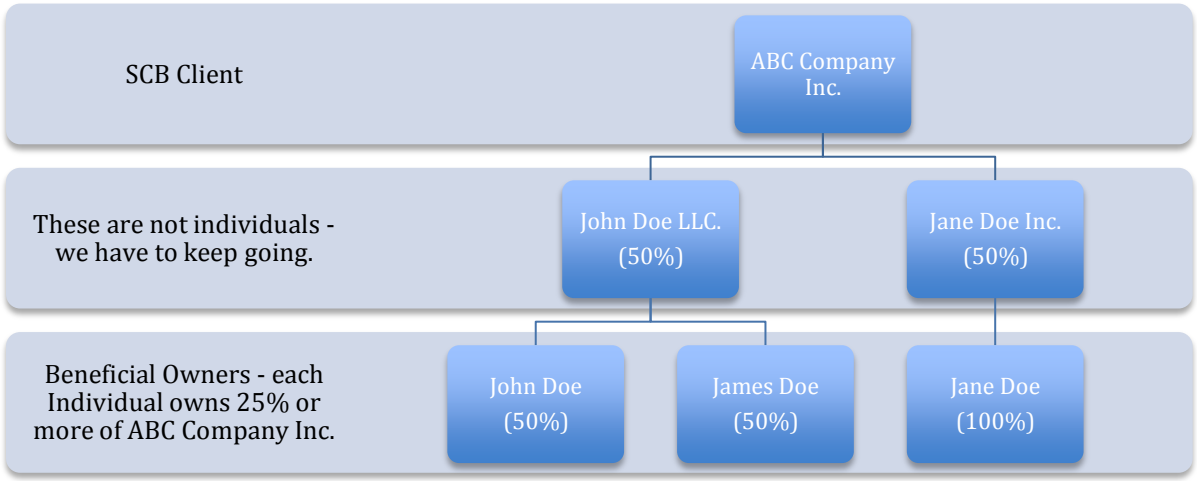
7.4.7 Informal Organisation

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

7.5 Direct Beneficial Ownership Example



7.6 Indirect Beneficial Ownership Example



8 Client Account Opening Process: Individuals

8.1 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 Program (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.

9 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[20].

10 Staff Using SCB's IT System

Staff who have access to SCB's IT system will input the above client information directly into the fields provided. If information is not correctly entered into the system, the account cannot be considered active.

11 Introducer/Affiliate Forms

Introducers/Affiliates may use SCB's account opening forms, which may be a physical paper document, to provide the sales staff with the required CIP, CDD and KYC information. All sections of the forms must be completed prior to submission and the Compliance Officer, or a delegate, may request additional information/documentation, where the risks presented in the client's supplied information must be sufficiently mitigated, which would fall under the Bank's EDD processes, which are described in detail above.

The Introducer/Affiliate must complete the CIP, CDD and KYC processes, and it is a best practice to fill out the required documentation, while looking at the documentation provided. The client's information must match what is known about the client, and if possible, what is already on file. If the information provided does not match what is already known, the Introducer/Affiliate must take notes and contact the Compliance Officer, prior to submitting the account opening forms. If the Bank's staff is unsure what forms are required, or have suspicions about the potential client, contact the Compliance Officer for clarification.

12 Regulatory Reporting

SCB must report certain types of transactions to the Bank's regulator[21](s). Reporting to any regulatory, law enforcement, or government agency, should always be completed by the Compliance Officer, or a delegate (a person that has been trained to submit regulatory reports in the Compliance Officer's absence). All other employees should use the internal forms included in this program, to submit reports to the Compliance Officer. If you are not sure whether or not you will need to submit a report, speak with the Compliance Officer for clarification. If it is not

---

[20]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.

[21] For AML/CTF reporting, the FIU is the regulator.

possible to speak with the Compliance Officer at that time, err on the side of caution by collecting the information that you need to fill out the form(s) and submit the report(s).

All regulatory reports have specific timelines in which they must be submitted. Therefore, all internal reports should be submitted to the Compliance Officer on the same day that the activity or transaction takes place.

12.1 Suspicious Transaction Guidelines and Reports

Suspicious Transaction Reports (STRs) are submitted to the FIU, where there is 'reasonable grounds' to suspect that a client's activity is related to money laundering or terrorist financing. STRs must be submitted to the FIU (by courier[22] or electronically[23]), even if the suspicious transaction is not completed, regardless of whether it 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 activity to be suspicious.

Employees must report any activity or transaction they find unusual, using the internal Unusual Activity Form (UTF) in Appendix 1 of this document. A list of suspicious indicators is also included in this document, and should be reviewed regularly by all staff, to ensure the Bank is familiar with the indicators, and therefore, adequately prepared to recognize potentially suspicious activities or transactions.

