**VIRGIN ISLANDS**

# ANTI-MONEY LAUNDERING AND TERRORIST FINANCING (AMENDMENT) CODE OF PRACTICE, 2022

## ARRANGEMENT OF SECTIONS

Section

38… Section 35 amended
39… Explanation to section 36 amended
40… Section 37 amended
41… Section 39 amended
42… Section 40 amended
43… Section 41 amended
44… Section 41A inserted
45… Part VA inserted
46… Section 42 amended
47… Section 43 revoked
48… Section 44 amended
49… Section 45 amended
50… Section 46 amended
51… Section 47 amended
52… Section 48 amended
53… Section 49 amended
54… Section 50 amended
55… Section 51 amended
56… Section 52 revoked
57… Section 53 amended
58… Section 53A inserted
59… Section 54 amended
60… Section 55 amended
61… Section 56 amended
62… Schedule 1 revoked and substituted
63… Schedule 2 revoked
64… Schedule 4 revoked and substituted

**VIRGIN ISLANDS**

**STATUTORY INSTRUMENT 2022 NO. 79**

**Proceeds of Criminal Conduct Act**
**(Revised Edition 2020)**

**Financial Services Commission Act**
**(Revised Edition 2020)**

**Anti-Money Laundering and Terrorist Financing (Amendment) Code of Practice, 2022**

*[Gazetted 29th August, 2022]*

The Financial Services Commission, pursuant to the powers conferred by section 27 (1) of the Proceeds of Criminal Conduct Act, Revised Edition 2020 and after consultation with the Joint Anti-money Laundering and Terrorist Financing Advisory Committee, amends the Anti-Money Laundering and Terrorist Financing Code of Practice, Revised Edition 2020.

**Citation and commencement**

**1.** (1) This Code may be cited as the Anti-Money Laundering and Terrorist Financing (Amendment) Code of Practice, 2022.

(2) Subject to subsection (3), this Code shall come into force on the 29th day of August, 2022.

(3) The provisions of this Code relating to virtual assets transfers shall come into force on the 1st day of December, 2022.

**Section 2 amended**

**2.** Section 2 of the Anti-Money Laundering and Terrorist Financing Code of Practice, Revised Edition 2020 (hereinafter referred to as "the principal Code of Practice") is amended

(a) in subsection (1)

(i) by inserting in their appropriate alphabetical order, the following new definitions:

"control", for the purposes of the definition of "beneficial owner", means having an influence over the activities of an applicant for business or customer without any ownership interest, and includes

(a) having an influence through close family relationships, or historical or contractual associations; or

(b) using, enjoying or benefitting from the assets owned by the applicant for business or customer;

"country" includes a territory or other jurisdiction, however described, that is a part of or in association or is assimilated with another country, or that,

though not independent, has internal self-government or other control with regard to the running of its own affairs, whether generally or specifically;

"financial group" means a group designated in writing as such by the Commission or the Agency that consists of

(a) a parent company, or any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision of AML/CFT policies and procedures; and

(b) its branches and subsidiaries that are subject to the AML/CFT policies and procedures;

"money laundering" has the meaning ascribed to it under section 2 (1) of the Act;

"NPO" means a body of persons whether incorporated or unincorporated, established solely or primarily for the promotion of charitable, religious, cultural, educational, social or fraternal purposes, or other activities or programmes for the benefit of the public and which raises or disburses funds in pursuance of its objectives primarily within the Territory;

"proliferation financing" has the meaning ascribed to it under section 6 of the Proliferation Financing (Prohibition) Act, No. 20 of 2021;

"terrorist financing" has the meaning ascribed to it in section 2(1) of the Financial Investigation Agency Act, Revised Edition 2020;

(ii) by deleting the definition of "applicant for business" and substituting the following new definition

"applicant for business" means the party intending to enter into a business relationship or one-off transaction with an entity or professional;";

(iii) by deleting the definition of "beneficial owner" and substituting the following definition

"beneficial owner" means the natural person who ultimately owns or controls an applicant for business or a customer or on whose behalf a transaction or activity is being conducted, and includes, though not restricted to

(a) in the case of a body corporate

(i) as it relates to a legal person that is not a company whose securities are listed on a recognised exchange, a natural person who ultimately owns or controls, whether directly or indirectly, 10% or more of the shares or voting rights in the legal person; and

(ii) as it relates to any body corporate, a natural person who otherwise exercises control over the management of the legal person; and

(b) in the case of a partnership

(i) a natural person who is ultimately entitled to or controls, whether directly or indirectly, 10% or more share of the capital or profits of the partnership or 10% or more voting rights in the partnership; and

(ii) a natural person who otherwise exercises control over the management of the partnership;

(c) in the case of a trust

(i) any natural person, characteristic or class of persons entitled to a vested right in the trust; and

(ii) the trustee, the settlor, the protector (if any), or any other person who has control over the trust; and

(d) in the case of any other type of legal person or legal arrangement, the natural persons in equivalent or similar positions or who exercise similar controls to those detailed in paragraphs (a) to (c);"

(iv) by deleting the definition of "high risk countries" and substituting the following definition

"high risk countries" means countries which

(a) are subject to sanctions, embargos or similar restrictive measures imposed under any other enactment or by the United Nations, or other regional or international organisation of which the Virgin Islands is a member or associate member, or of which the United Kingdom is a member and the sanctions, embargos or similar measures have been extended to the Virgin Islands by an Order in Council or through the exercise of any Royal Prerogative;

(b) satisfy any of the risk qualifications outlined in this Code;

(c) the Commission identifies and provides in a list published in the *Gazette* as representing high risk countries; or

(d) the Commission identifies in an advisory or a warning issued pursuant to the Financial Services Commission Act as having significant weaknesses in its anti-money laundering anti-terrorist financing or anti-proliferation financing systems, or as engaging in or promoting activities that are considered detrimental to public interest;

(v) in the definition of "key staff" or "key employee", by inserting after the word "transactions", the words ", or have responsibility for undertaking functions outlined in this Code";

(vi) by deleting the definition of "politically exposed person" or "PEP" and substituting the following definition

""politically exposed person" or "PEP" means an individual who is or has been entrusted with prominent public functions or is a member of senior management of an international organisation, including members of his or her immediate family, or persons who are known to be close associates of such an individual, and includes classifications established pursuant to section 22 (5);"

(vii) in the definition of "Reporting Officer", by deleting the words "Anti-money Laundering Reporting Officer" and substituting the words "Money Laundering Reporting Officer";

(viii) in paragraph (a) of the definition of "termination", by deleting the words, "or the completion of the last transaction" and substituting the words, ", expiration of a contract or on the basis of the terms agreed upon in an agreement";

(ix) by revoking the definitions of "non-account holding customer", "non-paying account", "Steering Committee" and "underlying beneficial owner"; and

(b) in subsection (2), by deleting the words, "are provided merely to serve as a guide and to" and substituting the words, "serve as guidance and".

**Section 3 amended**

**3**. Section 3 of the principal Code of Practice is amended

(a) by deleting paragraph (a) and substituting the following new paragraph

"(a) to outline the relevant requirements of the Act, Drug Trafficking Offences Act, Revised Edition 2020, Financial Investigation Agency Act, Revised Edition 2020, Counter-Terrorism Act, No. 33 of 2021, Proliferation Financing (Prohibition) Act, No 20 of 2021 and any other similar enactment, with respect to the detection and prevention of money laundering, terrorist financing and proliferation financing;"; and

(b) in paragraphs (b) and (e), by deleting the words "money laundering and terrorist financing" and substituting the words "money laundering, terrorist financing and proliferation financing".

---

*The Explanation to section 3 of the principal Code of Practice is amended*

*(a) by deleting paragraph (i) and substituting it with the following paragraph:*

*"**(i)** The Virgin Islands is a key player in the provision of financial services business (domestic and international) and must be committed to ensuring compliance with internationally established standards of regulation and enforcement relating to the detection and prevention of money laundering and countering the financing of terrorism. As a member of the Caribbean Financial Action Task Force (CFATF), the Territory is required to fully comply with the requirements of the 40 Recommendations of the Financial Action Task Force (FATF). The Territory is also a member of key organisations – International Organisation of Securities Commission (IOSCO), International Association of Insurance Supervisors (IAIS), Group*

*of International Finance Centre Supervisors (GIFCS) and Egmont – which apply FATF Recommendations as part of their sector specific benchmarks relative to anti-money laundering and terrorist financing measures in the areas of securities and investment, insurance, banking, fiduciary services and intelligence gathering and dissemination. In addition, the Territory fully observes all of the established standards designed to effectively combat acts of terrorism, proliferation of weapons of mass destruction and the financing of these activities."*

*(b) in paragraphs (ii) and (iii), by deleting the words "and terrorist financing" wherever they appear and substituting the words ", terrorist financing and proliferation financing"; and*

*(c) by deleting paragraph (iv) and substituting it with the following paragraph*

*"**(iv)** Accordingly, the objectives set out in this Code outline the Territory's commitment to good corporate governance and the promotion of international cooperation to ensure that global financial markets are not misused for illicit purposes. The provisions of the Code may be viewed as risk sensitive standards that are relevant and prudent to prevent the business of entities and professionals from being caught up in unsuspecting acts of money laundering, terrorist financing and proliferation financing. The Code, in effect, supplements the provisions of the Drug Trafficking Act, (DTOA), Proceeds of Criminal Conduct Act (PCCA), Financial Investigation Agency Act, (FIAA), Proliferation Financing (Prohibition) Act (PFPA), Counter Terrorism Act (CTA), The Terrorism (United Nations and Other Measures (Overseas Territories) Order ("the 2001 Order"), The Anti-terrorism (Financial and Other Measures) (Overseas Territories) Order ("the 2002 Order"), Anti-money Laundering Regulations (AMLR and other related enactments)."*

---

**Section 4 amended**

**4.** Section 4 of the principal Code of Practice is amended

(a) in subsection (1), by deleting paragraph (b) and substituting the following paragraph

"(b) an NPO to the extent specified in section 4A."

(b) in subsection (2), by deleting the words, "regulation 6 (1) or (3)" and substituting the words, "regulation 6 (3)"; and

(c) in subsection (3), by deleting the words "money laundering or terrorist financing" and substituting the words "money laundering, terrorist financing or proliferation financing".

---

*The Explanation to section 4 of the principal Code of Practice is deleted and substituted with the following*

*"**(i)** Section 27 (2) of the PCCA outlines the scope of the Commission's exercise of its powers to issue a Code of Practice. The definition of "entity" in section 2*

*essentially covers the scope permitted by section 27 (2) of the PCCA as fully outlined in the AMLR. The application section seeks to implement AML/CFT requirements on regulated entities and non-regulated entities within the defined parameters of FATF Recommendations, that are viewed as forming vital links in the anti-money laundering and countering the financing of terrorism (AML/CFT) efforts. The PCCA empowers the Commission to designate other businesses which are considered vulnerable to activities of money laundering, terrorist financing and proliferation financing and thus fall within the definition of "entity". These have been designated in the Non-financial Business (Designation) Notice which lists additional businesses that fall within the regime of the Code. The Notice may be amended from time to time to ensure a well-insulated business sector against the activities of money laundering, terrorist financing and proliferation financing, having regard, in particular, to the risks posed.*

***(ii)*** *Any entity or professional that is caught under this section of the Code must ensure full compliance with the due diligence, record keeping measures and all other requirements outlined in this Code.*

***(iii)*** *Section 4 (2) takes into account the exceptions to identification procedures outlined in regulation 6 (3) of the Anti-money Money Laundering Regulations with respect to the conduct of relevant business (as defined in regulation 2 (1) of the regulations).*

***(iv)*** *However, it must be borne in mind at all times that the burden of ensuring compliance with the obligations set out in this Code rests with the relevant entity or professional as outlined in section 2 (5). Accordingly, where an entity or a professional knows or suspects that an applicant for business or a customer who wishes to form a business relationship or conduct a one-off transaction is engaged in money laundering, terrorist financing or proliferation financing, it or he or she must not establish the business relationship or undertake the one-off transaction. Regulation 6 (4) (b) of the AMLR already provides for such a prohibition in relation to money laundering, terrorist financing and proliferation financing which is further prohibited pursuant to section 23(2D) of this Code. It would be incumbent under such circumstances for the entity or professional to submit a report to the Agency outlining its suspicion."*

---

**Section 4A amended**

**5**. Section 4A of the principal Code of Practice is amended

(a) in the heading, by deleting the words, "charities, etc." and substituting the word, "NPOs";

(b) in subsection (1)

(i) in the opening paragraph, by deleting the words, "charity or other association not for profit", and substituting the word, "NPO";

(ii) by deleting paragraph (a) and substituting the following paragraph

"(a) is incorporated or otherwise formed and carries on its business in the Virgin Islands; or";

(iii) in paragraph (b), by deleting the words "in or from within the Virgin Islands; or" and substituting the words, "in the Virgin Islands; and"; and

(iv) in paragraph (c), by deleting the words, "is established as provided in paragraph (a) and";

(c) in subsection (2)

(i) by deleting the opening paragraph and substituting the following opening paragraph

""An NPO shall –";

(ii) in paragraphs (a) and (c), by deleting the words, "charity or other association not for profit" and respectively substituting the word, "NPO"; and

(iii) by deleting paragraph (d) and substituting the following paragraph

"(d) adopt such measures as are considered appropriate to ensure that any funds or other assets that are received, maintained or transferred by or through the NPO are not for, or diverted to support

(i) the activities of any terrorist, terrorist organisation or other organised criminal group; or

(ii) any money laundering or proliferation financing activity.";

(d) in subsection (3), by inserting after the words, "appear to be linked" the words, "to other donations from the same donor or other donors";

(e) in subsection (4), by inserting after the words, "or its equivalent in any", the word, "other";

(f) in subsection (5), by deleting the opening paragraph and substituting the following opening paragraph

"An NPO that receives a donation shall carry out the requisite customer due diligence and record keeping measures under this Code on any person who makes a donation (whether in cash or otherwise in excess of the amount or its equivalent stipulated in this section), including";

(g) by inserting after subsection (5), the following new subsection

"(5A) Subsection (5) also applies where a person makes a donation to an NPO and does not wish to have its or his or her name publicly revealed.";

(h) in subsection (6), by deleting the opening paragraph and substituting the following opening paragraph

"Where an NPO suspects that a donation may be linked to money laundering, terrorist financing or proliferation financing, it shall"; and

(i) by inserting after subsection (6), the following new subsection

"(6A) Where an NPO suspects that a donation that has been accepted may be linked to money laundering, terrorist financing or proliferation financing, it shall report its suspicion to the Agency and act in accordance with any direction given by the Agency.".

---

*The Explanation to section 4A of the principal Code of Practice is deleted and substituted with the following:*

*"**(i)** As noted in section 4, this Code equally applies to NPOs as if they were entities. NPOs are not immune to abuse for money laundering, terrorist financing and proliferation financing activities and must accordingly adopt all necessary due diligence measures outlined in this Code to ensure compliance therewith. It is expected that in applying the provisions of this Code to an NPO, those provisions of the Code will be applied with such necessary modification as would enable proper compliance with the provisions. Where there is uncertainty, advice must be sought from the Agency and such advice complied with accordingly. Ultimately, the responsibility for full compliance with the requirements of this Code rests with the NPO (as already noted in section 2 (5)).*

***(ii)** Every NPO should expect that the laws, policies and guidelines relating to their activities and operations would be reviewed from time to time to verify compliance with the obligations outlined in this Code and ensure that they are not being used for money laundering, terrorist financing and proliferation financing purposes. It is therefore important that every NPO brings to the attention of the Agency any activity with respect to which it has a suspicion of money laundering, terrorist financing or proliferation financing. This would enable the Agency to guide and assist the NPO from being used for money laundering, terrorist financing and/or proliferation financing purposes."*

---

**Section 5 revoked and substituted**

**6**. Section 5 of the principal Code of Practice is revoked and substituted by the following section

**"Compliance with this Code**

**5**. (1) Every entity and professional is required to fully comply with this Code which provides requirements relating to money laundering, terrorist financing and proliferation financing.

(2) An entity or a professional shall adopt such standards and systems of internal controls as it or he or she considers commensurate with its or his or her risk-based methodology in order to reduce or mitigate identified money laundering, terrorist financing or proliferation financing risks."

***[Explanation***

*The Explanation to section 5 of the principal Code of Practice is deleted and substituted with the following:*

"*It should be noted that the imperatives outlined in this Code must be fully complied with by every entity and professional. The Code itself must be viewed as setting standards of compliance. These standards must be applied on a risk sensitive basis, whereby the entity or professional places a higher level of focus, resources and measures to matters that pose a higher level of ML/TF risk. Risk-based standards or systems of internal control must be appropriately documented and made available when required during an inspection or otherwise in pursuance of the provisions or objectives of this Code.]"*

**Section 6 amended**

**7.** Section 6 of the principal Code of Practice is amended

(a) by deleting subsection (1) and substituting the following subsection

"(1) The Agency is the reporting authority of the Virgin Islands and is responsible for matters relating to suspicious transaction reports concerning money laundering, terrorist financing and proliferation financing."

(b) in subsection (3)

(i) in paragraph (d), by deleting the word "and" at the end of the paragraph;

(ii) in paragraph (e), by deleting the full-stop at the end of the paragraph and substituting the word, "; and"; and

(iii) by inserting after paragraph (e), the following new paragraph

"(f) such other information as the Agency, in the exercise of its powers under this Code, Financial Investigation Agency Act, Revised Edition 2020 or any other enactment, may require in writing.".

**Section 7 amended**

**8.** Section 7 of the principal Code of Practice is amended

(a) in subsection (1)

(i) by deleting paragraph (a) and substituting the following paragraph

"(a) assign it to such investigating officer or other officer of the Agency as the Director of the Agency determines;";

(ii) in paragraph (b), by inserting after the words, "investigating officer" the words, "or other officer of the Agency";

(b) in subsection (3), by deleting the words, "the advice and guidance of the Agency" and substituting the words, "any direction given by the Agency"; and

(c) in subsection (5)

(i) by deleting the words, "advice or guidance" and substituting the word, "direction"; and

(ii) by deleting the words, "the Proceeds of Criminal Conduct Act" and substituting the words, "the Act".

---

*The Explanation to section 7 of the principal Code of Practice is amended*

*(a) in paragraph (i) by:*

*(i) inserting after the words "in addition to those prescribed in the DTOA, PCCA", the words ", CTA, PFPA and other related enactments"; and*

*(ii) by deleting the words "money laundering and terrorist financing" and substituting the words "money laundering, terrorist financing and proliferation financing";*

*(b) in paragraph (iii) by inserting after the words, "the DTOA, PCCA" the words, "PFPA, CTA"; and*

*(c) deleting paragraph (iv) and substituting the following paragraph*

*"**(iv)** While it is considered good practice for the entity or professional that filed a suspicious transaction report to be informed of the status of its report to the Agency, it should be noted that such information would essentially relate only to the general status; entities or professionals must not expect details of any investigation which may jeopardise or in any way compromise the investigation. It is expected that where the Agency, after the receipt of a report, decides not to proceed to investigation of the report or concludes investigation in relation to the report, it will advise the reporting entity or professional accordingly. Such advice may include information as to whether the person to whom the report relates poses a higher level of risk, measures to adopt to effectively deal with the associated risk, how such person should be dealt with now and in the future, how any pending and future transaction with the person should be handled, etc. Advice may also include feedback on the quality of the report filed and suggestions for improvement in reports going forward."*

---

**Section 8 amended**

**9.** Section 8 of the principal Code of Practice is amended

(a) by deleting subsection (1) and substituting the following subsection

"(1) It is the duty of the Commission to monitor compliance by its licensees with this Code and any other enactment (including any other code and any

guidelines) relating to money laundering, terrorist financing or proliferation financing as may be prescribed by this Code or any other enactment.";

(b) in subsection (2), by deleting the word "also"; and

(c) in subsection (3), by deleting the words "money laundering and terrorist financing" and substituting the words "money laundering, terrorist financing and proliferation financing".

---

*The Explanation to section 8 of the principal Code of Practice is deleted and substituted by the following*

*"(i) The Commission has a statutory duty to ensure full compliance with AML/CFT measures by those persons that it regulates. Similarly, the Agency is statutorily responsible for ensuring AML/CFT compliance of all entities and professionals that are not regulated by the Commission. Accordingly, any entity or professional that is caught under section 27 (2) of the PCCA – be it a licensee regulated by the Commission, a non-financial business and profession or Commission-designated entity or professional– falls to be dealt with under this Code and must comply with the requirements of the Code.*

*(ii) While the Commission has a duty to include AML/CFT matters in its educational programmes (such as its periodic Meet The Regulator fora, in its newsletters, through industry training sessions), entities and professionals have everything to gain by engaging in a similar exercise on a periodic basis; it certainly is an obligation under the requirement for staff training."*

---

**Section 9 amended**

**10**. Section 9 of the principal Code of Practice is amended

(a) by deleting subsection (1) and substituting the following subsection

"(1) As part of its inspection of an entity or professional that it regulates, the Commission is expected to review the anti-money laundering, terrorist financing and proliferation financing policies, processes, procedures and control systems of the entity or professional in order to make an objective assessment of

(a) the risk profile of the entity or professional;

(b) the adequacy or otherwise of the entity's or professional's mitigation measures;

(c) the entity's or professional's compliance with the requirements of the Act, Anti-money Laundering Regulations, Revised Edition 2020, Counter-Terrorism Act, No. 33 of 2021, Proliferation Financing (Prohibition) Act, No. 20 of 2021, this Code and any other code, guideline, practice direction or directive that the Commission issues, including any other enactment that applies to such an entity or professional.";

(b) by deleting subsection (2), and substituting the following subsection

"(2) In relation to an entity or a professional that is not regulated by the Commission but to which, or to whom, this Code applies, the Agency shall perform in relation to such an entity or a professional the duty imposed under subsection (1), and in such a case the reference to "Commission" shall be treated as a reference to the Agency."; and

(c) in subsection (3), by deleting the opening paragraph and substituting the following opening paragraph

"After every review of an entity's or a professional's anti-money laundering, terrorist financing and proliferation financing policies, processes, procedures and control systems, the Commission or the Agency, as the case may be".

---

*The Explanation to section 9 of the principal Code of Practice is amended*

*(a) by deleting paragraph (i) and substituting the following paragraph*

*"**(i)** As part of its prudential regulation process, the Commission conducts both on-site and off-site inspections of entities or professionals that it regulates. Inspectors are, during the course of their inspections, expected (amongst other things) to identity weaknesses in the entity's or professional's anti-money laundering, terrorist financing and proliferation financing policies, processes, procedures and control systems through an analysis of the entity's or professional's internal controls and management systems and other available information within or in respect of the entity or professional. This section requires the extension of such an inspection to every entity and professional caught by this Code. The Commission will review a regulated entity's or professional's risk assessments as part of its periodic inspections and the other entities and professionals caught by this Code will be similarly inspected by the Agency.";*

*(b) in paragraph (ii), by inserting after the words,* "*Inspectors are encouraged to use whatever knowledge they have of the risks associated with any products, services, customers", the words ", delivery channels"; and*

*(c) in the first bulleted point of paragraph (iv), by deleting the word "minimum".*

---

**Section 10 amended**

**11.** Section 10 of the principal Code of Practice is amended in subsections (1) and (2) by deleting the words, "and terrorist financing" wherever they appear and substituting the words, ", terrorist financing and proliferation financing".

---

*The Explanation to section 10 of the principal Code of Practice is amended*

*(a) in paragraph (ii), by deleting the words, "including what obtains elsewhere," and substituting the words, "including what information it obtains elsewhere";*

*(b) in paragraph (iii), by deleting the last sentence and substituting the following sentence*

*"Training should also provide a guideline as to how to properly embark on such a review process with the full cooperation of the entity or professional being inspected."*

---

**Section 11 amended**

**12.** Section 11 of the principal Code of Practice is amended

(a) by deleting subsection (1) and substituting the following subsection

"(1) An entity or a professional shall establish and maintain a written and effective system of internal controls, approved by senior management in the case of the entity, which provides appropriate policies, processes and procedures for forestalling and preventing money laundering, terrorist financing and proliferation financing, having regard to the money laundering, terrorist financing and proliferation financing risks and size of the entity's or professional's business.";

(b) by deleting subsection (2) and substituting the following subsection

"(2) The written system of internal controls established pursuant to subsection (1) shall be framed in a way that would enable the entity or professional to

(a) effectively identify, assess and understand the money laundering, terrorist financing and proliferation financing risks to which the entity's or professional's business is subject;

(b) manage and mitigate any money laundering, terrorist financing and proliferation financing risks identified by the entity or professional, a national risk assessment and any risk assessment conducted by a competent authority, law enforcement agency or any other authority with responsibility relating to money laundering, terrorist financing and proliferation financing; and

(c) apply enhanced measures to manage and mitigate higher risks that have been identified by the entity or professional, a national risk assessment and any risk assessment conducted by a competent authority, law enforcement agency or any other authority with responsibility relating to money laundering, terrorist financing and proliferation financing.";

(c) in subsection (3)

(i) in paragraph (a), by deleting the words "such as its or his or her products, services customers and geographic locations" and substituting the words, "such as its or his or her products and services, transactions, customers, geographic locations, and delivery channels";

(ii) in paragraph (f), by deleting the words "advice or guidance issued" and substituting the words "direction given";

(iii) in paragraph (l), by deleting the words "reportable transactions" and substituting the words "suspicious transactions or activities";

(iv) in paragraph (q), by deleting the words, "money laundering or terrorist financing" and substituting the words, "money laundering, terrorist financing, or proliferation financing";

(v) in paragraph (u), by deleting the word "and" at the end of the paragraph;

(vi)by inserting after paragraph (u), the following new paragraphs

"(u*a*) establishing policies and procedures to ensure compliance with sanctions obligations;

(u*b*) implementing systems and procedures for sanctions screening, monitoring and reporting; and"; and

(vii) in paragraphs (c), (d), (e), (h), (i), (m), and (n) by deleting the words "money laundering and terrorist financing" and substituting the words "money laundering, terrorist financing and proliferation financing";

(c) by deleting subsection (3A) and substituting the following subsection

"(3A) Every entity and professional shall, in relation to internal controls established under this section and other provisions of the Anti-money Laundering Regulations, Revised Edition 2020 and this Code

(a) establish mechanisms to monitor the implementation of those internal controls;

(b) establish and maintain an independent audit function that is adequately resourced to test compliance, including sample testing, with its or his or her written system of internal controls and produce an independent audit report of any compliance testing; and

(c) implement enhanced controls where higher risks are identified."; and

(d) deleting subsection (4) and substituting the following subsection

"(4) An entity or a professional that fails to comply with the requirements of this section commits an offence and is liable to be proceeded against pursuant to section 27 (4) of the Act.".

---

*The Explanation to section 11 is deleted and substituted with the following*

*"**(i)** This Code adopts a risk-based approach which is considered the most effective way of managing the risks that are associated with money laundering, terrorist financing and proliferation financing. It must be viewed as supplementing the AMLR, DTOA, PCCA, FSCA, FIAA, PFPA and CTA in so far as money laundering, terrorist financing and proliferation financing are concerned. The risk-based approach essentially enables an entity and a professional to balance the risks associated with their business, including customers, products, services, transactions,*

*delivery channels and geographic connections to the established measures to contain and properly deal with those risks. It provides an element of flexibility that enables an entity or a professional to devise and apply its or his or her own systems of internal controls and management to deal with specific cases and circumstances to forestall and prevent acts of money laundering, terrorist financing and proliferation financing in relation to the entity or professional. It is considered to be a more effective approach to dealing with money laundering, terrorist financing and proliferation financing in that it allows the entity or professional to concentrate resources proportionately to the more vulnerable areas of operations to ensure an effective system of controls. In a nutshell, the risk-based approach encompasses a recognition of the existence of the risks, an undertaking of the assessment of the risks and developing strategies to effectively manage and mitigate the risks identified.*

***(ii)*** *An entity's or a professional's ability to effectively deal with money laundering, terrorist financing and proliferation financing activities will depend immensely on the measures established and implemented to ensure appropriate internal controls. The entity or professional needs to develop appropriate compliance measures that properly enable the assessment of its or his or her business' risks by undertaking AML/CFT risk assessments, if it or he or she is to properly and effectively build a solid regime of internal controls.*

***(iii)*** *The nature, form and extent of AML/CFT compliance controls will invariably depend on several factors, considering the status and circumstances of the entity or professional in undertaking the assessment of the risks of its or his or her business. Some of those factors may be outlined as follows*

- *the nature, scale and complexity of the entity's or professional's business operations;*
- *the diversity of the entity's or professional's operations, including its or his or her geographical diversity;*
- *the profile of the entity's or professional's customers, products, services and activities;*
- *the distribution channels utilised by the entity or professional;*
- *the size and volume of the transactions engaged in by the entity or professional;*
- *the degree of risk associated with each area of the operations of the entity or professional;*
- *the extent to which the entity or professional is dealing directly with its or his or her customers or is dealing through intermediaries, third parties, correspondents or other non-face to face channels; and*

- *the measure of regulatory compliance which has effect on AML/CFT compliance.*

***(iv)*** *It is important therefore, in developing a system of internal controls, for an entity or a professional to adopt a holistic approach that takes the above factors into account. The factors operate as guidelines and adherence thereto will assist an entity or a professional in properly and effectively developing and establishing a strong AML/CFT regime that keeps the entity's or professional's name intact and insulates it or him or her against unwarranted criminal activity.*

***(v)*** *The internal controls of an entity or professional can only be effective at mitigating money laundering, terrorist financing and proliferation financing risks where controls are implemented appropriately. In that regard, it is important for every entity and professional to have mechanisms in place to monitor and audit the implementation of such controls. The requirement for monitoring the implementation of internal controls requires entities and professionals to ensure that employees are complying with relevant measures on an ongoing basis. This may include requirements for approvals of certain portions of activities and transactions, reviewing staff completed checklists and risk assessments, incremental reporting and other quality control reviews. Where weaknesses in compliance with requirements or effective mitigation of risks are identified via these ongoing mechanisms, entities and professionals must seek to implement means to ensure compliance or enhance relevant controls that enhance the entity's or professional's AML/CFT regime, as applicable.*

***(vi)****The requirement to establish and maintain an independent audit function creates an obligation on an entity and a professional to essentially ensure the* establishment *of appropriate and effective mechanisms which allow for a periodic evaluation of the implementation by the entity or professional of the provisions of the AMLR and this Code as well as the internal control systems developed by the entity or professional. This obligation must be implemented by a person or persons that function independently and who have the ability to make objective assessments in a transparent and fair manner. The audit function may form a separate and independent unit of the entity (such as its compliance portfolio) or the professional's undertaking, or the function may be outsourced. Whatever arrangement the entity chooses, it or he or she must provide adequate financial and human resources as would be commensurate with the size and volume of business of the entity or professional and adopt measures that guarantee the independent functioning of the arrangement. It should be noted that ultimately the objective is to ensure a proper and adequate testing of the entity's level of compliance with its AML/CFT obligations under the AMLR, this Code and other applicable laws and policies. It is imperative that the results of any testing of compliance obligations under this section are embodied in a compliance audit report to be maintained by the entity or professional and made available to the Agency or Commission in an inspection or whenever requested. In addition, the entity or professional must*

*provide an indication in writing as regards the steps taken, where applicable, to comply with any shortcomings identified in a compliance audit.".*

**Section 11A revoked**

**13.** Section 11A of the principal Code of Practice is revoked.

**Section 12 revoked and substituted**

**14.** Section 12 of the principal Code of Practice is revoked and substituted by the following section

**"Duty to carry out risk assessment**

**12**. (1) An entity and a professional, in addition to establishing a written system of internal controls, shall carry out

(a) an institutional money laundering, terrorist financing and proliferation financing risk assessment of its overall business, in consideration of relevant risk factors, including its or his or her customers, products, services or transactions, delivery channels and countries to which it or he or she is exposed; and

(b) money laundering, terrorist financing and proliferation financing risk assessment in relation to each applicant for business or customer, including any beneficial owners

in order

(i) to determine the existence of any risks;

(ii) to determine how best to manage and mitigate any identified risks;

(iii) to develop, establish and maintain appropriate anti-money laundering, terrorist financing and proliferation financing systems and controls to effectively respond to the identified risks; and

(iv) to ensure that at all times there is full compliance with the requirements of the Anti-money Laundering Regulations, Revied Edition 2020 and other enactments, policies, codes, practice directions, guidance and directives in place in relation to anti-money laundering, terrorist financing and proliferation financing activities.

(2) In relation to risk assessments undertaken pursuant to subsection (1), every entity and professional shall

(a) document and maintain records of the risk assessments conducted;

(b) consider all relevant risk factors before making a determination of the level of customer risk or institutional risk;

(c) apply the appropriate risk mitigation measures and controls based on the level of risk identified in risk assessments;

(d) regularly review and update risk assessments on an ongoing basis;

(e) update risk assessments where there are any changes in relevant risk factors; and

(f) have appropriate mechanisms in place to provide risk assessment information to the Commission or the Agency, on request.

(3) An entity or a professional shall, prior to the launch or use of new products, business practices, delivery mechanisms and technological developments

(a) identify and assess the money laundering, terrorist financing and proliferation financing risks that may arise in relation to the development of new products and new business practices, including new delivery channels and systems, and the use of new or developing technologies for new and pre-existing products or services; and

(b) take appropriate measures to manage and mitigate identified risks.

(4) In relation to any risk assessment conducted under subsection (3), an entity or a professional shall

(a) document and maintain records of the risk assessment conducted; and

(b) have appropriate mechanisms in place to provide risk assessment information to the Commission or the Agency as requested."

---

*The following explanation is inserted immediately after section 12*

*"[**Explanation***

***(i)*** *The internal controls required under section 11, contemplate the application of a risk-based approach (RBA) in forestalling and preventing money laundering, terrorist financing and proliferation financing via the business of an entity or professional. Consequently, it is imperative for entities and professionals to conduct ML/TF risk assessments to understand the ML/TF risk to which they are exposed and prioritise and deploy resources in an efficient manner; placing a higher emphasis on areas that pose the most significant ML/TF risks. Pursuant to section 12, entities and professionals must conduct two types of risk assessments: (i) institutional risk assessments, and (ii) customer risk assessments. These risk assessments must be documented to support the allocation of compliance resources and application of appropriate mitigation measures, and to be able to appropriately supply risk assessment information to the Agency or Commission.*

***Institutional Risk Assessment***

***(ii)*** *Entities and professionals are required to assess the risk inherent in their business, taking into consideration relevant factors, i.e. their customers, countries*

*or geographical areas to which they are exposed, the products, services or transactions they offer and the delivery channels used to access customers. A business risk assessment should assist an entity or a professional to holistically understand the ML/TF risks to which it or he or she is exposed and identify the areas that should be proritised to combat ML/TF. An important part of the risk assessment is to identify the level of risks posed by each relevant factor and develop a risk rating. The risk rating may differ from person to person, for example [Low, Medium, High] or [Low, Medium Low, Medium, Medium High, High], however, the entity or professional must be able to identify the areas that pose higher risks and apply enhanced measures accordingly.*

***(iii)*** *In undertaking an assessment of its business risk, an entity and a professional should consider the following in relation to each relevant risk factor:*

***(A)*** *<u>Customer risk:</u>*
*This requires an overall assessment of the risks posed by customers and requires an entity or a professional to consider the risk profiles of its customer base and determine the extent to which the entity's or professional's customer base consists of higher risk customers. This overall assessment is based on the individual customer risk assessments that must be conducted in accordance with section 12(1)(b) of this Code. Paragraphs (iv) to (vi) below and the Explanation to section 19 outline considerations that should be made in conducting customer risk assessments.*

***(B)*** *<u>Country risk:</u>*
*This examines the extent to which an entity or professional's business is exposed to ML/TF risks based on the countries to which it interacts, whether directly or via customers. The aim is to understand the level of interaction an entity or professional has with countries that pose a higher risk of ML/TF. An entity or professional is considered to interact with a country, where*

- *it operates or engages in business, in, from within or with a country, including the Virgin Islands;*
- *it has customers (including beneficial owners) that are based, operate, or have personal or business links in the country;*
- *its customers receive funds from or transmit funds to the country; and*
- *its customers' funds were generated for use in the business relationship or one-off transaction in the country.*

*In assessing the ML/TF risks of the countries to which it is exposed, an entity and a professional should give due consideration to*

- *the effectiveness of the country's regime as identified by credible sources, such as the FATF, CFATF, IMF, GIFCS, etc.;*
- *whether the country is either considered or identified as a high risk country (including a country identified as having higher risk by the FATF or CFATF);*
- *whether the country is subject to sanctions, embargos or similar measures issued (e.g., sanctions imposed by the UNSC or the UK);*
- *whether the country or geographic area has been identified by reliable and credible sources (such as the FATF, CFATF, IMF, GIFCS, etc.) as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within the country;*
- *whether the country or geographic area has been identified by reliable and credible sources (such as the FATF, CFATF, IMF, GIFCS, etc.) as having high levels of corruption; and*
- *the level of criminal conduct related to ML/TF within the country.*

***(C)*** *<u>Products, Services and Transactions Risk</u>*
*This is an assessment of the extent to which the products, services and/or transactions offered can be exploited for ML/TF purposes. Entities and professionals should consider*

- *the nature, scale and diversity of its business' products and services;*
- *the complexity of each of the products and services offered;*
- *whether products and services include new technologies;*
- *the volume and size of its transactions (as it relates to each type of transaction available);*
- *whether the characteristics of products, services and transactions facilitate anonymity of customers, layers of opacity, or can readily transcend international borders (this latter category would include online banking facilities, stored value cards, international wire transfers, private investment companies and trusts);*
- *the extent to which a product, service or transaction may be susceptible to an unknown third party to conduct business via another person;*
- *the extent to which certain transactions involve multiple persons and jurisdictions;*

- *the extent to which third party payments can be accepted; and*
- *whether transactions are more cash-based.*

***(D)*** *Delivery Channels Risk*

*This relates to the manner in which products and services are offered to a customer and an assessment of the extent that these mediums can be exploited by customers or other third parties for ML/TF purposes. The assessment should consider the extent to which the entity or professional*

- *receives customers on a face-to-face basis;*
- *receives customers on a non-face to face basis, for example:*
  - *via telephone or online interaction;*
  - *via an agent or intermediary;*
  - *via introduction from a third party; or*
  - *via digital or electronic means.*

*For assessing the risks associated with non-face to face business, the entity or professional should consider*

- *Where establishing relationships over telephone or email interaction, an entity or a professional*
  - *the possibility that an applicant for business or customer may be able to impersonate another person; and*
  - *the extent to which an applicant for business or customer may provide falsified documentation in support of his or her application;*
- *Where using agents, intermediaries or introductions from third parties*
  - *the country in which the agents, intermediaries or third parties are incorporated or operate and the level of ML/TF risks posed by that country;*
  - *whether the agents, intermediaries or third parties are subject to some form of AML/CFT oversight;*
  - *whether a third party making introductions maintains relevant CDD information and documentation in accordance with the terms of the third party agreements and as required pursuant to sections 31 to 31B of this Code ; and*
  - *whether agents or intermediaries are monitored to ensure adequate CDD measures are being undertaken when attracting clients; and*

- *In the case of use of digital or electronic means for the establishment of a business relationship or conduct of transactions*
    - *the extent to which the use of digital or electronic means exposes the entity or professional to cyber-attacks and security breaches and the consequent possibility of stolen data and identity fraud;*
    - *whether the entity or professional has measures in place to adequately and appropriately protect itself or him or her from cyberattacks and security breaches posed by use of the digital or electronic means; and*
    - *whether there are unknown vulnerabilities due to the novelty of the digital or electronic means being utilised.*

***(E)*** *<u>Other Risk Factors</u> that an entity or a professional should consider in determining the ML/TF risks posed to its or his or her business are*

- *the nature, scale and quality of available ML/TF risk management resources, including appropriately qualified staff with access to ongoing AML/CFT training and development;*
- *the level of AML/CFT breaches identified on an ongoing basis;*
- *the results of any internal compliance assessments or internal audits; and*
- *any regulatory assessments and findings, including onsite inspections and desk-based reviews.*

*In addition, where applicable, an entity or professional should also consider the ML/TF risks emanating from other third-parties with which it engages; for instance service providers, product suppliers, affiliates, contractors, consultants and advisors, etc.*

***(iv)*** *Entities and professionals must put systems and controls in place to ensure that business risk assessments are kept up to date. This may be achieved, for example, by*

- *setting a timeline on which the next risk assessment update is to take place, to ensure any changes in risks are captured;*
- *ensuring that emerging risks, increase in existing risks, and changes in threats and vulnerabilities as identified by credible sources are accounted for within a set timeline; and*
- *carefully recording issues throughout the year that could have a bearing on risk assessments, such as:*
    - *internal suspicious transactions;*

- *compliance failures;*
- *intelligence from front office staff; or*
- *findings from internal audit function.*

*Notwithstanding the above, an entity or a professional's institutional risk assessment should be updated and reviewed at least once a year.*

***Customer Risk assessment***

***(v)*** *A significant portion of an entity's or a professional's ability to manage and mitigate its or his or her ML/TF risks is through the management of its or his or her relationships and interactions with customers. As such it is vital for entities and professionals to assess the ML/TF risks associated with each applicant for business or customer to determine the level of controls and mitigation measures that must be implemented for each customer. The assessment conducted at the initial stage of the CDD process would determine the extent of CDD measures to be applied. This means that the amount and type of information obtained, and the extent to which this information is verified, should be increased where the ML/TF risks associated with the applicant for business or customer are higher. CDD may also be simplified, but not completely excluded, where the associated ML/TF risks are lower, as may be allowed in accordance with the provisions of the Anti-money Laundering Regulations and this Code.*

***(vi)*** *Based on a holistic view of the information obtained in relation to each customer, an entity's or a professional's customer risk rating must determine the level and type of ongoing monitoring (including ongoing CDD and transaction monitoring) applied to a customer. The risk assessment would also support the entity's or professional's decision on whether to enter into, continue or terminate, a business relationship; or complete or reject a transaction. As a customer's risk profile may change over time, entities and professionals should review and update the risk assessment of a customer on an ongoing basis, more frequently for higher risk customers (at least once a year for higher risk customers).*