It is important not to let the client know when the Bank is suspicious. It is against the law to deliberately 'tip off' a client about a potential STR filing, or even the escalation of a UTF. SCB is, however, protected under the Commonwealth of

---

[22] Director
Financial Intelligence Unit
Top Floor
11 Great Marlborough Street
Roseau
Commonwealth of Dominica
West Indies

Tel.: (767)-266-3349/3348/3374/3084/4145/4146
Fax: (767)-440-0373
E-mail: fiu@dominica.gov.dm
Website: www.dominica.gov.dm

[23] www.fiu.gov.dm; http://www.cbn4.com/2016/04/01/dominica-launches-e-filing-system/; http://www.caribbeannationalweekly.com/featured/dominica-launches-new-anti-crime-software/

Dominica law from any action when the Bank submits a report in good faith. In most scenarios, even when a case goes to court, the client will not know that this report has been filed.

It is a legislative requirement that SCB attempts to identify clients that conduct or attempt suspicious activities, and when the Bank is unable to do so, the Bank must record the attempts taken and the reason the client could not be identified. The client may ask SCB why the Bank is requesting their identification information, and in such cases, it is a best practice to let the client know that it is company policy to collect this information. If a client's contact details are not used for additional marketing purposes, let the client know that as well because often clients are more concerned about privacy and security issues, and reassuring them may be helpful.

STRs must be submitted to the FIU within 5 days of the date that the Compliance Officer deems the activity to be suspicious. In order to provide enough time for the Compliance Officer to properly investigate the incident, make an official determination and possibly file a report with the FIU, the UTF must be submitted on the same day that the activity occurs.

13 Suspicious Indicators and Red Flags

There are a wide variety of factors that can indicate that a client's activity may be related to money laundering or terrorist financing. These include behaviours, as well as transaction patterns. When it comes to concerns related to suspicious activity, trust "your" instincts – if something does not feel right (whether or not any of these indicators are present), file a UTF with the Compliance Officer.

The indicators provided below, are a sample contained on the FIU website, the FIU's STR Guidelines 2014, [24] and generally accepted red flags, which will be augmented regularly by the Compliance Officer, based on trends observed in banking, trade financing, and/or the financial services industry.

13.1 Suspicious Indicators and Red Flags Related to Money Laundering

13.1.1 Unwillingness or Inability to Provide Required Information

- Information provided by a client is insufficient or their behaviour seems unusual;
- A client provides unusual or altered identification documents that cannot be readily verified;

[24] http://fiu.gov.dm/strs/strs-guidelines and the Financial Intelligence Unit | STR Guidelines 2014.

- A client uses a different Taxpayer Identification Number with variations of their name;
- A business client is reluctant, or unable, to provide complete information about the nature and purpose of anticipated funds transfer activity, its key personnel or its physical location;
- A client's home or business telephone is disconnected;
- The client's transaction activity differs from that which would be expected on the basis of their business/occupation;

13.1.2 Efforts to Avoid Reporting or Recordkeeping Requirements

- A client tries to persuade an employee not to file the required regulatory or internal reports, in order to avoid the maintenance of required records;
- A client is reluctant to provide information needed to file a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed;
- A client asks to be exempted from regulatory reporting, identification or recordkeeping requirements; or
- A client sends funds to several different foreign beneficiaries, usually in amounts of less than USD 10,000, particularly to, or through, a location of specific concern (e.g., countries designated by national authorities on money laundering or the Financial Action Task Force as non-cooperative countries and/or territories).

13.1.3 Electronic Fund Transfers

- Many Electronic Fund Transfers (EFTs) that are sent in large, round dollar amounts;
- EFT activity related to a financial secrecy haven, or a high-risk jurisdiction, without an apparent purpose;
- EFT activity that is inconsistent with the client's history or what is expected, given what we know about the client;
- EFT activity that is unexplained, repetitive, or shows unusual patterns;
- Large, outgoing EFTs that are sent on behalf of a third party, with no apparent affiliation with the Bank's client, who is unable to provide a rational explanation; or
- Unusually complex series of transactions indicative of layering activity involving multiple accounts, banks, parties, jurisdictions.

13.1.4 Activity Inconsistent with the Client's Business

- A lack of evidence of legitimate business activity, or any business operations at all, undertaken by many of the parties to the transaction(s);
- An unusual financial nexus and transactions occurring among certain business types (e.g., food importer dealing with an auto parts exporter);
- A client's transaction patterns show a sudden change, which is considered inconsistent with normal activities and cannot be adequately explained;

- A large volume of EFTs sent, but the client's typical activity does not align with the total or velocity;
- A business has dramatically different transaction patterns from similar businesses, in the same general industry and location; or
- The beneficiary of EFTs, sent by a client who is a business, do not align with the expected transaction patterns or business activities.