***(vii)*** *Entities and professionals should adopt a risk-based approach in the design and implementation of their customer risk assessment framework. The complexity of the framework should be commensurate with the nature and size of the entity's or professional's business and based on the results of the ML/TF risk assessment of its or his or her business. The customer risk assessment framework should include risk factors such as; risks associated with the customer's business or activity, risks associated with the customer's reputation, the customer's geographic exposure and delivery channel risk factors. These are primarily based on information collected during the CDD process. The customer risk assessment process is expounded upon in the Explanation to section 19 of this Code.*

***New Products, Practices, Delivery Mechanisms and Technological Developments***

***(viii)*** *Entities and professionals offer new products to provide customers with a greater variety of options and create new opportunities and financial solutions.*

*Similarly, entities and professionals may introduce new delivery channels, enhance existing products using technological developments and implement changes in business practices to enhance accessibility, convenience and efficiency in providing products and services to their customers, facilitate ease of doing business, and reduce the occurrence of human error. Some of these can include, for example:*

- *Offering transactions via the internet or digital means;*
- *Mobile payments;*
- *Digital or electronic storage;*
- *Electronic verification of documentation;*
- *Electronic ongoing monitoring mechanisms;*
- *Digital or electronic onboarding mechanisms; and*
- *Facilitation of virtual assets transactions.*

***(ix)*** *Notwithstanding the benefits of introducing new products, technology and business practices, they may present new vulnerabilities in facilitating ML/TF. Subsection (3) therefore obligates an entity or a professional to identify the ML/TF risks associated with new products, new technologies and new business practices, prior to introducing and implementing them, and have mechanisms in place to manage and mitigate the ML/TF risks identified.*

***(x)*** *In assessing the ML/TF risks associated in these particular circumstances, an entity or a professional should consider, amongst other factors, whether a new product, technology or practice*

- *makes its or his or her business more vulnerable to theft, cybercrime, data and security breaches and other fraudulent activities;*
- *inhibits on the entity's or professional's ability to monitor customer transactions and activities;*
- *creates opportunities for establishing business relationships in a way that circumvents appropriate identification procedures as required under this Code;*
- *can be appropriately understood by employees so as not to create unintended facilitation of ML/TF and other nefarious activities and breaches of legislation;*
- *may facilitate the conduct of transactions with anonymity; or*
- *may facilitate the operation of business in breach of AML/CFT or any other relevant legislation.*

***(xi)*** *Entities and professionals should also review other relevant types of information to understand the types of risks posed by new products and services, business practices, delivery channels and technological developments, including*

*information on how they may be involved in existing and emerging ML/TF schemes and exploited for ML/TF purposes. Such information can be sourced from, for example, risks assessment and/or typology reports issued by any competent authority with responsibility for AML/CFT matters, both locally and internationally, warnings issued by local, regional or international regulatory authorities and law enforcement agencies and reports issued by international standard setting bodies such as the FATF, CFATF, IMF, Basel Committee, GIFCS, IOSCO and IAIS.*

***(xii)*** *Once relevant risks have been identified, an entity or a professional must ensure, prior to implementing the new products, services, business practices or delivery channels, that it or he or she has appropriate measures to mitigate against the ML/TF risks identified, when they are implemented. This should include ensuring that relevant policies and procedures are updated to account for any new potential risks to the business of the entity or professional.*

***(xiii)*** *Risk assessments of new products, services, business practices, technological developments and delivery channels should feed into the institutional risk assessment as required under subsection (1) and kept-up-to date as required.*

***Sources of Information***

***(xiv)*** *There are a wide variety of sources that an entity or a professional can utilise in obtaining information to form the basis of its or his or her risk assessments, in addition to information obtained during the customer due diligence process. These may include*

- *any risk assessments on ML/TF (including sectoral assessments) undertaken for the Virgin Islands by any authority with responsibilities in relation to the jurisdiction's AML/CFT regime;*
- *guidance, circulars and other communication from the Agency, the Commission or any other authority with powers relating to ML/TF;*
- *reports issued by the Agency and law enforcement agencies;*
- *National Risk Assessments or other similar types of assessment of other jurisdictions in which the entity or professional conducts business or its or his or her customers are located or conducts business;*
- *guidance issued by FATF, IMF or any other international standard setting body;*
- *assessment reports of compliance with international standards issued by international standard setting bodies such as FATF, CFATF, IMF, Global Forum;*
- *public Statements issued by the FATF and CFATF and other FSRBs;*
- *UNSC and UK Sanctions listings;*

- *typologies Reports issued by domestic and international competent authorities, financial intelligence units or law enforcement agencies, or international standard setting bodies;*
- *information from industry associations; and*
- *the entity's or professional's own knowledge of its or his or her industry.**]**"*

---

**Section 13 amended**

**15.** Section 13 of the principal Code of Practice is amended

(a) in subsection (1), by deleting the words "money laundering and terrorist financing" and substituting the words "money laundering, terrorist financing or proliferation financing";

(b) in subsection (2)

(i) by deleting paragraph (b) and substituting the following paragraph

"(b) ensure compliance with the reporting requirements to the Agency pursuant to the provisions of the Drug Trafficking Offences Act, Revised Edition 2020, Proceeds of Criminal Conduct Act, Revised Edition 2020, Counter-Terrorism Act, No. 33 of 2021, Proliferation Financing (Prohibition) Act, No. 20 of 2021 and any other enactment relating to money laundering, terrorist financing or proliferation financing;";

(ii) in paragraph (d)(ii), by deleting the words, "Steering Committee" and substituting the word, "Agency", and inserting after the words "financing of terrorist", the words "or proliferation";

(iii) in paragraph (d)(iii), by deleting the words "Steering Committee" and substituting the word "Agency"; and

(iv) in paragraph (g), by deleting the words, "money laundering or terrorist financing" and substituting the words, "money laundering, terrorist financing or proliferation financing"; and

(c) by revoking subsection (3).

---

*The Explanation to section 13 of the principal Code of Practice is amended*

*(a) in paragraph (i)*

*(i) by deleting the words, "money laundering and terrorist financing" and substituting the words, "money laundering, terrorist financing and proliferation financing"; and*

*(ii) by inserting after the words, "the reporting requirements under the DTOA, PCCA", the words ", PFPA, CTA";*

*(b) in paragraph (ii), by deleting the words, "money laundering or terrorist financing" and substituting the words, "money laundering, terrorist financing or proliferation financing"; and*

*(c) in paragraph (vi), by deleting in the first sentence, the words "Anti-money Laundering Reporting Officer" and substituting the words "Money Laundering Reporting Officer".*

---

**Section 14 amended**

**16.** Section 14(2) of the principal Code of Practice is amended by deleting the words, "and terrorist financing" in paragraphs (a), (c), (d), (e), (f) and (g) and substituting the words, ", terrorist financing and proliferation financing".

---

*The Explanation to section 14 of the principal Code of Practice is amended in paragraph (i) by deleting the words, "and terrorist financing" and respectively substituting the words, ", terrorist financing and proliferation financing".*

---

**Section 15 amended**

**17.** Section 15 of the principal Code of Practice is amended

(a) in subsection (1)(a), by deleting the words, "anti-money laundering and terrorist financing" and substituting the words, "anti-money laundering, terrorist financing and proliferation financing"; and

(b) by deleting subsection (3) and substituting the following subsection

"(3) Where an employee fails to comply with the requirements of this section, he or she commits an offence and is liable to be proceeded against under section 27 (4) of the Act.".

**Section 16 amended**

**18.** Section 16 of the principal Code of Practice is amended

(a) in subsection (1), by inserting after the words, "An entity" the words, "or a professional";

(b) in subsection (2), by deleting paragraph (b) and substituting the following paragraph

"(b) understands the business of the entity or professional and is well-versed in the different types of transactions and products which the entity or professional handles and which may give rise to opportunities for money laundering, terrorist financing or proliferation financing."; and

(c) in subsection (3)

(i) in the opening paragraph, by inserting after the words, "An entity" the words, "or a professional";

(ii) in paragraph (c), by deleting the words money laundering and terrorist financing" and substituting the words "money laundering, terrorist financing and proliferation financing"; and

(iii) in paragraph (d), by deleting the words, "notify the Agency or the Commission in the case of a regulated entity" and substituting the words, "notify the Agency and, in the case of an entity or a professional regulated by the Commission, also notify the Commission".

---

*The Explanation to section 16 of the principal Code of Practice is amended*

*(a) in paragraph (i)*

*(i) in the first sentence, by inserting after the word, "entity's" wherever it appears, the words "or professional's"; and*

*(ii) by deleting the second sentence and substituting the following sentence*

*"He or she effectively functions as the liaison between the entity or professional and the Agency with respect to the entity's or professional's compliance with established AML/CFT laws, policies and procedures.";*

*(b) in paragraph (ii), by deleting the third sentence and substituting the following sentence*

*"He or she must be given unrestricted access to the entity's or professional's records and board of directors or equivalent body (such as in a partnership), or the professional (where applicable) in order to ensure a balanced and objective assessment of suspicious transactions or of customers.";*

*(c) in paragraph (iii), by inserting after the words, "the reporting requirements under the DTOA, PCCA, the 2002 Order", the words ", PFPA, CTA";*

*(d) in paragraph (iv), by deleting the words, "money laundering or terrorist financing" and substituting the words, "money laundering, terrorist financing or proliferation financing";*

*(e) by deleting paragraph (v) and substituting the following paragraph*

*"**(v)** While a Reporting Officer may be tasked with other responsibilities within an entity or in relation to a professional, as part of his or her official assignments, it is important that such responsibilities are not so onerous as to hinder the Reporting Officer from effectively performing his or her statutory functions. It is the duty of a Reporting Officer who finds himself or herself in such a situation to discuss the matter with the entity's senior management or the professional (where applicable) to seek an acceptable resolution that enables an effective performance of his or her reporting functions. Such*

*discussions and the outcome thereof must be documented by the Reporting Officer and where there is no acceptable resolution the Reporting Officer must immediately inform the Agency or the Commission, as the supervisor of the entity or professional. Following an assessment by the Agency or the Commission, the entity may be required to scale back the Reporting Officer's other official responsibilities or seek to appoint another person as the entity's or professional's Reporting Officer."*

*(f) by deleting paragraph (vi);*

*(g) by deleting paragraph (vii) and substituting the following paragraph*

*"**(vii)** The AMLR and this Code set out the internal reporting obligations of entities and professionals with respect to suspicious transactions and the appointment of a Reporting Officer. However, in the case of mutual funds and private investment funds, it is recognised that there are instances where fund administrators undertake customer due diligence, the issuance and administration of subscriptions and redemptions on behalf of a fund and would be in a better position to identify suspicious transactions and activities. In such a case, the mutual fund or private investment fund may appoint the Reporting Officer of the mutual fund's or private investment fund's administrator, or such other qualified person within the mutual fund's or private investment fund's administrator, as its own Reporting Officer."; and*

*(h) by inserting after paragraph (vii), the following new paragraph*

*"**(viii)** Where a professional does not appoint a person as its Reporting Officer, the professional is assumed to perform the role of the Reporting Officer in accordance with the Anti-money Laundering Regulations and this Code."*

---

**Section 17 amended**

**19.** Section 17 of the principal Code of Practice is amended by revoking subsection (1) and substituting the following subsection

"(1) A Reporting Officer shall promptly make a report to the Agency of every suspicious customer or transaction relevant to money laundering, terrorist financing or proliferation financing relating to his or her entity or professional and such report may

(a) be made in such form as prescribed by the Agency and in compliance with the requirements of section 55; and

(b) be sent electronically by a secure reporting system as required by the Agency."

**Section 18 amended**

**20.** Section 18 of the principal Code of Practice is amended

(a) in subsection (1)

(i) by deleting paragraph (a) and substituting the following paragraph

"(a) report a suspicious activity or transaction to a Reporting Officer in a form established by the entity or professional as part of its or his or her internal control system as the Commission or the Agency may approve in writing, provided that the report complies with the requirements of section 55; and"; and

(ii) in paragraph (b), by inserting at the end of the paragraph, before the full-stop, the words, "(such as name, date of birth or date of incorporation or formation, and address)";

(b) in subsection (2), by inserting at the end of the subsection, before the full-stop, the words ", regardless of the amount of the transaction"; and

(c) in subsection (5), in the opening paragraph and in paragraph (a), by deleting the words "money laundering or terrorist financing" and substituting the words "money laundering, terrorist financing or proliferation financing".

---

*The Explanation to section 18 of the principal Code of Practice is amended*

*(a) in paragraph (i), by deleting the third and fourth sentences and substituting the following sentences*

*"Similar provision is made in respect of terrorist financing under the 2002 Order and the CTA and in respect of proliferation financing under the PFPA. This obligation applies to the entity or professional and any of its or his or her employees who possess the information in the circumstance described."; and*

*(b) by deleting paragraph (iii) and substituting the following paragraph*

***"(iii)** There may be circumstances where an applicant for business or a customer may be unwilling to provide or may simply fail to provide adequate information requested to verify his or her identity or, in the case of a legal person or legal arrangement, the identity of the beneficial owner, or information required to undertake CDD. As a result, the transaction may not be concluded or the business relationship may not be established. It is important in such a situation for the employee to record the fact of such an activity and the details of the person and the transaction concerned. Where the entity or professional turns away the applicant for business or customer, it must nevertheless record the essential information and transmit that to the Reporting Officer who must in turn inform the Agency if in his or her assessment the information substantiates a suspicion of money laundering, terrorist financing or proliferation financing. It should be noted, however, that it may not be in all cases that such a requirement comes into play: the employee dealing with the applicant for business must consider the nature, size and volume of the desired business relationship, the amount involved and source of the funds, whether or not the person is acting for himself or herself or on behalf of somebody else (legal or natural), the demeanour of the applicant for business, the risks involved and so on. It becomes a question of judgment as to whether the*

*relationship or transaction sought by the applicant for business or customer merits suspicion for reporting purposes; but in any case where a suspicion is held, it must be reported to the Reporting Officer. Yet there are also situations where an applicant for business or a professional may turn away before any essential information is recorded of or from him or her; in such a case the obligation provided under section 18 (2) will not apply."*

---

**Section 19 amended**

**21.** Section 19 of the principal Code of Practice is amended

(a) in subsection (1), by inserting after the words, "terrorist financing" the words, ", proliferation financing";

(b) in subsection (3)

(i) in paragraph (a), by deleting the words, "applicant for business, or the intended customer" and substituting the words, "applicant for business or customer";

(ii) by deleting paragraph (c) and substituting the following paragraph

"(c) to use reliable and independent source documents, data, information or evidence through such inquiry as is necessary to verify the identity of the applicant for business or customer, including the beneficial owner;";

(iii) in paragraph (d)

*(aa)* by deleting the words, "or the intended customer" and substituting the words, "or customer"; and

*(bb)* inserting the word "and" at the end of the paragraph;

(iv) by deleting paragraph (e); and

(v) by deleting paragraph (f) and substituting the following paragraph

"(f) to verify that a person who acts or purports to act on behalf of an applicant for business or a customer is so authorised and to identify and verify that person's identity.";

(c) in subsection (4)

(i) in the opening paragraph, by inserting after the word, "entity" the words, "or a professional";

(ii) in paragraph (b), by inserting after the word "entity", the word "or professional";

(iii) by inserting after paragraph (b), the following new paragraphs

"(b*a)* in the case of an entity or a professional providing a virtual assets service, when effecting a one-off transaction involving virtual assets valued at or above $1,000 or such lower threshold as the entity or professional may establish;

*(*b*b)* in the case of an entity or a professional licensed or registered pursuant to the Virgin Islands Gaming and Betting Control Act, No. 14 of 2020, when

effecting a one-off transaction involving funds of or above $3,000 or the equivalent in any other currency;"; and

(iv) in paragraph (c), by deleting the words, "money laundering or terrorist financing" and substituting the words, "money laundering, terrorist financing or proliferation financing";

(d) by inserting after subsection (4), the following new subsection

"(4A) Subject to subsection (4), in the case of a trust or a life insurance policy, an entity or a professional shall undertake customer due diligence measures on a beneficiary as soon as the beneficiary is identified or designated

(a) for a beneficiary that is identified as a specifically named natural person, legal person or legal arrangement, taking the name of the person, legal person or legal arrangement; and

(b) for a beneficiary that is designated by characteristics or by class, obtaining sufficient information concerning the beneficiary to satisfy the entity or professional that it or he or she will be able to establish the identity of the beneficiary at the time of the payout.";

(e) in subsection (5)

(i) by deleting the opening paragraph and substituting the following opening paragraph

"In circumstances where an applicant for business or a customer is the trustee of a trust or a legal person, customer due diligence measures to be undertaken by an entity or professional shall also include determining the following"

(ii) by deleting paragraph (c)(i) and substituting the following paragraph

"(i) where the trust forms part of an ownership structure involving other legal persons or legal arrangements, details of the structure, including any underlying legal persons or arrangements; and"; and

(iii) in paragraph (d), by inserting after the words, "the ownership", the words "and beneficial ownership";

(f) in subsection (6)

(i) by deleting the opening paragraph and substituting the following opening paragraph

"Adopting the risk-based approach, an entity or a professional may determine customers or transactions that it or he or she considers carry low risk in terms of the business relationship, and to make such a determination the entity or professional may take into account such factors as"

(ii) in paragraph (b), by deleting the words "and terrorist financing" and substituting the words ", terrorist financing and proliferation financing";

(iii) by deleting paragraph (g) and substituting the following paragraph

"(g) beneficial owners of pooled accounts held by non-financial businesses and professions if they are subject to anti-money laundering, terrorist financing or proliferation financing requirements and are subject to effective systems for monitoring and supervised for compliance with anti-money laundering, terrorist financing and proliferation financing requirements that are consistent with the FATF Recommendations;";

(iv) by deleting paragraph (h);

(v) by deleting paragraph (i) and substituting the following paragraph

"(i) in the case of a body corporate that is part of a group, the group is subject to and properly and adequately supervised for compliance with anti-money laundering, terrorist financing and proliferation financing requirements that are consistent with the FATF Recommendations; and"

(vi) by revoking paragraph (j) and substituting the following paragraph

"(j) the entity or professional considers, in all the circumstances of the customer, having regard to the entity's anti-money laundering, terrorist financing and proliferation financing obligations, pose a lower level of risk.";

(g) by deleting subsection (7) and substituting the following subsection

"(7) Where pursuant to subsection (6) an entity or a professional makes a determination that a customer poses low risk, having regard to the money laundering, terrorist financing and proliferation financing risks identified by a Virgin Islands' national risk assessment, or a risk assessment conducted by a competent authority, law enforcement agency or any other authority with responsibility relating to money laundering, terrorist financing and proliferation financing in the Virgin Islands, the entity or professional may simplify the customer due diligence measures as required under subsections (2), (3) and (4) (b).";

(h) by inserting after subsection (7), the following new subsections

"(8) Subsection (7) shall not apply where

(a) the entity or professional suspects money laundering, terrorist financing or proliferation financing; or

(b) a higher risk scenario applies.

(9) Where an entity or a professional suspects that a transaction relates to money laundering, terrorist financing or proliferation financing, and believes that performing customer due diligence will tip-off the applicant for business or customer, the entity or professional shall

(a) not conduct customer due diligence; and

(b) in lieu of conducting customer due diligence, file a suspicious transaction report with the Agency in accordance with section 30A of the Act and section 18 (1) herein."

*The Explanation to section 19 of the principal Code of Practice is deleted and substituted by the following Explanation*

***"[Explanation:***

***(i)*** *Customer due diligence (CDD) is a very useful mechanism to protect an entity or a professional (and by extension the Territory) from the risks associated with money laundering, terrorist financing, proliferation financing and other financial crimes. CDD also promotes transparency in business transactions and thus reduces the possibilities of identity theft. An entity or a professional that appropriately develops and applies AML/CFT systems and controls reduces the chances of itself, or himself or herself from falling afoul of the law and the consequences that flow from criminal proceedings. An effectively applied CDD process also helps to build a close relationship between an entity or a professional and the regulator and law enforcement generally which helps in keeping criminals at bay.*

***(ii)*** *An entity or a professional must establish an appropriate record in respect of its or his or her dealings with applicants for business and customers. The aim of CDD is to*

- *get to know the applicant for business or customer (including any beneficial owners) and ensure that they are who they claim to be;*
- *understand what to expect from doing business with the applicant for business or customer;*
- *determine the level of ML/TF risks that an applicant for business or customer poses; and*
- *implement measures to manage and mitigate the level of ML/TF risk posed by the applicant for business or customer.*

***(iii)*** *Customer due diligence must be undertaken initially (i.e. at the point of establishing a business relationship or effecting a one-off transaction above the required thresholds) and on an ongoing basis. Requirements for ongoing customer due diligence are outlined in section 21 of this Code.*

***(iv)*** *Initial Customer Due diligence consists of the following key steps—*

*(A)* ***Identifying the Applicant for Business or Customer***
*This entails gathering and recording information about the applicant for business or customer to establish who the applicant for business or customer is. Information that must be gathered and recorded differs based on whether the customer is an individual, a legal person, or a legal arrangement. Where the applicant for business or customer is a legal person or legal arrangement, an entity or a professional is required to understand the ownership and*

*control structure of the legal person or legal arrangement, by also identifying the persons responsible for performing managerial functions and directors (where applicable), as well as any beneficial owners of the applicant for business or customer. The requirements for identifying varying types of applicants for business or customers are outlined in sections 23 to 28 of this Code.*

*(B)* ***Verifying the Applicant for Business or Customer's Identity***
*This entails gathering evidence, via reliable and independent information, data and/or documentation, to confirm that a customer is who he or she or it is and authenticate that the identification information provided is true and accurate. Verification of an applicant for business' or customer's identity also reduces the risk of impersonation and fraud by persons imitating others.*

*Sections 23 to 28 outline the requirements relating to verification of customer identity and Explanation to those sections provide further guidance accordingly.*

*(C)* ***Obtaining details of the purpose or intended nature of the business relationship or transaction***
*This requires an entity or a professional to establish the reason why a customer is seeking to establish a business relationship or conduct a one-off transaction. For example, establishing a personal bank account or establishing a business account to facilitate international business transactions; or establishing a life insurance policy for the benefit of a close relative.*

*(D)* ***Understanding the applicant for business or customer and their circumstances***
*This requires an entity or a professional to obtain information on the applicant for business' or customer's business and activities in order to create a base profile of the types and levels of activities that would be undertaken by that customer throughout the business relationship. This aids the entity or professional in identifying any deviations in behaviour (as outlined in section 21 of this Code). In understanding the applicant for business or customer and its or his or her circumstances, the following relevant information should be considered*

- *nature and details of occupation or employment;*
- *nature and details of the applicant for business' or customer's business activities;*
- *assets held or managed or to be held or managed (in the case of an applicant for business or customer that is a trust or holding company);*

- *the anticipated level and nature of activity to be undertaken throughout the business relationship;*
- *the applicant for business' or customer's source of funds, i.e. where the funds or assets that will be used for the business relationship or transaction were derived (e.g. income, business profits, investments, dividends, inheritance, property sale, business sale, etc.);*
- *the applicant for business' or customer's source of wealth, i.e. how the customer derived his or her or its wealth, particularly in higher risk scenarios (e.g. income, business profits, investments, dividends; inheritance, property sale, business sale, etc.) and level of wealth (i.e. the total value of a applicant for business' or customer's wealth);*
- *the rationale behind an ownership structure where the applicant for business or customer has a complex ownership or control structure;*
- *the countries with which the applicant for business or customer intends to engage or have connections;*
- *whether the applicant for business or customer has a criminal record or is a known associate of criminals or criminal organisations; and*
- *whether the applicant for business or customer is a PEP.*

*Depending on the level or risk posed by the applicant for business or customer, in addition to the information that may be gathered from posing questions to the applicant, an entity or a professional may require independent information or documentation to verify an applicant for business' or customer's circumstances. That is to say, an entity or a professional may require more in-depth information and application of higher levels of scrutiny or verification of information for an applicant for business or customer that poses higher ML/TF risks. The following are some examples of some sources that an entity or professional may utilise—*

- *an individual's pay slips;*
- *an employment letter on behalf of a customer;*
- *review of a customer's bank statements;*
- *review of a customer's business website or brochure;*
- *a customer's business plan, estimated financial projections, etc.*

- *a customer's trade licence;*
- *copies of contracts, or draft contracts relating to the activities to be undertaken;*
- *review of business databases or regulatory website (in the case of a regulated entity);*
- *a legal person's or a legal arrangement's financial statements;*
- *review of Register of Interests, Income Declarations (in relation to PEPs);*
- *evidence of source of wealth (e.g. extract of inheritance, bill of sale or receipt from sale of property, copies of trust deeds, etc);*
- *review of internet and news media; and*
- *review of third-party search sites and internationally accepted screening databases.*

*It is important to note that the sources above are examples and may not necessarily be applied for all customers. Determination of sources required should be based on customer risks as outlined in paragraphs (vi) to (viii) below.*

***Acting or Purporting to Act on behalf of an Applicant for Business or a Customer***

***(v)*** *An entity or a professional is required to apply customer due diligence measures on a person who is acting or purporting to act on behalf of an applicant for business or a customer, as if he or she were the actual applicant for business or customer. This applies whether the applicant for business or customer is an individual (e.g. an individual applicant for business or customer with assets under a power of attorney), or a legal person or legal arrangement (e.g. a company utilising an agent to establish a business relationship, a legal person's signatory, or an agent of a settlor establishing a trust). Where a person acts or purports to act on behalf of an applicant for business or a customer, the entity or professional must ensure that it or he or she obtains evidence of the authority of the person acting or purporting to act on behalf of the customer and identify and verify the identity of that person. Examples of evidence of authority may include, as applicable—*

- *a copy of the original power of attorney or equivalent instrument;*
- *board resolution appointing a signatory to a legal person;*
- *authorised signatory letter; and*
- *agency services agreement.*

*In relation to a signatory of a legal person or legal arrangement, an entity or a professional should also, in its or his or her CDD process, seek to establish the true*

*nature of the relationship between the signatory and the directors or beneficial owners of the legal person or legal arrangement and determine the level of ML/TF risk that may exist from this relationship. This is because there is a money laundering tactic whereby persons use signatories that are not of directors, managers, partners or employees of the legal persons or legal arrangements, to launder proceeds via the legal entity. As such, the entity or professional should verify whether there is any other existing relationship between the signatories and the directors or beneficial owners of the legal person or legal arrangement. The level of CDD measures imposed on a signatory will depend on the level of ML/TF risk posed by the relationship.*

***Risk-sensitive Nature of CDD***

***(vi)*** *CDD should be applied on a risk sensitive basis, such that the level of information and verification required for an applicant for business or a customer is dependent on the level of ML/TF risk posed by that applicant for business or customer, based on the information received in the initial CDD process. This therefore requires an entity or a professional to make an initial risk assessment of, and form a risk rating for, each applicant for business or customer. The initial customer risk assessment undertaken should provide an entity or a professional with an informed determination of the extent of CDD information to be sought, how and the extent to which such information is to be verified. In addition, a customer risk assessment is intended to assist an entity or a professional in determining how a particular applicant for business or customer exposes the entity or professional to ML/TF risk and enable the entity or professional to apply proportionate measures to that applicant for business or customer in order to effectively mitigate against the risks the customer poses. In assessing risks posed by an applicant for business or a customer, the following should be taken into account*

***(A) Applicant's or Customer's Business or Activity:***

*An entity or a professional must determine whether the nature, size and complexity of an applicant's or a customer's business or activities (including its beneficial owner's activities) pose higher ML/TF risk or lower ML/TF risk. In making this determination, an entity or a professional should consider (as applicable) whether the customer (including its or his or her beneficial owner)*

- *utilises products, services or transactions that pose a higher ML/TF risk (as determined in the entity's or professional's institutional risk assessment);*
- *utilises new products, services or transactions, or existing products, services with new technologies or delivery channels that pose higher ML/TF risks (as determined in accordance with section 12(3) of this Code);*

- *is or will be involved in high frequency, high value transactions or complex transactions;*
- *has political connections, for example:*
  - *the customer or its or his or her beneficial owner is a PEP or has other relevant links to PEPs;*
  - *one or more of the customer's directors, senior management or equivalent, are PEPs and if so, these PEPs exercise significant control over the customer or beneficial owner;*
- *has links to sectors that are commonly associated with higher risks of corruption;*
- *has links to sectors that are associated with higher ML/ TF risk;*
- *has cash intensive businesses, including those that generate significant amounts of cash or undertake large cash transactions, money service businesses (examples may include money transfer agents, bureaux de change and money transfer or remittance facilities), casinos, betting and other gambling or game related activities;*
- *is a public body or government owned entity from a country with known higher levels of corruption;*
- *is a recognised stock exchange under the Regulatory Code (Recognised Exchanges) Notice that is subject to enforceable disclosure requirements;*
- *is a legal person with nominee shareholders or has the ability to issue bearer shares;*
- *is a financial institution or DNFBP acting on its own account from a country with an effective AML/CFT regime; or*
- *has a background that is consistent with what the entity or professional knows about the applicant for business or customer. For example:*
  - *its former, current or planned business activity;*
  - *the turnover of the business;*
  - *its source of funds; and*
  - *the customer's or beneficial owner's source of wealth.*

***(B) Applicant's or Customer's Reputation***

*An entity or a professional should consider the applicant's or customer's reputation, insofar as it relates to financial crime risk. This may be achieved by assessing whether*

- *there are adverse media reports or other relevant information sources about the applicant for business or customer and/or its beneficial owner(s) providing credible allegations against the customer or beneficial owner on ML/TF, other financial crimes and/or predicate*

*offences (entities and professionals should determine the credibility of allegations based, inter alia, on the quality and independence of the source data and the persistence of reporting of these allegations);*

- *the applicant for business or customer (or their beneficial owner) has been criminally charged and/or convicted for ML/TF, other financial crimes and/or predicate offences;*
- *the applicant for business or customer, beneficial owner or anyone publicly known to closely associate with the applicant or customer has currently, or had in the past, been listed on sanctions lists and their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing or other crime-related activity;*
- *the applicant for business or customer (or their beneficial owner) has been the subject of a suspicious transactions report by the entity or professional in the past; and*
- *the entity or professional has in-house information about the applicant's or customer's and/or their beneficial owner's integrity (e.g. information obtained over the course of an existing business relationship).*

***(C)*** ***<u>Applicant's or Customer's Geographic Exposure</u>***

*The customer risk assessment must consider the countries to which the applicant for business or customer has exposure and the extent that the customer is exposed to countries that have a higher ML/TF risk (based on country risk factors considered in paragraph (iii) (B) in the Explanation to section 12). An applicant for business or a customer is exposed to a country if*

- *the applicant or customer and/or its beneficial owners are resident or established in that country;*
- *the applicant or customer conducts business in that country;*
- *the applicant or customer receives funds from or transmits funds to that country; or*
- *the funds used or to be used in the business relationship or one-off transaction were derived from that country.*

***(D)*** ***<u>The Delivery Channels</u>***

*An entity or a professional must consider the ML/TF risks posed by the delivery channels by which its or his or her products or services are distributed to the applicant for business or customer (based on risk factors considered in institutional risk assessment on delivery channels as outlined in paragraph (iii) (D) in the Explanation to section 12).*

***(vii)*** *In implementing an appropriate risk-based approach to CDD, an entity or a professional must determine the level and extent of information and verification of information that must be undertaken for CDD. This is where the entity or professional should consider the evidence of identification required and the sources of verification that would apply for a standard relationship or engagement with an applicant or a customer. The RBA must consequently also prescribe the measures (additional to CDD) that must be employed for enhanced CDD of higher risk applicants or customers. This may include requiring more than standard information and documentation and applying more and/or stricter means of verification to understand who the applicant or customer is and the nature of activities he or she or it wishes to engage in with the entity or professional. Further details on enhanced customer due diligence are outlined in section 20 of this Code. The RBA should also outline the reduced simplified CDD measures that would be applied for applicants or customers that have been identified as low risk, in consideration of the ML/TF risk assessments of the Virgin Islands conducted by any person with the relevant authority outlined in subsection (7). Notwithstanding the simplified measures, an entity or a professional must ensure that it or he or she has adequately identified and verified the identity of its or his or her applicant or customer (including beneficial owners) and has sufficient information documented to support the determination of an applicant's or a customer's low risk.*

***(viii)*** *It must be remembered that not all customers within a risk category are the same, as they may pose different types of risks (e.g. higher risks based on geographic exposure, or higher risk based on business activities). Consequently, the level and type of CDD, enhanced CDD or simplified CDD applied for an applicant for business or a customer should take into account the particular circumstances of each customer, on a case-by-case basis.*

***(ix)*** *It should be appreciated that identifying an applicant for business or a customer as high risk does not necessarily mean that the applicant for business or customer is a money launderer or is involved in terrorist financing, proliferation financing or other criminal financial activity. Conversely, identifying an applicant for business or customer carrying a lower risk of involvement in money laundering, terrorist financing, proliferation financing or other financial crime does not necessarily mean that the applicant for business or customer cannot be a money launderer or engaged in terrorist financing, proliferation financing or other criminal financial activity. In addition, where a customer engages in occasional financial transactions below the established financial threshold but in a series that appear to be linked, serious consideration should be given to the level of ML/TF risks posed by that customer in the series of transactions. It must always be remembered that those bent on abusing the legitimate facilities offered by financial institutions in particular go to great lengths to identify 'loopholes' in the internal control systems of the institution. It is therefore advisable that even in cases of known identified low risk customers, appropriate CDD measures are applied to transactions relating to them. In any case, simplified CDD measures must not be applied where a suspicion of money laundering, terrorist financing or proliferation*

*financing or specific higher risk scenario exists. Where there is a suspicion of money laundering, terrorist financing or proliferation financing, this must be reported immediately in accordance with the reporting requirements of the DTOA, PCCA, PFPA, CTA, AMLR, this Code or any other enactment (as applicable).]"*

---

**Section 20 amended**

**22.** Section 20 of the principal Code of Practice is amended

(a) in subsection (1), by deleting the words "prevent money laundering, terrorist financing, and other financial crime" and substituting the words "prevent the higher risk of money laundering, terrorist financing, proliferation financing and other financial crime that have been identified by the entity or professional";

(b) in subsection (2), by deleting the words "is determined to be a higher risk applicant for business or customer, or transaction" and substituting the words "presents a higher risk";

(c) in subsection (3)(b), by inserting after the word, "processes" the words ", that present a higher risk";

(d) in subsection (4)

(i) in paragraph (a), by inserting before the words "politically exposed person", the word "foreign";

(ii) by inserting after paragraph (a), the following new paragraph

"(a*a)* a domestic PEP or an international organisation PEP that presents a higher risk;";

(iii) in paragraph (b) by deleting the word, "or" at the end of the paragraph;

(iv) by deleting paragraph (c) and substituting the following paragraph

"(c) a person, business relationship or transaction located in or from a country that is either considered or identified as a high-risk country (including a country identified as having higher risk by the FATF) or that has international sanctions, embargos or other restrictions imposed on it; or";

(v) by inserting after paragraph (c), the following new paragraph

"(d) any other situation that may present a higher risk of money laundering, terrorist financing or proliferation financing;"; and

(vi) in the closing paragraph, by inserting after the words, "enhanced due diligence" the words, ", proportionate to the risks,"; and

(e) by inserting after subsection (4), the following new subsections

"(5) In the case of a trust or life insurance policy, an entity or a professional shall consider the beneficiary of the trust or life insurance policy as a relevant risk factor in determining whether enhanced customer due diligence measures are required.

(6) Where an entity or a professional determines that a beneficiary of a life insurance policy that is a legal person presents a higher risk, the entity or professional shall perform enhanced customer due diligence at or before the time of pay-out, including reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, where applicable."

---

*The Explanation to section 20 of the principal Code of Practice is deleted and substituted by the following new Explanation:*

***"[Explanation***

***(i)*** *Enhanced customer due diligence (ECDD) must be viewed as an additional precautionary measure designed to assist in truly identifying an applicant for business or customer (including a beneficial owner) and verifying the information relating to it or him or her and ensuring that the risks that may be associated with the customer are minimal or manageable; this is in addition to ensuring that the source of funds or wealth is legitimate. These additional measures are relative to what an entity or a professional is already required to undertake for CDD. However, the type of ECDD applied in high-risk scenarios will differ on a case-by-case basis, taking into account the higher ML/TF risk, the particular circumstances of the customer, and the measures that will enable them to manage and mitigate the higher ML/TF risks presented.*

***(ii)*** *Examples of ECDD measures that could be applied for high-risk business relationships include*

- *obtaining additional information on the applicant for business or customer (e.g. volume of assets, information available through public databases, internet, etc.);*
- *requiring additional information from the applicant for business or customer to gain a deeper understanding of the applicant's or customer's activities;*
- *undertaking further research, where considered necessary, in order to understand the background of the applicant for business or customer and its or his or her business and verify such information;*
- *obtaining additional information on the source of funds or source of wealth of the applicant for business or customer and verifying this information (i.e. obtaining more than standard information on source of funds and source of wealth, including requiring evidentiary documentation to confirm the customer's source of funds and wealth, and verifying information provided against publicly available information sources);*
- *obtaining the approval of senior management to commence or continue the business relationship with a higher risk applicant for business or customer;*

- *requiring additional information before effecting transactions above an established threshold amount;*
- *requiring senior management sign-off when engaging in transactions with a higher risk applicant for business or customer;*
- *requiring the first payment to be carried out through an account in the applicant for business' or customer's name with a bank or similar financial institution subject to anti-money laundering, terrorist financing and proliferation financing requirements that are consistent with the FATF Recommendations and are supervised for compliance with such requirements; and*
- *conducting enhanced monitoring of the business relationship (e.g. increasing the number and timing of controls applied, obtaining information on the reasons for a particular transaction, selecting patterns of transactions that need further examination).*

***(iii)*** *Where an existing customer is subsequently assessed by a customer risk assessment review as posing a higher ML/FT risk, the AML/CFT measures must be heightened and ECDD measures must be conducted immediately after the customer (or beneficial owner) has been determined to be high risk.**]"***

---

**Section 21 amended**

**23.** Section 21 of the principal Code of Practice is amended

(a) by deleting the heading and substituting the heading "Ongoing customer due diligence";

(b) by deleting subsection (1) and substituting the following subsection

"(1) An entity or a professional shall conduct ongoing customer due diligence on its business relationships by

(a) scrutinising the transactions undertaken by each customer throughout the course of that relationship, for purpose of making an assessment of consistency between the transactions undertaken by the customer and the entity's or professional's knowledge of the customer, the customer's business and risk profile, including source of funds where necessary;

(b) screening all its or his or her customers to identify the customers that may present a higher risk, including customers that

(i) have become PEPs;

(ii) are subject to applicable sanctions; and

(iii) are associated with criminal activities; and

(c) reviewing and updating customer due diligence information, including information on beneficial ownership

(i) on a risk sensitive basis, prioritising the review and update of customers that present a higher risk; and

(ii) upon certain trigger events as determined by senior management of the entity or professional.";

(b) by revoking subsection (2); and

(c) by deleting subsection (3) and substituting the following subsection

"(3) Where the business relationship with a customer terminates, the entity or professional shall to the extent possible, in respect of that customer, review and update the customer due diligence information, including beneficial ownership information, as of the date of the termination of the relationship.";

(d) by deleting subsection (4) and substituting the following subsection

"(4) Notwithstanding anything contained in this section, as it relates to existing customers, an entity or a professional shall apply customer due diligence requirements on the basis of materiality of risk, and conduct customer due diligence at appropriate times, taking into account whether and when customer due diligence measures have previously been undertaken and the adequacy of the data obtained."; and

(e) by revoking subsection (5).