13.1.5 Other Unusual or Suspicious Client Activity—Trade Based[25]

- Over invoicing;
- Under invoicing;
- Multiple invoicing by issuing more than one invoice for the same goods;
- Short shipping – seller ships less than the invoiced quantity or quality of goods;
- Over shipping – seller ships more than the invoiced quantity or quality of goods;
- Deliberate obfuscation of the type of goods by simply omitting information from relevant documentation or deliberately disguising or falsifying it; or
- Phantom shipping – no goods are shipped and all documentation is completely falsified.

13.1.6 Other Unusual or Suspicious Client Activity

- Correspondent accounts being utilized as "pass-through" points by foreign jurisdictions with subsequent outgoing funds to another foreign jurisdiction.
- EFTs that are structured through multiple beneficiaries by the same client, or groups of clients, simultaneously;
- EFTs that are requested in amounts just below the identification and/or reporting thresholds;
- A client who is not concerned with the associated costs of the transaction, but is more focused on immediate execution or avoiding reporting requirements;
- A client who is clearly attempting to use personal funds for business purposes, such as providing personal bank account details, for a payment that is specifically related to their business;
- Client makes multiple and/or frequent transactions to various beneficiaries, or destinations, without a reasonable explanation;
- A client conducts high-value transactions that do not align with the client's expected income volume; or
- Beneficiaries maintaining accounts at foreign banks that have been subject to previous STR filings.

13.2 Suspicious Indicators and Red Flags Related to Terrorist Financing

---

[25] FATF's study notes regarding the basic techniques of trade-based money laundering.

13.2.1 Activity Inconsistent with the Client's Business

- The stated occupation, or nature of business, of a client is not consistent with the type or volume of activity stated;
- Persons involved in transactions who share a common address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or retired); or
- In regards to a non-profit or charitable organisation, EFTs are conducted where there appears to be no logical economic purpose or commonality between the stated activity of the organisation and the beneficiaries of the funds being transferred.

13.2.2 Electronic Fund Transfers

- A large number of outgoing EFTs where there does not appear to be a logical business or other economic purpose for the transfers, particularly when this activity involves high-risk jurisdictions;
- EFTs requested in small amounts in an apparent effort to avoid triggering reporting requirements;
- EFTs requested by a client who is unable or unwilling to provide information on the beneficiary or the person on whose behalf the transaction is being conducted; or
- In regards to a non-profit or charitable organisation, multiple EFTs which are all sent to a specific foreign beneficiary, particularly when there appears to be no logical economic purpose for the transaction and/or a high-risk jurisdiction is involved.

13.2.3 Other Transactions That Appear Unusual or Suspicious

- Multiple transactions within a short period of time, that involve high-risk jurisdictions;
- Multiple clients simultaneously request EFTs to a foreign beneficiary in high-risk jurisdiction; or
- A client engages in transactions involving the movement of funds to a high-risk jurisdiction, when there appears to be no logical economic purpose and/or an explanation cannot be provided.

14 Requests from Regulators and Law Enforcement

SCB cooperates with all of the Bank's regulators and all law enforcement agencies, both local and abroad. Any staff member, Introducer or Affiliate, who receives a request from any regulator or law enforcement agency, is required to forward the request immediately to the Compliance Officer.

All SCB staff need to be aware of the illegality of "Tipping Off"[26].

[26] 2011 Money Laundering (Prevention) Act No. 8.

(1) A person who has reasonable grounds to believe that an investigation into a money laundering offence has been, is being or is about to be made shall not prejudice the investigation by divulging the fact to another person.

(2) A person who contravenes the above commits an offence and is liable on conviction to a ***fine not exceeding five hundred thousand dollars and to imprisonment for a term not exceeding five years***.

15 Appendix 1: Unusual Transaction Form (Internal)

This form should be completed if the Bank has reasonable grounds to suspect that a client's activities are related to money laundering or terrorist financing. This form should be submitted to the Compliance Officer on the same day that it is completed.

Do not let the client know that you are filling out this form or discuss its contents with anyone other than the Compliance Officer or a delegate.

Your Name & Location (SCB Office or Introducer/Affiliate Location): _____

_____

Client's Name: _____

Were you able to identify the client?

If yes, please include the client's identification information in the section below. If not, please explain why this was not possible (please use additional pages as needed):

_____

_____

Describe the client's request or transaction, including whether the transaction was completed or not (please use additional pages as needed):

_____

_____

Describe in your own words what happened, and what made you suspicious. Please be as detailed as possible, and include facts about the client's behaviour, and any specific words or phrases that they used. Describe what you did and said, as well as how the client responded. Please use additional pages as needed:

_____

_____

Date: _____ Time: _____

Your Signature: _____

For Compliance Use Only

Date reviewed: _____

Reviewed By: _____

Is this transaction deemed to be suspicious: _____ Yes _____ No

Describe the rationale for the decision above (whether or not the transaction is deemed to be suspicious). Please use additional pages if required.

_____

_____

_____

_____

Describe any follow up actions (if applicable). For example, adjustments to the client's risk rating, enhanced due diligence activities, etc.

_____

_____

_____

_____