---

*The Explanation to section 21 of the principal Code of Practice is deleted and substituted by the following new Explanation:*

***"[Explanation:***

***Ongoing Monitoring***

***(i)*** *The initial customer due diligence process should enable an entity or a professional to gain an understanding of the applicant for business and their circumstances, develop a profile of the applicant for business' proposed business activities, and determine the level of ML/TF risk posed by that applicant. However, an applicant for business' circumstances, activities, and consequently risk profile, may change once he, she or it becomes a customer and commences business activities. As such, it is vital for entities and professionals to monitor customer transactions, conduct on-going CDD reviews and update customer information to identify when transactions or behaviours fall outside a customer's profile. Where behaviours fall outside of a customer's profile, an entity or professional must determine whether there are changes in the customer's circumstances and consider whether the ML/TF risks of that customer have also changed. Monitoring of a customer's transactions may increase or decrease the perceived risk that may be associated with the customer or transaction. These essentially would relate to*

- ***the purpose of an account or a business relationship****: regular account openings involving small amounts or simply to facilitate routine consumer transactions tend to pose a lower risk compared to account openings designed to facilitate large cash transactions from an unknown source;*

- ***the size and volume of assets to be deposited****: an unusual high level of assets or large transactions not generally associated with an applicant for business or a customer within a designated profile may need to be considered as higher risk; similarly, an otherwise high profile applicant for business or customer involved in low level assets or low value transactions may be treated as lower risk;*

- ***the level of regulation, compliance and supervision****: less risk may be associated with an applicant for business or a customer that is subject to regulation in a jurisdiction with satisfactory AML/CFT compliance regime compared to one that is unregulated or only subject to minimal regulation; thus publicly traded companies subject to AML/CFT regulation in their home jurisdictions pose minimal AML/CFT risks and may therefore not be subject to stringent account opening CDD measures or transaction monitoring;*

- ***the regularity or duration of the relationship****: long standing business relations with the same customer may pose less AML/CFT risk and therefore may not require a stringent application of the CDD measures;*

- ***the familiarity with the jurisdiction in which the applicant for business or customer is located****: this entails adequate knowledge of the laws and the regulatory oversight which govern the applicant for business or customer, considering the entity's or professional's own operations within that jurisdiction; and*

- ***the use of intermediaries or other structures with no known commercial or other rationale or which simply obscure the relationship and create unnecessary complexities and lack of transparency****: the risks associated with such relationships or transactions generally increase the risk profile of the applicant for business or customer.*

***(ii)*** *In addition, conducting ongoing CDD on a business relationship, and particularly monitoring, is vital for forestalling acts of money laundering, terrorist financing, proliferation financing and other activities designed to abuse the facilities offered by an entity or a professional. This is because scrutinising and synthesizing of executed or proposed transactions, allows an entity or professional to identify transactions and/or activities that are inconsistent with their knowledge of a customer, determine whether unusual transactions and/or activities can be reasonably explained or point to a suspicion of ML/TF activities. Therefore, it is imperative that an entity or a professional has an effective monitoring system in place that*

- *flags unusual transactions and/or activities for further examination;*
- *allows senior management to examine unusual transactions and/or activities promptly; and*

- *takes appropriate action based on the findings of the examination.*

***(iii)*** *Some indications of an unusual transaction or activity that can be flagged may include—*

- *transactions, activities or requests with no apparent legitimate purpose or commercial rationale;*
- *unnecessarily complex transactions, activities or requests;*
- *the size or pattern of transactions is inconsistent with expectations for that customer;*
- *the customer withholding information about their activities, for example, reason for a transaction, source of funds, or CDD documentation;*
- *the customer engages in frequent, complex one-off transactions which are appropriate for a business relationship, but refuses to establish a business relationship;*
- *transfers to or from high-risk countries which are inconsistent with what is expected from that customer;*
- *unnecessary routing of funds through third party accounts;*
- *unusual investment transactions with no discernible purpose; and*
- *extreme urgency in requests from the customer, particularly where they are not concerned by factors such as large transfer fees and early repayment fees.*

*The Agency may issue guidance with indications of unusual transactions and activity that may be flagged that should also be taken into consideration.*

***(iv)*** *A flagged transaction does not in itself mean suspicious activity. In examining unusual transactions or activities, the entity or professional should gather sufficient information, including from the customer or other reliable sources, in determining whether the transactions or activities can be explained. Where the activities can be explained, this may be an indication that the customer's circumstances and/or purpose for the business relationship has changed and the customer's profile (including ML/TF risk profile) needs updating (see paragraph (xi) below). Where the entity or professional determines that the activities cannot be explained, it or he or she should initiate the internal processes for filing a suspicious transaction or suspicious activity report.*

***(v)*** *Based on the nature, size and complexity of an entity's or a professional's business or the ML/TF risks posed, an entity or a professional should consider whether*

- *transactions will be monitored in real time (i.e. when transactions and/or activities are taking place or are about to take place), post event, (i.e.*

*through a retrospective review of transactions) or a combination of both; and*

- *transactions or activities will be monitored manually or automated.*

***(vi)*** *An entity or a professional may utilise a combination of real time and/or post event monitoring, based on the type of product or service, the risk level of the customer, etc. In deciding, an entity or a professional should consider which high-risk factors or combination of high-risk factors will always trigger real-time monitoring or which inherently higher risk transactions are to be monitored in real time, in particular, where the risk associated with the business relationship is already elevated.*

***(vii)*** *Where an entity or a professional engages in a high volume of customers and customer transactions, that entity or professional must be able to demonstrate that it or he or she has adequate systems in place to monitor the volume of its or his or her business. This may require the use of an automated or electronic system, as there is increased difficulty in adequately monitoring high volumes of transactions and relationships without some level of automated assistance.*

***(viii)*** *Monitoring of customers does not only relate to customers within a business relationship, but also customers that conduct one-off transactions. An entity or a professional should have systems in place to determine whether any series of one-off transactions conducted by a customer over time may indicate some unusual or suspicious activity, and gather information in the same way as information would be gathered on a customer in a business relationship. An entity or a professional should also consider whether the customer is avoiding establishing a business relationship to evade monitoring of its activities.*

***(ix)*** *Not all relationships or transactions are expected to be monitored the same way; the degree of monitoring employed will very much depend on the perceived risks presented by a customer or a transaction, the products or services being used and the location of the customer and the transactions. This means higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent monitoring, requiring more additional information and verification to ascertain whether an unusual transaction has a reasonable explanation, requiring senior management approval to continue the business relationship.*

***Customer Screening***

***(x)*** *The ongoing CDD systems of an entity or a professional should be able to detect where a customer (including its beneficial owner(s)) has become a PEP, has become subject to sanctions; or has been connected to criminal activity or any higher risk activity. In this regard, entities and professionals must have systems in place to screen customers on a regular basis to identify them against sanctions listing, and press and media releases. Screenings may be manual or automatic, in real time or through periodic reviews, based on the nature, size, and complexity of*

*business of the entity or professional and the ML/TF risks posed. As with transaction monitoring, an entity or a professional with a large customer base must be able to demonstrate that it or he or she has appropriate systems in place relative to the size of its business, which may require some automated assistance for screening. Periodic reviews, however, may not be adequate when they relate to sanctions listing, as this requires action (e.g. freezing of assets) to be taken in a timely manner. As such, entities and professionals should seek to screen their customer-base immediately after the Commission and the Agency issue notifications of updated sanctions lists related to UNSCR, the UK and the BVI. The Virgin Islands Financial Sanctions Guidelines provides further details of entities' and professionals' obligations as they relate to sanctions. Entities and professionals may also wish to have measures in place to monitor where individuals and legal persons have been listed on other sanctions lists (such as OFAC and EU).*

***Updating CDD information***

***(xi)*** *Any data or other information received and kept under the CDD process must be kept up-to-date and relevant through updates of information received via ongoing monitoring and a regular review and assessment of current records, especially as they relate to higher risk customers. Procedures and controls for reviewing CDD information to ensure they are up-to-date, accurate and appropriate should ensure that the entity or professional continues to understand the customer and its circumstances throughout the business relationship. It does not necessarily mean that relevant persons must automatically replace, for example, expired passports, especially where there is sufficient information to indicate that the identification of the customer can readily be verified by other means. However, depending on the outcomes from the risk assessments, it may be deemed necessary. Generally, updating CDD should entail confirming and verifying whether there have been any changes to the elements of CDD, i.e.—*

- *the customer's name, or address (including jurisdiction of domicile, registered office or address of business in the case of a legal person or legal arrangement);*
- *the customer's directorship, shareholding or beneficial ownership;*
- *the customer's business activities or the size of the customer's business;*
- *the customer's circumstances including occupation, sources of wealth, sources of funds; and*
- *person(s) acting or purporting to act on behalf of the customer (including signatories).*

*The level of ML/TF risk posed by the customer should drive the level of information that needs to be updated and extent of verification that must be undertaken during the update process. It is imperative that any changes in the particulars of any customer obtained via the ongoing monitoring process, and regular review of records is appropriately documented, builds upon existing customer due diligence*

*and is considered in the update of a customer's ML/TF risk assessment (required pursuant to section 12 (2) of the Code).*

***(xii)*** *An entity or a professional is to determine the manner, form and occasion when it or he or she updates the information relative to a business relationship. However, certain trigger events, might prompt an entity or a professional to seek appropriate information on the customer and its current circumstances. Examples of trigger events could include:*

- *a customer applying to open a new account, requesting new products or establishing a new relationship;*
- *a customer changing its geographic location or requesting services from a new geographic location;*
- *a material change in ownership and/or management structure;*
- *a customer becoming a PEP, the subject of a sanctions list, or associated with criminal behaviour; and*
- *identification of unusual transactions or activities through transactions monitoring.*

***(xiii)*** *An entity or a professional must also review and update all its customers' CDD (and risk profiles) based on the level of risks posed (i.e. higher risk customers are to be reviewed more frequently than other customers). Higher risk customers' CDD must be reviewed and updated at least once annually.*

***(xiv)*** *Updating CDD may be achieved through the entity's or professional's own review of independent sources, and/or entail contacting the customer concerned to ask relevant questions relating to the relationship and updating changes that would have occurred, or to do that during a specific or routine dealing with the customer. It helps to inform the customer that such a process is simply a part of the entity's or professional's statutory duty to maintain up-to-date information with respect to all business relationships.*

***Considerations for Entities providing trust and/or company services (TCSPs)***

***(xv)*** *TCSPs are responsible for incorporating, registering, administering and/or managing companies and partnerships in the Territory and must act as gatekeepers in preventing the misuse of these legal persons and legal arrangements. For this reason, TCSPs should have sound ongoing CDD measures and practices in place. A TCSP's ongoing CDD measures must ascertain any changes in the identity of a legal person or arrangement (including directorship and beneficial ownership) and any changes in the intended use of the legal person. To determine whether there have been any changes of the use of the legal person as envisaged, a TCSP must obtain evidence of their customers' activities and make a determination as to whether the activities are consistent with the known business of the customer. Examples of evidence include*

- *copies of minutes from meetings of directors and shareholders or partners (as applicable);*
- *copies of management accounts;*
- *copies of financial statements;*
- *copies of invoices;*
- *copies of property registers; and*
- *copies of contracts relating to the companies' activities.*

*Where a TCSP has identified changes in the company's or partnership's identity or its activities, the customer must be re-assessed to consider these changes and/or determine whether suspicious activity has occurred, thus triggering the internal suspicious activity reporting process.*

***(xvi)*** *Section 21 requires an entity or professional to review and update customer due diligence at the time of termination of a business relationship. Termination of a business relationship may arise for varying reasons some of which may not make it possible for an entity or a professional to review and update relevant information relating to the customer. Yet in some instances the entity or professional may already be in possession or be aware of or be able to access relevant information relating to the customer. In the case of the former, the entity or professional need only record its satisfaction on the customer's file that it has done what was reasonable in the circumstances and had been unable to obtain any information to update the customer's due diligence information. In the latter case, the entity or professional must record on the customer's file the information that it is in possession or is aware of or has been able to access. It is for the entity or professional to satisfy itself or himself or herself, in either case, that it or he or she has taken reasonable measures to comply with the requirements of section 21 (3). The relevant record of the customer must be kept and maintained in accordance with the record keeping requirements of the AMLR and this Code.*

***(xvii)*** *While it is required that an entity or a professional must effect the necessary review and updating of customer due diligence information for the periods stated in section 21 (1) and (2), depending on whether a customer is assessed as low or high risk, subsection (4) provides the additional requirement to perform a similar review and update in respect of customers with whom an entity or a professional had had a business relationship prior to the effective date of this Code (20th February, 2008) which continued beyond the effective date. However, this requirement applies only in the circumstances where the entity or professional forms the view that any of those customers presents some risk or engages in transactions that are of a material nature as to present some risk. It is a question of judgment on the part of the entity or professional concerned to make that assessment and come to a conclusion. In such cases, the entity must not wait for the period specified in section 21 (1) or (2) to mature before effecting the required review and updating of the customer's due diligence information. Where an existing*

*customer is not assessed as presenting a high risk or to be engaged in any material transaction that has the potential to present a high risk, the entity or professional need only comply with the requirements of section 21 (2).*

***(xviii)*** *The customer, it should be noted, is in effect the applicant for business and it is in relation to that applicant that the review and updating of customer due diligence information is required. Thus where, for instance, a mutual fund is a customer of a registered agent, the registered agent (as the relevant entity) is obligated to effect the necessary review and updating of customer due diligence information on the fund as the applicant for business. It is therefore essential for every entity or professional to determine from the outset of establishing a business relationship as to who actually is the applicant for business in the relationship and proceed accordingly in ensuring compliance with the requirements of section 21.****]"***

---

**Section 22 amended**

**24.** Section 22 of the principal Code of Practice is amended

(a) by deleting subsection (1) and substituting the following subsection

"(1) An entity or a professional shall have, as part of its or his or her internal control systems, appropriate risk-based policies, processes and procedures for determining whether an applicant for business or a customer, or the beneficial owner of an applicant for business or customer, is a politically exposed person.";

(b) by inserting after subsection (1), the following new subsections

"(1A) In relation to an applicant for business or customer, or beneficial owner of an applicant for business or customer that is a foreign politically exposed person, an entity or a professional, in addition to the customer due diligence measures outlined under section 19, shall

(a) take such reasonable measures as are necessary to establish the source of funds and source of wealth respecting such person;

(b) ensure that senior management approval is sought for establishing or maintaining a business relationship with a foreign politically exposed person;

(c) ensure a process of enhanced ongoing monitoring of the business relationship with a foreign politically exposed person;

(d) ensure that there is in place adequate supervisory oversight of the entity's or professional's business relationship with a foreign politically exposed person; and

(e) ensure that the requirements of paragraphs (a) to (d) apply in relation to a customer who becomes a foreign politically exposed person during the course of an existing business relationship.

(1B) Where an entity or a professional determines that the business relationship or transaction with a domestic politically exposed person or an international organisation politically exposed person presents a higher risk, subsection (1A) shall apply as if the domestic politically exposed person were a foreign politically exposed person.";

(c) by deleting subsection (2) and substituting the following subsection

"(2) Where a third party acts for a foreign politically exposed person, a domestic politically exposed person or an international organisation politically exposed person that presents a higher risk in establishing a business relationship or performing a transaction, subsection (1A) shall apply to that third party and the entity or professional shall perform the necessary enhanced customer due diligence measures, as if the business relationship or transaction is being made directly with the politically exposed person.";

(d) by deleting subsection (3) and substituting the following subsection

"(3) An entity or a professional shall have risk-based policies, processes and procedures in place to determine when a customer, or the beneficial owner of a customer, who ceases to qualify as a politically exposed person by virtue of no longer holding the post or relationship that qualified him or her as a politically exposed person shall, cease to be treated as a politically exposed person.";

(d) by deleting subsection (4) and substituting the following subsection

"(4) In the case of a life insurance policy, an entity or a professional shall take reasonable measures, no later than at the time of payout

(a) to determine whether the beneficiary and, where applicable, the beneficial owner of the beneficiary is a politically exposed person;

(b) to inform senior management of the higher risk before payout of the policy proceeds; and

(c) to conduct enhanced scrutiny on the whole business relationship with the policy holder and if necessary, to consider making a suspicious activity report.";

(e) by inserting after subsection (4), the following new subsection

"(4A) For the purposes of this section, the reference to

(a) "foreign politically exposed person" means an individual who is or has been entrusted with prominent public functions in a jurisdiction outside the Virgin Islands, and includes the family members and close associates of that individual;

(b) "domestic politically exposed person" means an individual who is or has been entrusted with prominent public functions in the Virgin Islands, and includes the family members and close associates of that individual; and

(c) "international organisation politically exposed person" means an individual that is a member of senior management of an international organisation, and includes the family members and close associates of that individual."; and

(f) in subsection (5), by deleting the words, "the Proceeds of Criminal Conduct Act" and substituting the words, "the Act".

---

*The Explanation to section 22 of the principal Code of Practice is deleted and substituted by the following new Explanation:*

***"[Explanation***

***(i)*** *Individuals that have a high political profile or hold a public office can pose higher risk for ML/TF or PF due to the potential to misuse their political powers and influence to commit offences related to corruption, bribery, terrorism and proliferation financing offences. Given the particular ML/TF and PF risks, these individuals are classified as politically exposed persons (PEPs). The categorisation of PEPs also extends to family members and close associates of these individuals. This is because persons entrusted with these functions may use family members and/or close associates to hide misappropriated funds, assets gained through abuse of power, bribery or corruption or assets to be used to fund terrorism or proliferation of weapons of mass destruction. The mere fact that an individual falls within the PEP bracket does not necessarily mean that the individual is connected to a wrongful action. However, an entity or a professional must remain aware that PEPs have a greater risk of exposure to bribery and corruption, ML/TF and PF, and apply appropriate CDD and ECDD measures to identify PEPs, identify any unusual and/or suspicious activity and mitigate against the associated ML/TF and PF risks.*

***Classification of PEPs***

***(ii)*** *In considering the measures to be applied to PEPs, an entity or a professional must identify the category of PEP in which an applicant for business, customer, or beneficial owner falls. There are 3 main types of PEPs:*

- *<u>Foreign PEPs</u> refer to PEPs that have been entrusted with prominent public functions in a country outside of the Virgin Islands. These generally comprise persons who are Heads of State/government, cabinet ministers/secretaries of state, judges (including magistrates where they exercise enormous jurisdiction), senior political party functionaries and lower political party functionaries with an influencing connection in high ranking government circles, military leaders and heads of police and national security services, senior public officials and heads of public utilities/corporations, members of ruling royal families, senior representatives of religious organisations where their functions are connected with political, judicial, security or administrative responsibilities.*

- *<u>Domestic PEPs</u> comprise the same class of persons categorised as foreign PEPs; however, these individuals are entrusted with prominent public functions in the Virgin Islands.*

- *<u>International Organisation PEPs</u> relate to individuals that serve as senior management, directors and deputy directors, and members of the board (or their equivalents) of international organisations. An international organisation refers to an entity formed by political agreements (international treaties) between their member states that are recognised by law in their member countries. This also extends to similar regional organisations. Some examples of international organisations include*
    - *the United Nationals and affiliated international organisations;*
    - *the International Monetary Fund;*
    - *the World Bank;*
    - *the Organisation for Economic Cooperation and Development;*
    - *CARICOM;*
    - *Organisation of Eastern Caribbean States;*
    - *Pan American Health Organization;*
    - *European Commission;*
    - *FATF; and*
    - *CFATF.*

*The examples of foreign and domestic PEPs are not exhaustive. It should be noted that the named positions do not include middle-ranking or more junior officials. However, when the political exposure of a middle-ranking or junior official is comparable to that of similar positions at national level, an entity or a professional should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs.*

***(iii)*** *As noted in the definition of PEPs, family members and close associates of PEPs also qualify as PEPs and the same measures in relation to establishing business relationships and engaging in transactions apply to them. Family relations generally cover persons in consanguine and affinity relations with PEPs; these would include, amongst others:*

- *a spouse;*
- *a partner considered by national law as equivalent to a spouse;*
- *a child;*
- *a spouse or partner of a child;*
- *a brother or sister (including a half-brother or half-sister);*
- *a parent;*

- *a parent-in-law;*
- *a grandparent; or*
- *a grandchild.*

*Close associates would comprise*

- *personal advisers/consultants to PEPs;*
- *close business colleagues and friends likely to benefit from association with, PEPs;*
- *individuals who have joint beneficial ownership of a legal person or legal arrangement with a PEP; and*
- *PEP-supported NPOs.*

***(iv)*** *Establishing whether an individual qualifies as a PEP may not be easy; in addition to reviewing CDD information and documentation, much is acquired from interviews and answers given at the time of a request to establish a business relationship or enter into a transaction. Entities or professionals may also wish to consult commercially available databases and screening tools and review internet and media sources, to aid in determining whether a customer or a beneficial owner, is a PEP.*

***Application of Measures to PEPs***

***(v)*** *It should be noted that foreign PEPs are considered to pose higher risks for money laundering, terrorist financing or proliferation financing, and require the application of both CDD and ECDD measures. However, the determination as to whether only CDD or both CDD and ECDD measures are required for a domestic and international organisation PEP is based on the level of risk identified at the establishment of the relationship or engagement of the transaction. The CDD and ECDD measures relative to PEPs do not prohibit business dealings or relationships with PEPs. However, because of the serious potential business risks that they pose, compliance with the applicable CDD and ECDD measures is requisite.*

***(vi)*** *Entities and professionals are required to implement enhanced customer due diligence measures (see section 20 of this Code) on all foreign PEPs and apply the following specific measures*

- *establish source of funds and source of wealth of the foreign PEP (i.e. obtaining more than standard information on source of funds and source of wealth, including requiring evidentiary documentation to confirm the foreign PEP's source of funds and wealth, verifying information provided against publicly available information sources such as asset and income declarations);*
- *require senior management approval to establish or continue a business relationship with the foreign PEP;*

- *conduct enhanced monitoring of the business relationship (e.g. increasing the number and timing of controls (such as CDD and risk assessment reviews) applied, obtaining information on the reasons for a particular transaction, selecting patterns of transactions that need further examination); and*
- *ensure appropriate supervisory oversight where a junior staff member deals with an entity or a professional.*

***(vii)*** *As it relates to domestic PEPs and international organisation PEPs, an entity or a professional is required to consider the customer or beneficial owner's PEP status as a high-risk factor. However, unlike foreign PEPs, an entity or a professional is only required to apply enhanced measures on a domestic or international organisation PEP, where the PEP poses higher ML/TF and PF risk. The risk rating of a domestic or international organisation PEP is dependent on the overall risk factors of the customer risk assessment conducted. Where the risk assessment identifies that a domestic PEP or an international organisation PEP poses a higher risk, the entity or professional must apply enhanced measures, as identified in paragraph (vi) above. Essentially, a domestic PEP or international organisation PEP that poses higher ML/TF and PF risk must be treated as if he or she were a foreign PEP. In addition to the standard customer risk factors assessed, in determining whether the business relationship or one-off transaction with a PEP should be classified as high risk, an entity or a professional should consider the following additional factors specific to PEPs:*

- *whether the PEP has business interests that are related to his/her public functions;*
- *whether the PEP is involved in public procurement processes;*
- *whether the PEP is from a country or jurisdiction that represents a higher risk of money laundering, corruption, terrorist financing or being subject to international sanctions;*
- *whether the PEP has executive decision-making responsibilities;*
- *whether the PEP has a prominent public function in industries known to be exposed to high levels of corruption, such as the oil and gas, mining, construction, natural resources, defence, sports, gaming and gambling industries; and*
- *whether the PEP has a prominent public function that would allow him/her to exert a negative impact on the effective implementation of the international AML/CFT standards in the Virgin Islands (e.g. the Governor, the Premier, Ministers of Government and other political or parliamentary leaders).*

*Notwithstanding the fact that all foreign PEPs are considered to pose higher ML/TF and PF risks, the factors listed above should be considered in relation to foreign PEPs to understand the particular ML/TF and PF risks that the foreign PEP may pose that may require additional or specific mitigation measures.*

***Screening for PEPs***

***(viii)*** *A new customer may not qualify as a PEP but may so qualify in the future. It is therefore important that entities and professionals screen customers on an ongoing basis to identify when an existing customer becomes a PEP (see section 21 of this Code). Where an entity or a professional identifies an existing customer or beneficial owner as a PEP, the entity or professional must undertake risk assessment and determine the level of risk the PEP relationship poses. Where a customer or beneficial owner is determined to be a foreign PEP, or a domestic or international organisation PEP that poses a higher risk, senior management must review and approve the continued business relationship with that customer. Enhanced customer due diligence and enhanced monitoring must also be applied with respect to this relationship.*

***Expiration of status as PEP***

***(ix)*** *A PEP's influence and prominence may not have diminished after leaving the role and he or she may continue to have influence and power, making that individual potentially more susceptible to bribery and corruption, and ML/TF and PF. As such, an entity or a professional must apply a risk-based approach in determining whether a PEP should continue to be treated as a PEP, after ceasing to qualify as such. As part of its risk-based approach in determining whether the customer should continue to be treated as a PEP, an entity or a professional should consider the following*

- *whether the customer may still pose potential risks, such as where there are ongoing legal proceedings relating to him or her or where there may be lingering issues in relation to his or her family members or close associates or where there are pending investigations in relation to him or her, etc.;*
- *the level of (informal) influence that the individual could still exercise;*
- *the seniority of the position that the individual held as a PEP;*
- *the amount of time that had passed since the individual were in the PEP role;*
- *whether the individual's PEP function and current function are linked in any way (e.g. formally by the appointment of the PEP's successor, or informally by the fact that the PEP continues to deal with the same substantive matters in an advisory capacity);*
- *the level of inherent corruption risk in the jurisdiction of the individual's political exposure;*
- *the level of transparency about the source of wealth and origin of funds; and*
- *whether the individual has links to higher risk industries.*

*Where an entity or a professional determines, based on its or his or her risk assessment of the relationship, that a customer should no longer be treated as a PEP, a detailed rationale for changing the customer's status should be recorded.*

*In addition, any decision to change the classification from a PEP, must be subject to senior management review and approval.**]**"*

---

**Section 23 amended**

**25.** Section 23 of the principal Code of Practice is amended

(a) in subsection (1)

(i) in the opening paragraph, by inserting after the words, "an applicant for business or a customer", the words "including the beneficial owner of the applicant for business or customer,";

(ii) in paragraph (c), by inserting after the words "in accordance with", the words, "sections 31, 31A and 31B of"; and

(iii) in paragraph (d), by inserting after the words "parent company", the words, "in accordance with the requirements and standards of, or requirements or standards at least equivalent to, the Anti-money Laundering Regulations, Revised Edition 2020 and this Code";

(b) in subsection (2)(c), by deleting the words, "money laundering or terrorist financing" and substituting the words, "money laundering, terrorist financing or proliferation financing";

(c) by inserting after subsection (2B), the following new subsection

"(2B*a*) Notwithstanding subsection (1)(b), in the case of a beneficiary under a life insurance policy or trust, an entity or a professional may verify the identity of that beneficiary, after the business relationship has been established, if it takes place at or before the time of payout or at or before the time the beneficiary exercises a right vested under the policy or trust."

(d) in subsection (2C)

(i) in the opening paragraph, by deleting the words "establishes a business relationship pursuant to subsection (2) and it or he or she";

(ii) in paragraph (a), by deleting the words "money laundering or terrorist financing" and substituting the words "money laundering, terrorist financing or proliferation financing";

(iii) in paragraph (c), by inserting after the words, "applicant for business", the words "or customer"; and

(iv) by revoking the closing subparagraphs (i), (ii) and (iii) and substituting the following closing subparagraphs

"(i) not open an account, establish a business relationship, or carry out the transaction for that applicant for business or customer; or

(ii) terminate any existing business relationship with the customer; and

(iii) submit, in relation to paragraph (a), a report to the Agency outlining its or his or her discovery or suspicion; and

(iv) submit, in relation to paragraph (b) or (c), a report to the Agency if it or he or she forms the opinion that the conduct of the applicant for business or customer raises concerns regarding money laundering, terrorist financing or proliferation financing.";

(e) in subsection (6B)

by deleting the opening paragraph and substituting it with the following opening paragraph,

"Where, for the purposes of subsection (6A), an entity or a professional relies on the electronic or digital data or other data of an organisation or any other person to carry out verification, it or he or she shall ensure that the organisation or that other person"; and

(f) in subsection (6D), by deleting the words, "money laundering or terrorist financing" and substituting the words, "money laundering, terrorist financing or proliferation financing".

---

***The Explanation to section 23 of the principal Code of Practice is amended***

*(a) in paragraph (i)*

*(i) in the third sentence, by deleting the word "or control", after the words "beneficial ownership"; and*

*(ii) by deleting the last sentence and substituting the following sentence "It is also important that in circumstances where there is a change in the third party acting on behalf of a customer, this should be noted, verified and updated, in accordance with section 21 of this Code."*

*(b) in paragraph (ii), by deleting the words "as considered feasible" in the first sentence;*

*(c) by deleting paragraph (iiA) and substituting the following paragraph*

*"(iiA) It should be noted that the effect of a termination of a business relationship as provided in subsection (2C) in circumstances where there is a suspicion of money laundering, terrorist financing or proliferation financing on the part of an applicant for business or a customer must be carried out in a manner so as not to tip off the applicant for business of customer. If an entity or a professional forms the opinion that an immediate termination of business relationship might tip off the applicant for business or customer, it or he or she must liaise with and seek the advice of the Agency and act according to the Agency's direction.";*

*(d) in paragraph (iii), by deleting the words, "Section 27 outlines the obligation for verification of underlying principals of legal persons, which section";,*

*(e) in paragraph (iv), by deleting the word "origin" in the first sentence, and substituting the words "risk rating";*

*(f) in paragraph (vi), by deleting the word "may" in the second sentence and substituting the word "must";*

*(g) in paragraph (vii), in the first bullet point, by deleting the words, "recognised jurisdiction listed in Schedule 2 of this Code, or with an assess low risk jurisdiction" and substituting the words, "country that the entity's or professional's risk assessment has not determined to pose a higher level of risk";*

*(h) in paragraph (xii) by deleting the words, "money laundering and/or terrorist financing", and substituting the words, "money laundering, terrorist financing and/or proliferation financing";*

*(i) in paragraph (xiii), by deleting the word "might" and substituting the word "must";*

*(j) in paragraph (xvi), by deleting the words, "money laundering or terrorist financing", and substituting the words, "money laundering, terrorist financing or proliferation financing"; and*

*(k) by deleting paragraphs (xviii), (xix), (xx), (xxi), (xxii) and (xxiii).*

---

**Section 24 amended**

**26**. Section 24 of the principal Code of Practice is amended

(a) in subsection (1)

(i) in the opening paragraph, by inserting after the words, "verification measures where", the words "the individual";

(ii) in paragraph (a), by deleting the words "the individual";

(iii) by deleting paragraph (b) and substituting the following paragraph

"(b) is the beneficial owner of an applicant for business;"; and

(iv) by deleting paragraph (c), and substituting the following paragraphs

"(c) is a director, or a person with a similar position responsible for the management of an applicant for business; or

(d) is acting on behalf of the applicant for business.";

(b) in subsection (2), by inserting after the words, "shall obtain information" the words, "and evidence";

(c) in subsection (3), by deleting the words, "makes a determination that from its risk assessment an individual or the product or service channels in relation to him or her", and substituting the words, "makes a determination from the customer risk assessment conducted in accordance with section 12(1)(b), that an individual";

(d) in subsection (4), by deleting the words, "key staff" and substituting the words, "senior management";

(e) in subsection (5)

(i) in paragraph (b), by deleting the words, "facsimile number, occupation, employer's name" and substituting the words "occupation and employer's name (if applicable)"; and

(ii) by deleting paragraph (c) and substituting the following paragraph

"(c) the full legal name and residential address and, in the case of a member of senior management introducing the individual, his or her job title and a brief description of the customer's or member of senior management's knowledge of the individual."

---

*The Explanation to section 24 of the principal Code of Practice is amended*

*(a) by re-designating paragraph (ii) as paragraph (viii);*

*(b) by re-designating paragraph (iii) as paragraph (ix);*

*(c) by inserting after paragraph (i), the following paragraphs*

***Documentation for Identity Verification***

***(ii)*** *The process for verifying the identity of a person may take varying forms. It is crucial that an entity or a professional not only knows its or his or her applicant for business or customer, it or he or she must also be able to verify the actual beneficial owner of the applicant for business or customer. In order to ensure a greater degree of certainty and provide smooth business conduct without undue hindrance, uniformity of approach is essential to the extent possible, bearing in mind that exceptions may apply in certain instances with respect to applicants or customers that are assessed as high risk. In relation to an individual, the following guide should be adopted to confirm the identity of an individual*

- *where identity is to be verified from documents, this should be based on either:*

  - *a government-issued document which incorporates the applicant for business' or customer's full name and photograph and either his or her residential address or his or her date of birth; or*

  - *a government, court or local authority-issued document (with or without a photograph) which incorporates the applicant for business' or customer's full name, supported by a second document, either government-issued, or issued by a judicial authority, a statutory or other public sector body or authority, a statutory or regulated utility company, or a Commission-*

*regulated entity in the financial services sector, which incorporates—*

- *the applicant's or customer's full name; and*
- *either his or her residential address or his or her date of birth.*

***(iii)*** *For purposes of the first bullet point under paragraph (ii) above, a government-issued document with photograph includes the following*

- *a valid passport;*
- *a valid photo-card driving licence, whether permanent or provisional;*
- *a national identity card;*
- *a valid work permit card;*
- *an immigration status-issued card (for example, a belonger card);*
- *an election/voter identity card;*
- *a national insurance card; and*
- *a valid student identity card.*

***(iv)*** *For purposes of the second bullet point under paragraph (ii) above, a government-issued document with or without a photograph includes the following*

- *instrument of a court appointment (such as appointment as liquidator, or grant of a probate);*
- *letter of appointment by the Commission as an examiner or a qualified person; and*
- *current Inland Revenue tax demand letter, or statement.*

***(v)*** *Examples of other documents to support a customer's identity include utility bills or current bank statements or credit/debit card statements issued by a bank or other similar financial institution regulated by the Commission or another financial institution regulated in a country that the entity's or professional's risk assessment has not determined to pose a higher risk. If the document is obtained from the internet, it should only be relied upon where the entity or professional is satisfied of its authenticity. Where a member of staff of the entity or professional has visited the applicant or customer at his or her home address, a record of this visit may constitute evidence corroborating that the individual lives at this address (that is, equivalent to a second document).*

***(vi)*** *It should be noted that some applicants for business or customers may not be able to produce identification information equal to those outlined above. Such cases may include, for example, some low-income earners, customers with a legal, mental or physical inability to manage their affairs, individuals dependent on the care of others, dependent spouses/partners or minors, students (without student identity cards), refugees and asylum seekers, migrant workers and prisoners. There may be other examples not listed herein and these must be considered in the same context as and when they arise or are discovered. The entity or professional will therefore need an approach that compensates for the difficulties that these classes of individuals may face in providing the standard evidence of identity. Nothing should be done that has the effect of shutting off an individual from establishing a business relationship or conducting a transaction with or through an entity or a professional simply on account of an inability brought on by the individual's status or circumstances.*

***(vii)*** *Notwithstanding what is provided in the above paragraphs, an entity or a professional may, where it or he or she assesses an applicant for business or a customer as presenting a high risk, require and rely on such additional documentation as it or he or she considers appropriate and reasonable as further proof of identity. However, this must not be used as an excuse or a pretext for making inappropriate or unreasonable demands of an applicant for business or a customer or for negatively profiling an applicant or a customer thereby hindering a business relationship or transaction with the entity or professional.";*

*(d)* ***in*** *paragraph (viii), as re-designated, by inserting the heading "****Reliance on personal introduction****"; and*

*(e) in paragraph (ix), as re-designated, by inserting after the words "the telephone", the words, "or via electronic means".*

---

**Section 25 amended**

**27.** Section 25 of the principal Code of Practice is amended

(a) in subsection (1)

(i) in paragraph (a), by deleting the words, "in its own right";

(ii) by deleting paragraph (b), and substituting the following paragraphs

"(b) is a shareholder of an applicant for business, holding 10% or more interest or voting rights in the applicant for business;

(b*a*) is a director of an applicant for business; or"; and

(iii) by deleting paragraph (c) and substituting the following paragraph

"(c) is a third party acting or purporting to act on behalf of an applicant for business.";

(b) by deleting subsection (2) and substituting the following subsection

"(2) For purposes of the identification and verification of a legal person, an entity or a professional shall

(a) obtain information regarding

(i) the full name of the legal person and any trading name of the legal person;

(ii) the official registration or other identification number of the legal person;

(iii) the date and place of incorporation, registration or formation of the legal person;

(iv) the address of the registered office in the country of incorporation of the legal person and its mailing address, if different;

(v) where applicable, the address of the registered agent of the legal person to whom correspondence may be sent and the mailing address of the registered agent, if different;

(vi) the legal person's principal place of business and the type of business engaged in;

(vii) the powers that regulate and bind the legal person, as well as the names of the relevant persons having a senior management position in the legal person; and

(viii) the ownership and control structure of the legal person, including direct and indirect ownership; and

(b) identify and verify the identity of

(i) each director of the legal person or any other similar position a the legal person responsible for management of the legal person;

(ii) each beneficial owner of the legal person; and

(iii) any person acting or purporting to act on behalf of the legal person.";

(c) in subsection (3), by deleting the words "from its or his or her risk assessment a legal person or the product or service channels in relation to the legal person presents a higher level of risk," and substituting the words, "from the customer risk assessment conducted in accordance with section 12 (1) (b), that the legal person presents a higher level of risk,"; and

(d) in subsection (6), by deleting the words, "other than a company, partnership and trust," and substituting the words, "other than a company and partnership,".

*The Explanation to section 25 of the principal Code of Practice is deleted and substituted by the following Explanation*

***"[Explanation***

*"(i) The reference to a "legal person" refers to a body corporate. To be specific for the purposes of this Code, the reference to a "legal person" must be taken to cover bodies corporate, including partnerships, companies, foundations, anstalts, Waqf, associations and any incorporated or unincorporated clubs, societies, NPOs, churches, institutes, friendly societies established pursuant to the Friendly Societies Act (Cap. 268), provident societies or cooperative societies established pursuant to the Cooperative Societies Act (Cap. 267) and any similar bodies. Thus the verification requirements in establishing a business relationship will apply to all of these bodies, irrespective of their structure or place of formation.*

***(ii)*** *There are different forms of verification that an entity or a professional may employ in trying to verify the identity of a legal person with whom it or he or she wishes to establish a business relationship. Based on the level of risk present, an entity or professional may require a range of forms of verification for a particular legal person. For instance, for a higher risk company from a jurisdiction with high instances of fraud, an entity or a professional may require documentary evidence from the customer of its existence and additionally conduct a company search at a company registry or other electronic verification means to further verify that the company exists. Furthermore, an entity or a professional may require more than the standard number of documentation to verify the higher risk company's existence. As for all aspects of customer due diligence in general, it is for the entity or professional to establish its or his or her standard verification requirements and determine the additional verification measures that will be put in place for higher risk legal persons, on a case by case basis (based on the type of ML/TF risk posed and measures required for mitigation of those risks). Verification needs may also vary based on the type of legal person that is applying for business (e.g. an incorporated company would require a Certificate of Incorporation, whilst this is not possible for an unincorporated organisation). Where an entity or a professional determines that a legal person poses a lower level of ML/TF risk, it or he or she may apply simplified due diligence measures, including requiring less than standard verification requirements in establishing the relationship. Where simplified due diligence measures are applied, the rationale must be appropriately documented and the entity or professional must be able to justify the*

*application of simplified measures to the Commission or Agency, as applicable.*

***Documentation for Identity Verification (Legal Persons)***

***(iii)*** *In relation to verification relying on documentation, the types of documentation may vary, depending on the type of legal person. Some basic examples of documentation that can be used for verification include—*

- *Certificate of Incorporation, or certificate of Registration or Formation;*
- *a copy of constitutional documents (i.e. Memorandum and Articles of Association, Partnership Agreement, by-laws, charters or similar document); and*
- *a copy of a trade licence, registration certificate or regulatory licence (where applicable).*

*In relation to the first bullet point above, the certificate may be differently referenced. The important thing is that there is a valid written document showing the incorporation, registration or formation of a legal person.*

*The following are examples of documentation that can be requested as additional documents to verify a legal person's existence (as applicable)—*

- *Certificate of Good Standing or similar document confirming that the legal person is registered in the place of incorporation, registration, formation or continuation;*
- *copy of audited financial statements within the last year of the establishment of the business relationship;*
- *copy of a certificate of membership in a professional or trade association;*
- *copies of previous bank statements or financial reference on the legal person; and*
- *copies of utility bills in relation to the legal person.*

***(iv)*** *Outside of identifying and verifying that a legal person exists, and is who it says it is, an entity or a professional must, where applicable, also verify information in relation to the legal person's directors, partners, beneficial owners, and persons acting or purporting to act on behalf of the applicant for business or customer. Relevant documentation an entity or a professional should obtain include*

- *Register of Directors, Register of Partners or similar documents;*
- *Register of Shareholders or other similar documents;*

- *ownership structure charts (where applicable);*
- *verification documents of each director of the legal person or any similar position a legal person responsible for management of the legal person;*
- *verification documents of each beneficial owner of the legal person; and*
- *verification documents of any person acting or purporting to act on behalf of the legal person (these include persons with powers of attorney and signatories of accounts).*

***(v)*** *In verifying a legal person that is a director or shareholder of a customer or applicant for business, an entity or professional must verify that the legal person exists, as outlined in paragraphs (ii) and (iii) above. However, the extent to which an entity or professional should verify the identity of the directors and shareholders of that legal person (director or shareholder), should be based on the level of risk posed by the customer or applicant for business and its beneficial owners, and the director or shareholder itself.*

***Considerations for identification and verification of Segregated Portfolio Companies***

***(vi)*** *As outlined in paragraph (iv), identification and verification of a legal person includes identifying and verifying the identities of the beneficial owners of the legal person. In identifying and verifying the beneficial owners of a legal person structured as a segregated portfolio company, an entity or a professional must consider the individuals that own or control 10% or more of the shares or voting rights of the segregated portfolio company and any particular segregated portfolio. This also extends to any individual exercising control over the management of the segregated portfolio company and any particular segregated portfolio."*

---

**Section 26 revoked**

**28.** Section 26 of the principal Code of Practice is revoked.

**Section 27 revoked**

**29.** Section 27 of the principal Code of Practice is revoked.

**Section 28 amended**

**30.** Section 28 of the principal Code of Practice is amended

(a) in the heading, by deleting the word, "trust" and substituting the words, "legal arrangement";

(b) by deleting subsection (1) and substituting the following subsection

"(1) An entity or a professional shall, with respect to a legal arrangement that is a trust, undertake identification and verification measures by

(a) obtaining the following information

(i) the name of the trust;

(ii) the date and country of establishment of the trust;

(iii) where there is an agent acting for the trust, the name and address of the agent;

(iv) the nature and purpose of the trust;

(v) the powers that regulate and bind the trust, as well as the names of the relevant persons having a senior management position in relation to the trust; and

(vi) the ownership and control structure of the trust; and

(b) identifying and verifying the identity of

(i) the beneficial owners of the trust; and

(ii) any person acting or purporting to act on behalf of the trust, or the settlor of the trust.";

(c) by inserting after subsection (1), the following new subsection

"(1A) Where an entity or a professional is a trustee of a trust, that entity or professional shall, in addition to the requirements established under subsection (1), obtain the name and address of any other regulated agent of, and service provider to, the trust, including any investment advisor or manager, accountant, and tax advisor.";

(d) by deleting subsection (2), and substituting the following subsections

"(2) An entity or a professional shall perform customer due diligence on its or his or her business relationship with a trust and apply enhanced customer due diligence where, from its or his or her risk assessment, it is determined that a relationship with a trust presents a higher level of risk."

(2A) Where an entity or a professional enters into a business relationship with or conducts a one-off transaction in relation to a legal arrangement, other than a trust, the provisions of this section are modified to apply to that legal arrangement."

---

*The Explanation to section 28 of the principal Code of Practice is deleted and substituted by the following Explanation*

***"[Explanation***

***(i)*** *It is important in establishing proportionate AML/CFT systems and procedures that entities' and professionals' ML/TF risk assessments of trusts take into account the following relevant factors, in addition to those outlined in the Explanation to section 19 of this Code*

- *the country in which the trust is established;*
- *the legal form, nature and purpose of the trust (e.g. fixed interest, discretionary, testamentary, purpose, bare, wealth management);*
- *the type and value of assets to be held or managed in the trust;*
- *the ownership and control structure of the trust;*
- *the risks posed by the beneficial owners of the trust and, in particular, the settlor where the trust has not yet been established.*

***(ii)*** *In establishing a business relationship relating to trust business, an entity or a professional must identify and verify the existence of the trust or the identify and verify details of the trust to be established (as applicable). This involves obtaining information outlined in subsection 1(a) above. Where the trust is already established, it is imperative that the entity or professional obtains a copy of the trust deed and any amendments to the trust. Where the trust is yet to be established, the entity or professional may obtain copies of draft trust deeds, contractual agreements, declarations from the settlor of the trust and verification documents of the source of assets to be settled in the trust, to verify the details of the proposed trust.*

***(iii)*** *Although an entity or professional must obtain identifying information and verifying evidence in relation to trusts as outlined in paragraph (ii) above, trusts do not have legal personalities. As such, the applicant for business or customer in relation to a trust, is a combination of its beneficial owners. These include the trustees, settlors, beneficiaries, classes or characteristics of beneficiaries, any appointed protectors, and any other person that has control over the trust. Consequently, the identification and verification requirements under sections 24 (verification of an individual) and 25 (verification of a legal person) of this Code applies for all the beneficial owners of the trust. An entity or a professional is neither required to establish the detailed terms of the trust nor the rights of the beneficiaries.*

***Identification and Verification of Beneficiaries of Trusts***

***(iv)*** *Identification and verification of a trust (i.e. identification and verification of the beneficial owners of the trust and any person acting on behalf of a party to the trust) must be undertaken at the point of establishing a business relationship or engaging in a one-off transaction. However, the Code offers other timelines when it comes to identification and verification of beneficiaries or classes and characteristics of beneficiaries. Specifically, where it relates to the identification of beneficiaries, section 19(4A) of this Code provides the following:*

- *where a beneficiary is specifically named as the beneficiary of a trust, the entity or professional must take the full name of this person, if available at the establishment of the business relationship, or as soon as the beneficiary is specifically named; and*

- *where a beneficiary is designated by characteristics or by class, an entity or professional must obtain, at the time of establishment of the business relationship or as soon as the beneficiary is designated, sufficient information about the beneficiary that it or he or she would be able to identify the beneficiary at the time of payout.*

*Additionally, section 23(2C) of this Code permits verification of beneficiaries of trusts at or before the time of payout, or the point at which a beneficiary exercises the vested right under the trust. This applies whether the beneficiary is specifically named as a beneficiary of the trust, or the beneficiary is part of a designation by class or characteristics.*

***Designated classes or characteristics of beneficiaries***

***(v)*** *Identifying the beneficiaries of designated classes or characteristics of trust can be different, depending on the designations of beneficiaries made and the number of different types of class or characteristics definitions made in a trust. The following are examples of designated classes or characteristics of beneficiaries:*

- *the children of "Mrs. A";*
- *The grandchildren of Ms. A;*
- *The adult children and spouses of Mr. A;*
- *Charity ABC;*
- *The employees of company A;*
- *Pension holders and their dependents; or*
- *Unit holders.*

*Below is an example of the identification and verification steps that an entity or a professional should take in relation to a trust with designated classes or characteristics.*

*The beneficiaries of trust ABC are the children of Mr. A. The entity or professional needs to:*

- *Obtain the names of all the children of Mr. A;*
- *Before payout:*
    - *Identify the children of Mr. A (including each of the children's full legal name (including any former name, other current name or aliases used), gender, principal residential address and date of birth); and*
    - *Verify the identity of the children of Mr. A in accordance with section 24 of this Code.*

***(vi)*** *It should be noted that in circumstances where an entity or a professional makes a determination that, having regard to the customer risk assessment conducted in accordance with section 12 (1) (b) of this Code, a relationship with a*

*trust does not present higher risks, relevant customer due diligence information must be obtained with respect to the trust. Where an entity or professional makes a determination that such a relationship presents a higher risk, enhanced customer due diligence information must be obtained. The nature of the identification to be made or verification to be effected is a matter of judgment for the entity or the professional, based on the level or risk posed by the trust structure, including the beneficial owners of the trust. In verifying the appointment of a trustee, it is important to verify the nature of the trustee's duties.*

***(vii)*** *Throughout the existence of a trust, changes in the beneficial owners, jurisdiction, assets of the trust, etc., may occur. For this reason, entities and professionals must ensure that ongoing customer due diligence on their trust relationships is undertaken in accordance with section 21 of this Code; updating, noting and properly recording any changes accordingly. Where any new beneficial owners are introduced to a trust, an entity or professional must identify and verify these new beneficial owners. These changes should prompt a re-assessment of the trust relationship.*

***(viii)*** *Legal arrangements refer to trusts or other similar arrangements such as fiducie, treuhand and fideicomiso. In the Virgin Islands trusts are the only legal arrangements that are established, as such the explanation relates prevalently to trusts. Notwithstanding, where an entity or professional establishes a business relationship or undertakes a transaction with or for another type of legal arrangement, it or he or she must be satisfied that the legal arrangement has been verified in a manner similar to the verification of a trust.".*

---

**Explanation to section 29 amended**

**31.** *The Explanation to section 29 of the principal Code of Practice is amended*

*(a) in paragraph (ii), by deleting the words "the assessed money laundering and/or terrorist financing risk presented by the applicant or customer", and substituting the words, "the assessed money laundering, terrorist financing and/or proliferation financing risk presented by the applicant or customer";*

*(b) in paragraph (v), in the fifth bullet point, by inserting the word "and" at the end of the bullet point; and*

*(c) by deleting paragraph (vi).*

---

**Explanation to section 30 amended**

**32.** *The Explanation to section 30 of the principal Code of Practice is amended in paragraph (ii), by deleting the last bullet point and substituting the following bullet point*

*"• a director, manager or senior officer of a licensed entity, or of a branch or subsidiary of a group headquartered in a country that the entity's or professional's*

*risk assessment has not determined to present a higher risk or other well-regulated country that applies group standards to subsidiaries and branches worldwide and tests the application of and compliance with such standards."*

**Section 31 amended**

**33.** Section 31 of the principal Code of Practice is amended in subsection (5), by deleting paragraph (a) and substituting the following paragraph

"(a) the third party has in place a system of monitoring any change in risk with respect to the applicant for business or customer and reviewing and updating customer due diligence information on the applicant for business or customer, including information on beneficial ownership

(i) on a risk sensitive basis, prioritising the review and update of customers that present a higher risk at least once every year; and

(ii) upon certain trigger events as determined by senior management of the third party; and".

*The Explanation to section 31 of the principal Code of Practice is amended*

*(a) in paragraph (iii), by deleting the words "legal persons (companies) and legal arrangements (partnerships and trusts), these entities from being used to carry out money laundering, terrorist financing and other financial crime activities;" and substituting the words, "legal persons (companies and partnerships) and legal arrangements (trusts), these entities from being used to carry out money laundering, terrorist financing, proliferation financing and other financial crime activities;"*

*(b) in paragraph (iv), by deleting the words "paragraph (ii) of"; and*

*(c) by deleting paragraph (viii) and substituting the following paragraph*

*"**(viii)** One of the fundamental elements of customer due diligence is the need to update information on the applicant for business or customer. Accordingly, an entity or a professional that relies on an introduction by a third party must ensure that the third party has in place appropriate measures for updating information on the applicant or customer. This will include changes in the applicant's general profile (business or otherwise), name, address, registered office or principal place of business, senior management, beneficial ownership, purpose and nature of business, risk profile, etc. The obligation to review and update an applicant's or a customer's due diligence information must be carried out periodically, with priority being placed on reviewing and updating high risk applicants or customers at least once every year. An applicant's or a customer's due diligence should also be established upon certain trigger events (e.g. significant changes in ownership, change in the customer's location, customer becoming a PEP). While this obligation lies with the third party, the entity or customer is equally obligated to test and ensure that the third*

*party is complying with its system of reviewing and updating the applicants' or customers' customer due diligence information.".*

---

**Section 31A amended**

**34.** Section 31A of the principal Code of Practice is amended

(a) subsection (1)

(i) in paragraph (c), by deleting the words, "within a period of forty eight hours, but not exceeding seventy-two hours (calculated from the time of dispatch of the request)" and substituting the words, "within 1 business day"; and

(ii) by deleting paragraph (k); and

(b) by revoking subsection (3).

---

*The Explanation to section 31A of the principal Code of Practice is amended*

*(a) in paragraph (iv), by deleting the first bullet point and substituting the following bullet point;*

"• *notify the Agency or the Commission, as the case may be, in writing of the failure to notify contrary to the written agreement by providing the name, address, competent authority by which the third party is regulated, supervised or monitored for compliance with anti-money laundering, terrorist financing and proliferation financing obligations, and other details of the third party as would enable the Agency or the Commission to properly identify the third party;";*

*(b) in paragraph (vi), by deleting the first sentence and substituting the following sentence*

*"With regard to a third party's undertaking in a written agreement to provide relevant information whenever requested by the entity or professional within the prescribed time of 1 business day, public holidays and non-working days shall be excluded.";*

*(c) in paragraph (vii), by deleting the first 3 sentences; and*

*(d) by deleting paragraph (viii).*

---

**Section 31B amended**

**35.** Section 31B(5) of the principal Code of Practice is amended

(a) by deleting paragraph (a) and substituting the following paragraph

"(a) prepare a report of its testing, including

(i) the name of the third party relationship that was tested;

(ii) the date of the testing;

(iii) the percentage of customers introduced by the third party for which due diligence and documentation was requested during the testing;

(iv) details of customer information requested from the third party during testing;

(v) the results of testing of the third party relationship; and

(vi) any follow-up actions to be taken as a result of the testing"; and

(b) in paragraph (b), by deleting the word "record" and substituting the word "report".

---

*The Explanation to section 31B of the principal Code of Practice is amended*

*(a) in paragraph (i), by deleting the first 3 sentences and the word "Accordingly" at the beginning of the fourth sentence; and*

*(b) in paragraph (ii), by deleting the last sentence.*

---

**Section 33 is amended**

**36.** Section 33 of the principal Code of Practice is amended

(a) in paragraph (a), by deleting the word "and" at the end of the paragraph;

(b) in paragraph (b), by deleting the full-stop at the end of the paragraph and substituting the word, "; and"; and

(c) by inserting after paragraph (b), the following new paragraph

"(c) "shell bank" means a bank, or any other financial institution engaged in activities similar to banking business, that

(i) does not have meaningful mind and management in the country in which it is incorporated or registered; and

(ii) is not affiliated with a regulated financial group that is subject to effective consolidated supervision.".

**Explanation to section 34 amended**

**37.** *The Explanation to section 34 of the principal Code of Practice is amended by inserting after the words "money laundering, terrorist financing" wherever they appear in the paragraph, the words, ", proliferation financing".*

**Section 35 amended**

**38.** Section 35 of the principal Code of Practice is amended

(a) in subsection (1)

(i) in paragraph (b)(iii), by inserting after the words "terrorist financing", the words ", proliferation financing"; and

(ii) in paragraphs (c) and (f), by deleting the words, "anti-money laundering and terrorist financing" and substituting the words, "anti-money laundering, terrorist financing and proliferation financing"; and

(b) in subsection (3), by deleting the words, "money laundering or terrorist financing" and substituting the words, "money laundering, terrorist financing or proliferation financing".

**Explanation to section 36 amended**

**39.** *The Explanation to section 36 of the principal Code of Practice is amended in the second sentence, by deleting the words, "money laundering or terrorist financing", and substituting the words, "money laundering, terrorist financing or proliferation financing".*

---

**Section 37 amended**

**40.** Section 37 of the principal Code of Practice is amended

(a) in subsection (1)

(i) by inserting in their appropriate alphabetical order, the following new definitions

""cross-border transfer of funds" means

(a) a single wire transfer in which the payment service provider of the payer and the payment service provider of the payee are located in different countries; or

(b) any chain of a transfer of funds in which at least one payment service provider is located in a different country;

"full beneficiary information", means

(a) the payee's name; and

(b) the payee's account number, or a unique identifier in the absence of an account number;

"straight-through processing" means payment transactions that are conducted electronically without the need for manual intervention;";

(ii) by deleting the definition of "full originator information" and substituting the following definition

"full originator information" means the name of the payer, together with

(a) the payer's account number, or a unique identifier in the absence of an account; and

(b) the payer's address; or

(c) the payer's date and place of birth; or

(d) the customer identification number or national identity number of the payer;";

(iii) by renaming the definition "intermediate payment service provider" as "intermediary payment service provider"; and

(iv) in the definition of "unique identifier", by inserting at the end of the definition, before the full-stop, the words ", which permits traceability of the transaction";

(b) by inserting after subsection (2), the following new subsection

"(3) A payment service provider that holds a Class A licence pursuant to the Financing and Money Services Act, Revised Edition 2020, shall comply with all the relevant requirements of this Part, in the countries in which it operates directly or through its agents."

---

*The Explanation to section 37 of the principal Code of Practice is amended*

*(a) by deleting paragraph (i) and substituting the following paragraph*

*"**(i)** This Part of the Code effectively implements measures required by FATF Recommendations that ensure transparency in the execution of wire transfers. The application relates to both domestic and cross-border transfers so as to facilitate the tracking of funds associated with such transfers by persons who may be engaged in money laundering, terrorist financing, proliferation financing and other forms of financial crime. Implementation of these measures is essential to the Territory's international cooperation regime and facilitates trade and commerce where wire transfers allows for smooth business transactions. Failure to implement these measures could have the adverse effect of having financial institutions in compliant jurisdictions refusing to accommodate business originating from or destined to the Territory.";*

*(b) in paragraph (ii), by inserting after the last sentence, the following new sentence*

*"Payment service providers are also required to provide information on the persons receiving the proceeds of the wire transfer."; and*

*(c) in paragraph (iii), by inserting after the words, "terrorist financing", the words, ", proliferation financing".*

---

**Section 39 amended**

**41.** Section 39 of the principal Code of Practice is amended

(a) in subsection (1), by inserting after the words "full originator information" the words, "and full beneficiary information";

(b) in subsection (2)(a), by deleting the words "the complete information on the payer" and substituting the words, "full originator information and full beneficiary information that is fully traceable within the payee's country";

(c) in subsection (5)(c), by inserting after the words "terrorist financing", the words, ", proliferation financing";

(d) by deleting subsection (6) and substituting the following subsection

"(6) The payment service provider of the payer shall keep records of full originator information on the payer and full beneficiary information on the payee that accompany the transfer of funds for a period of at least 5 years

(a) from the date of the wire transfer, in the case of a wire transfer not made from an account; and

(b) from the date that the business relationship ended, in the case of a wire transfer made from an account.";

(e) in subsection (7)(a), by deleting the word "payee" and substituting the word "payer";

(f) by deleting subsection (8) and substituting the following subsection

"(8) Where subsection (7) applies, the payment service provider of the payer shall, upon request from the payment service provider of the payee, the Agency or the Commission, make available the full originator information and full beneficiary information within 3 working days of receiving the request, excluding the day on which the request was made.";

(g) by deleting subsection (9) and substituting the following subsection

"(9) Where a payment service provider of the payer fails to comply with a request from the payment service provider of the payee to provide the full originator information or full beneficiary information within the period specified in subsection (8), the payment service provider of the payee shall notify the Agency (in the case of a payment service provider that is supervised by the Agency) or the Commission (in the case of a payment service provider of the payer that is regulated by the Commission), which shall require the payment service provider of the payer to comply with the request immediately.";

(h) by deleting subsection (10) and substituting the following subsection; and

"(10) Where a payment service provider of the payer fails to comply with a request from the Agency or Commission pursuant to subsection (8) or an instruction from the Agency or Commission to comply with a request pursuant to subsection (9), it or he or she commits an offence and is liable to be proceeded against under section 27 (4) of the Act."; and

(i) by inserting after subsection (11), the following new subsection

"(12) The payment service provider of the payer shall not execute a transfer of funds where the transfer of funds does not comply with the requirements of this section."

*The Explanation to section 39 of the principal Code of Practice is deleted and substituted by the following Explanation*

***"[Explanation***

***(i)*** *A fundamental AML/CFT principle with respect to cross-border wire transfers, is the provision of full originator and full beneficiary information by the payment service provider of the payer to the payment service provider of the payee, along with the transfer. The payment service provider of the payer must ensure that the originator information on the payer is accurate and complete through verification of the customer's information. Where the payer holds an account with the payment service provider of the payer, the payer's originator information may be considered verified based on the customer due diligence (including ongoing customer due diligence) measures undertaken with respect to the business relationship. However, a payment service provider of a payer may wish to verify and undertake additional customer due diligence measures in relation to a customer that holds an account, prior to executing a wire transfer, where additional risks are present (e.g. transfers to a high-risk jurisdiction, involvement of a higher risk third party in the transaction, a type of transfer that is unusual for the particular customer). For a payer that does not hold an account with the payment service provider of the payer, verification of the customer's information is not required where the transfer is less than $1,000 and the entity or professional does not suspect ML/TF. It is, however, important to note that verification of the customer's information will be required where the transaction is linked to other transfers which together exceed $1,000.*

***(ii)*** *Where domestic wire transfers are concerned, the payment service provider of the payer may supply limited specified information with the transfer; however, that payment service provider is required to provide full originator or beneficiary information within 3 days after the date of the request from the payment service provider of the payee, the Agency or the Commission. It is advisable that such requests be documented; this is particularly important for enforcement purposes where a request is not complied with as provided under this Code. Where a payment service provider of the payee has not received the information within the specified period, the payment service provide may notify the Commission, where the payment service provider of the payer is regulated by the Commission. Where the payment service provider of the payer is not regulated by the Commission, the payment service provider of the payee should notify the Agency.*

***(iii)*** *Where the Agency or the Commission is notified of a failure to accede to a request within the specified period, the directives issued by the Agency or the Commission must be produced in writing. A record of regular or persistent breach on the part of a payment service provider of the payer should itself, where the payment service provider of the payer is licensed by the Commission, be a serious cause for concern and for necessary action by the Commission against the payment service provider of the payer.*

***(iv)*** *While routine batched wire transfers may not ordinarily present money laundering, terrorist financing and proliferation financing risks, entities are required to adopt relevant measures to ensure that non-routine transactions are not batched in circumstances where doing so will or is likely to present such risks.*

***(v)*** *Irrespective of the amount of the transfer, whether the customer has an account with the payment service provider of the payer, or whether transfers are ordered for individual or batch transfers, the payment service provider of the payer must have systems in place to detect whether a transfer is suspicious and initiate internal suspicion reporting processes promptly. Some examples of suspicious behaviour relevant to the ordering of transfers may include*

- *a payer refusing to provide required information;*
- *the originator information of a payer cannot be verified; or*
- *a payer seeking to route the transfer through intermediary payment service providers, with no apparent rationale.*

***(vi)*** *The payment service provider of the payer is required to maintain records of all information relating to wire transfers, including any requests that may have been received from the payment service provider of the payee or any intermediary payment service provider, for a period of 5 years from the date of the transfer, in the case of a wire transfer not made from an account. Where the transfer is made from an account, an entity or professional must maintain the wire transfer records for 5 years after the business relationship with the accountholder has ended.]"*

---

**Section 40 amended**

**42.** Section 40 of the principal Code of Practice is amended

(a) in subsection (1), by deleting the words "full originator information on the payer" and substituting the words, "full originator information and full beneficiary information";

(b) in subsection (2), by deleting the words "for the detection of any missing or incomplete full originator information" and substituting the words, ", including post-event monitoring or real-time monitoring where feasible, for the detection of any missing or incomplete full originator information or full beneficiary information";

(c) in subsection (3), by deleting the words "the full originator information is" and substituting the words, "the full originator information and full beneficiary information are";

(d) by inserting after subsection (3), the following new subsections

"(3A) The payment service provider of the payee shall verify the identity of the beneficiary on the basis of documents, data or information obtained from a reliable and independent source.

(3B) In the case of a transfer to an account, the payment service provider of the payee may deem verification of the payee to have taken place if it has complied with the provisions of the Anti-money Laundering Regulations, Revised Edition 2020, and this Code relating to the verification of the identity of the payee in connection with the opening of that account.

(3C) In the case of a transfer of funds not made to an account, the payee shall be deemed to have been verified by a payment service provider of the payee if

(a) the transfer consists of a transaction of an amount not exceeding $1,000;

(b) the transfer is not a transaction that is carried out in several operations that appear to be linked and that together comprise an amount exceeding $1,000; and

(c) the payment service provider of the payee does not suspect that the payee is engaged in money laundering, terrorist financing, proliferation financing or other financial crime.";

(e) by deleting subsection (4) and substituting the following subsection

"(4) Where the payment service provider of the payee becomes aware that the full originator information or full beneficiary information is missing or incomplete when receiving transfers of funds, the payment service provider of the payee shall have risk-based policies and procedures to determine whether to

(a) execute, reject or suspend the transfer; and

(b) undertake an appropriate follow-up action which may include

(i) requesting the missing information on the payer;

(ii) rejecting future transfers of funds from the payment service provider of the payer;

(iii) restricting or terminating its relationship with the payment service provider of the payer;

(iv) determining whether the transfer of funds or any related transaction should be reported to the Agency as a suspicious transaction or activity; and

(v) taking any other reasonable measures to mitigate risks of money laundering, terrorist financing or proliferation financing involved.";

(f) by revoking subsection (5);

(g) by deleting subsection (6) and substituting the following subsection

"(6) The payment service provider of the payee shall keep records of any information received on the payer and the payee, as well as any information on the verification of the payee, for a period of at least 5 years

(a) from the date the wire transfer was completed, in the case of a wire transfer to a payee that does not hold an account; and

(b) from the date that the business relationship ended, in the case of a wire transfer to a payee that holds an account."; and

(h) in subsection (7), by deleting the words "the Proceeds of Criminal Conduct Act" and substituting the words, "the Act".

---

*The following Explanation to section 40 of the principal Code of Practice is inserted*

***"[Explanation:***

***(i)*** *Section 40 imposes obligations on payment service providers that receive transfers, in order to ensure that appropriate information is collected and recorded before distributing funds to a payee. In order to aid in transparency and efficient tracking of transactions, the payment service provider of the payee must have systems in place to detect whether the incoming transfer has the required full originator and full beneficiary information.*

***(ii)*** *The payment service provider of the payee must have risk-based policies and procedures in place to determine the appropriate action to take where required information is missing or incomplete. The payment service provider of the payee may decide to execute, reject or suspend the transfer and perform relevant follow-up action as outlined in subsection (4), based on the perceived ML/TF risks.*

***(iii)*** *Prior to disbursing any funds from a transfer, a payment service provider of the payee must ensure that the payee's information is accurate and up-to-date by verification of the payee's identity. Where the payee holds an account with the payment service provider of the payee, the beneficiary information may be considered verified based on the customer due diligence (including ongoing customer due diligence) measures undertaken with respect to the business relationship. However, a payment service provider of a payee may wish to verify and undertake additional customer due diligence measures on a payee prior to executing a wire transfer where higher risks are present (e.g. transfers from a high-risk jurisdiction, involvement of a higher risk third party in the transaction). For a payee that does not hold an account with the payment service provider of the payee, verification of the customer's information is not required where the transfer does not exceed $1,000 and the entity or professional does not suspect ML/TF, unless the transfer is linked to other transfers which together exceed $1,000.*

***(iv)*** *Irrespective of the amount of the transfer, whether the customer has an account with the payment service provider of the payee, or whether transfers are received for individual or batch transfers, the payment service provider of the payee must have systems in place to detect whether a transfer is suspicious and initiate internal suspicion reporting processes promptly. Some examples of suspicious behaviour relevant to transfers received may include*

- *a transfer with missing, inaccurate or incomplete information on the payer and/or the payee;*
- *a payee for whom or which beneficiary information cannot be verified;*
- *a payee seeking to route the transfer through intermediary payment service providers, with no apparent rationale; or*
- *a transfer for which there is evidence suggesting that the intended final recipient is not the payee.*

***(v)*** *The payment service provider of the payee is required to maintain records of all information received from the payment service provider of the payer and any intermediary payment service providers. These records must be maintained for a period of 5 years from the date of the transaction (in the case of a transfer to a payee that does not hold an account) or from the date a business relationship ends (in the case of a payee that is an account holder). The records must include*

- *any information that pertains to the transfer, whether received through a messaging system or through any other means; and*
- *evidence of verification of its payee identities.**]"***

---

**Section 41 amended**

**43.** Section 41 of the principal Code of Practice is amended

(a) in subsection (2), by inserting after the words "the payer", the words "and the payee";

(b) by deleting subsection (3) and substituting the following subsection

"(3) Subject to subsections (5) and (6), an intermediary payment service provider may use a system with technical limitations which prevents the information on the payer and the payee from accompanying a cross-border transfer of funds, where the intermediary payment service provider will make the transfer of funds to another payment service provider in the Virgin Islands.";

(c) by revoking subsection (4);

(d) by deleting subsection (5) and substituting the following subsection

"(5) An intermediary payment service provider that uses a system with technical limitations shall, upon request from the payment service provider of the payee, make available to the payment service provider of the payee all the information on the payer and the payee that the intermediary payment service provider has received, whether or not the information is the full originator information and full beneficiary information, within 3 working days of receiving the request, excluding the day on which the request was made.";

(e) by deleting subsection (6) and substituting the following subsection

"(6) An intermediary payment service provider that uses a system with technical limitations which prevents the information on the payer or the payee from accompanying the transfer of funds shall keep records of all the information on the payer and the payee that it has received for a period of at least 5 years from the date the transfer was completed."; and

(f) by inserting after subsection (6), the following new subsections

"(7) An intermediary payment service provider shall put in place effective procedures, consistent with straight-through processing, for the detection of wire transfers that lack full originator information and full beneficiary information.

(8) Subject to subsection (9), where an intermediary payment service provider becomes aware that the full originator information or full beneficiary information is missing or incomplete when receiving transfers of funds, the intermediary payment service provider shall, relying on its risk-based policies and procedures, determine whether to

(a) execute, reject or suspend the transfer; and

(b) undertake an appropriate follow-up action which may include

(i) requesting the missing information from the payment service provider of the payer;

(ii) rejecting future transfers of funds from the payment service provider of the payer;

(iii) restrict or terminate its relationship with the payment service provider of the payer; and

(iv) determining whether the transfer of funds or any related transaction should be reported to the Agency as a suspicious transaction or activity.

(9) Where an intermediary payment service provider executes a wire transfer that does not contain the full originator and full beneficiary information, the intermediary service provider may only use a system with technical limitations if the intermediary service provider provides confirmation to the payment service provider of the payee, that the information is incomplete."

---

*The following Explanation to section 41 of the principal Code of Practice is inserted*

***"[Explanation:***

***(i)*** *For cross-border wire transfers, an intermediary payment service provider must ensure that information on the payer and payee that it receives with a transfer is kept with the transfer, through a messaging system capable of carrying full originator information and full beneficiary information. However, where technical limitations associated with a messaging system prevents all information received on the payer and payee from accompanying the transfer, an intermediary payment*

*service provider may use the messaging system with technical limitations where the intermediary payment service provider—*

- *is forwarding the transfer to a payment service provider in the Virgin Islands; and*
- *agrees to provide all the information that accompanied the wire transfer within 3 working days after the payment service provider of the payee makes such a request.*

***(ii)*** *Intermediary payment service providers must have measures in place to identify wire transfers, including those carried out with straight-through processing, that do not have all the information on a payer and payee that would constitute full originator information and full beneficiary information. Where missing or incomplete information has been identified, the intermediary payment service provider should have risk-based policies, procedures and controls in place to determine whether to*

- *execute, suspend or reject the transfer; and*
- *apply appropriate following up action.*

***(iii)*** *Where the intermediary payment service provider determines that it should execute the transfer with the missing or incomplete information, the intermediary payment service provider must confirm to the payment service provider of the payee that the information is incomplete. This confirmation may take place via—*

- *a payment or messaging system; or*
- *another procedure that is accepted or agreed upon between the intermediary payment service provider and the payment service provider of the payee.*

***(iv)*** *Where the intermediary payment service provider decides to suspend or reject the transfer, follow-up action must be undertaken, which may include such actions outlined in subsection (8).*

***(v)*** *The intermediary payment service provider is required to maintain records of all information on the payer and payee that it receives with each transfer, for a period of 5 years.**]"***

---

**Section 41A inserted**

**44.** The principal Code of Practice is amended by inserting after section 41, the following new section

"**Payment service provider that holds both payer and payee side of transfer**

**41A**. Where a payment service provider that holds a Class A licence pursuant to the Financing and Money Services Act, Revised Edition 2020, controls both the payer and the payee side of a transfer of funds, that payment service provider shall

(a) consider the information from both the payer and payee sides of the transfer of funds in order to determine whether a suspicious transaction report should be filed; and

(b) file a suspicious transaction report in any country affected by the suspicious transfer of funds and make relevant transaction information available to the Agency and the relevant competent authority of any country affected by the suspicious transfer."

**Part VA inserted**

**45**. The principal Code of Practice is amended by inserting after Part V, the following new Part

**"PART VA**

**VIRTUAL ASSETS TRANSFERS**

**Definitions for and application of this Part**

**41B.** (1) For the purposes of this Part

"batch file transfer of virtual assets" means several individual transfers of virtual assets which are bundled together for transmission;

"beneficiary" means the natural or legal person or the legal arrangement that will own the virtual asset on completion of a transfer;

"beneficiary virtual asset service provider" means a virtual asset service provider which received a transfer of virtual assets on behalf of a beneficiary;

"complete beneficiary information", means

(a) the beneficiary's name; and

(b) the beneficiary's account number where such an account is used to process the transaction, or a unique identifier in the absence of an account number;

"complete originator information", means the name and address of the originator, together with

(a) the originator's account number where the account is used to process a transaction, or a unique identifier in the absence of an account; and

(b) the originator's date and place of birth; or

(c) the customer identification number or national identity number of the payer;

"intermediary virtual asset service provider" means a virtual asset service provider which

(a) participates in the execution of a transfer of virtual assets; and

(b) is not the originating virtual asset service provider or the beneficiary virtual asset service provider;

"obliged entity" means a person who receives a transfer of virtual assets on behalf of a beneficiary and is licensed or registered and supervised for the provision of virtual asset services in a jurisdiction outside the Virgin Islands;

"originating virtual asset service provider" means a virtual asset service provider which conducts a transfer of virtual assets on behalf of an originator;

"originator" means

(a) a person that places an order with the virtual asset service provider for the virtual asset transfer; or

(b) where the transfer is carried out by a virtual asset service provider on behalf of a client or other third party, the client or third party who owned the virtual asset immediately before the transfer;

"transfer of virtual asset" or "virtual assets transfer" means any transaction carried out on behalf of an originator with a view to making the virtual asset available to a beneficiary; and

"virtual asset service provider" means a person who provides, as a business, one or more of the following activities or operations for or on behalf of another person

(a) exchange between virtual assets and fiat currencies;

(b) exchange between one or more forms of virtual assets;

(c) transfer of virtual assets, where the transfer relates to conducting a transaction on behalf of another person that moves a virtual asset from one virtual asset address or account to another;

(d) safekeeping or administration of virtual assets or instruments enabling control over virtual assets;

(e) participation in, and provision of, financial services related to an issuer's offer or sale of a virtual asset;

(f) perform such other activity or operation as may be specified by enactment.

(2) This Part applies to the transfer of virtual assets which is sent or received by a virtual asset service provider that is established in the Virgin Islands.

(3) A virtual assets service provider shall comply with all the relevant requirements of this Part, in the countries in which it operates directly or through its agents.

**Originating virtual asset service provider**

**41C.** (1) An originating virtual asset service provider shall, in relation to every transfer

(a) obtain and maintain complete originator information and complete beneficiary information on each transfer of virtual assets; and

(b) submit complete originator information and complete beneficiary information to the beneficiary virtual assets service provider or obliged entity, with the transfer of virtual assets.

(2) Subsection (1) does not apply in the case of a batch file virtual asset transfer from a single payer, if

(a) the batch file contains complete originator information and complete beneficiary information that is fully traceable within the beneficiary's country; and

(b) the individual virtual assets transfers bundled together in the batch file carry the account number of the payer or a unique identifier.

(3) The originating virtual assets service provider shall, before transferring any virtual assets, verify the complete originator information on the basis of documents, data or information obtained from a reliable and independent source.

(4) In the case of a transfer from an account, the originating virtual assets service provider may deem verification of the complete originator information to have taken place if it has complied with the provisions of the Anti-money Laundering Regulations, Revised Edition 2020, and this Code relating to the verification of the identity of the originator in connection with the opening of that account.

(5) In the case of a transfer of virtual assets not made from an account, the complete originator information on the payer shall be deemed to have been verified by an originating virtual assets service provider if

(a) the virtual assets transfer does not exceed $1,000 in value;

(b) the virtual assets transfer is not carried out in several operations that appear to be linked and that together comprise a value exceeding $1,000; and

(c) the originating virtual assets provider does not suspect that the originator is engaged in money laundering, terrorist financing, proliferation financing or other financial crime.

(6) Information accompanying a transfer of virtual assets in accordance with subsection (1) shall be provided to the beneficiary virtual assets service provider or obliged entity

(a) simultaneously with the transfer of virtual assets;

(b) either directly by attaching the information with the transfer, or providing the information indirectly; and

(c) in a secure manner that protects

(i) the integrity and use of the information; and

(ii) the information from unauthorised disclosure.

(7) A beneficiary virtual assets service provider shall, upon request from the Agency or Commission, provide complete originating information and complete beneficiary information that accompanies a transfer of virtual assets, within 3 working days of receiving the request, excluding the date on which the request is made.

(8) Where a beneficiary virtual assets service provider fails to comply with a request from the Agency or Commission pursuant to subsection (7), it or he or she commits an offence and is liable to be proceeded against under section 27 (4) of the Act.

(9) The originating virtual assets service provider shall keep records of complete originator information and complete beneficiary information that accompany the transfer of virtual assets, for a period of at least 5 years

(a) from the date of the transfer, in the case of a transfer not made from an account; and

(b) from the date that the business relationship ended, in the case of a transfer made from an account.

(10) The originating virtual assets service provider shall not execute a transfer of virtual assets where the transfer of virtual assets does not comply with the requirements of this section.

**Beneficiary Virtual Asset Service Provider**

**41D**. (1) A beneficiary virtual assets service provider shall

(a) on receipt of a transfer of virtual assets, obtain and maintain complete originating information and complete beneficiary information on each transfer of virtual assets received; and

(b) put effective procedures in place for the detection of incomplete or missing complete originator information or complete beneficiary information, including post-event monitoring or real-time monitoring, where feasible.

(2) In the case of batch file virtual assets transfers, complete originator information and complete beneficiary information are required only in the batch file, and not in the individual virtual assets transfers bundled together in it.

(3) A beneficiary virtual assets service provider shall verify the accuracy of information on the beneficiary under paragraph (1) on the basis of documents, data or information obtained from a reliable and independent source.

(4) In the case of a transfer to an account, the beneficiary virtual assets service provider may deem verification of the beneficiary to have taken place if it has complied with the provisions of the Anti-money Laundering Regulations, Revised Edition 2020, and this Code relating to the verification of the identity of the beneficiary in connection with the opening of that account.

(5) In the case of a transfer of virtual assets not made to an account, the beneficiary shall be deemed to have been verified by a virtual assets service provider if

(a) the virtual assets transfer does not exceed a value of $1,000;

(b) the virtual assets transfer is not carried out in several operations that appear to be linked and that together comprise a value exceeding $1,000; and

(c) the beneficiary virtual assets service provider does not suspect that the beneficiary is engaged in money laundering, terrorist financing, proliferation financing or other financial crime.

(6) Where a beneficiary virtual assets service provider becomes aware that the complete originator information or complete beneficiary information is missing or incomplete

when receiving a transfer of virtual assets, the virtual assets service provider shall have risk-based policies and procedures to determine whether to

(a) execute, reject or suspend the transfer; and

(b) undertake an appropriate follow-up action, which may include

(i) requesting the missing information on the originator;

(ii) rejecting future transfers of funds from the originating virtual assets service provider;

(iii) restricting or terminating its relationship with the originating virtual assets service provider;

(iv) determining whether the transfer of virtual assets or any related transaction should be reported to the Agency as a suspicious transaction or activity; and

(v) taking any other reasonable measures to mitigate risks of money laundering, terrorist financing or proliferation financing involved.

(7) A beneficiary virtual assets service provider shall, upon request from the Agency or Commission, provide complete originating information and complete beneficiary information that accompanies a transfer of virtual assets, within 3 working days of receiving the request, excluding the date on which the request is made.

(8) A beneficiary virtual assets service provider shall keep records of complete originating information and complete beneficiary information which accompanies each transfer of virtual assets, for at least 5 years

(a) from the date the transfer was completed, in the case of a transfer to a beneficiary that does not hold an account; and

(b) from the date that the business relationship ended, in the case of a transfer to a beneficiary that holds an account.

(9) A person who fails to comply with a provision of this section commits an offence and is liable to be proceeded against under section 27 (4) of the Act.

**Intermediary virtual assets service provider**

**41E**. (1) This section applies where the intermediary virtual assets service provider is situated within the Virgin Islands.

(2) An intermediary virtual assets service provider shall

(a) ensure that any information it receives on the originator and the beneficiary that accompanies a transfer of virtual assets is kept with that transfer; and

(b) put effective procedures in place for the detection of virtual assets transfers that lack complete originator information and complete beneficiary information, consistent with straight-through processing.

(3) Where the intermediary virtual assets service provider becomes aware that the complete originator information or complete beneficiary information is missing or incomplete

when receiving transfers of funds, the intermediary virtual assets service provider shall, relying on its risk-based policies and procedures, determine whether to

(a) execute, reject or suspend the transfer; and

(b) undertake an appropriate follow-up action which may include

(i) requesting the missing information from the originating virtual assets service provider;

(ii) rejecting future transfers of funds from the originating virtual assets service provider;

(iii) restrict or terminate its relationship with the originating virtual assets service provider; and

(iv) determining whether the transfer of virtual assets or any related transaction should be reported to the Agency as a suspicious transaction or activity.

(4) An intermediary virtual assets service provider shall, upon request from the Agency or Commission, provide complete originating information and complete beneficiary information that accompanies a transfer of virtual assets, within 3 days working days of receiving the request, excluding the date on which the request is made.

(5) An intermediary virtual assets service provider shall, for at least 5 years from the date of the transfer, keep records of complete originating information and complete beneficiary information which accompanies each transfer of virtual assets.

**Virtual assets service provider that holds both payer and payee side of transfer**

**41F**. Where a virtual assets service provider that holds or controls both the originator and the beneficiary side of a transfer of virtual assets, that virtual assets service provider shall

(a) consider the information from both the originator and beneficiary sides of the transfer of funds in order to determine whether a suspicious activity report should be filed; and

(b) file a suspicious activity report in any country affected by the suspicious transfer of virtual assets, and make relevant transaction information available to the Agency and the relevant competent authority of any country affected by the suspicious transfer."

**Section 42 amended**

**46.** Section 42 of the principal Code of Practice is amended by deleting subsection (2) and substituting the following subsection

"(2) A record of a business relationship or transaction, any attempt to establish a business relationship or transaction which has not been completed, or any other matter required to be maintained under the Anti-money Laundering Regulations, Revised Edition 2020, and this Code shall, unless otherwise prescribed, be maintained in a form that it can be

(a) easily retrievable; and

(b) promptly provided when requested by the Agency, the Commission, a law enforcement agency or other person entitled to access them."

---

*The Explanation to section 42 of the principal Code of Practice is amended*

*(a) in paragraph (i)*

*(i) in the first sentence, by deleting the words "FATF Recommendation 10 provides" and substituting the words, "FATF Recommendations provide"; and*

*(ii) in the second sentence, by inserting after the words "terrorist financing", the words ", proliferation financing";*

*(b) in paragraph (ii)*

*(i) by deleting the words "within a reasonable period" wherever they appear in the paragraph and substituting the word, "promptly"; and*

*(ii) by deleting the last sentence; and*

*(c) in paragraph (iii)*

*(i) by deleting the first 2 sentences and substituting the following sentences*

***"****The minimum retention period of records required under the AMLR and this Code is 5 years. However, there may be circumstances where it becomes necessary to retain records for longer periods extending beyond the prescribed minimum."; and*

*(ii) by deleting the last sentence of the paragraph.*

**Section 43 revoked**

**47.** Section 43 of the principal Code of Practice is revoked.

**Section 44 amended**

**48.** Section 44(c) of the principal Code of Practice is amended by deleting the word "monetary".

---

*The Explanation to section 44 of the principal Code of Practice is amended*

*(a) by deleting paragraph (i) and substituting the following paragraph*

***"(i)*** *Every entity or professional must ensure that sufficient information is obtained with respect to every transaction involving or relating to a customer and other persons connected therewith as may be appropriate. Different transactions may present different levels of risk which in turn may obligate or necessitate the taking and maintaining of records additional to those outlined in section 44. This is in line with an entity's or professional's customer due diligence process, which requires varying types of information and documentation, depending on the risks present with respect to any particular transaction. An entity or professional must maintain sufficient, clear and*

*reliable records of the information and documentation and the action taken with respect to each transaction that can be readily accessed whenever required."; and*

*(b) in paragraph (ii), in the opening paragraph, by inserting after the words "with a customer", the words "or the level of ML/TF and PF risk posed by a customer".*

---

**Section 45 amended**

**49.** Section 45 of the principal Code of Practice is amended

(a) in subsection (1)

(i) in the opening paragraph, by inserting after the words "terrorist financing", the words ", proliferation financing";

(ii) in paragraph (a), by inserting after the words "customer due diligence,", the words "undertaking risk assessments,";

(iii) in paragraph (g), by deleting the word "and" at the end of the paragraph;

(iv) in paragraph (h), by deleting the full-stop at the end of the paragraph and substituting the words "and customers; and"; and

(v) by inserting after paragraph (h), the following new paragraph

"(i) any other records that may be required to be maintained pursuant to the provisions of the Anti-money Laundering Regulations, Revised Edition 2020, and this Code.";

(b) in subsection (2)(b)

(i) by deleting the words "subsection (1)(e), (f), (g) and (h)," and substituting the words, "subsection (1)(b), (e), (f), (g) and (h),"; and

(ii) by deleting the words "relationship ended" and substituting the words, "relationship was terminated";

(c) in subsection (3), by deleting the words "money laundering and terrorist financing" and substituting the words, "money laundering, terrorist financing and proliferation financing"; and

(d) in subsection (4)(b), by inserting after the words "having regard to", the words "to the risks presented by".

---

*The Explanation to section 45 of the principal Code of Practice is amended*

*(a) in paragraph (i), by inserting after the words "terrorist financing", the words ", proliferation financing"; and*

*(b) in paragraph (iv), by deleting the first sentence and substituting the following sentence*

*"(iv) Where an entity that is a financial institution maintains a business relationship relative to an account that is dormant, it is required to continue to maintain records with respect to that account until the business relationship is terminated in accordance with regulation 10 (1) of the AMLR.".*

---

**Section 46 amended**

**50.** Section 46 of the principal Code of Practice is amended in subsections 1(b) and 2(b), by deleting the words "money laundering or terrorist financing" and respectively substituting the words, "money laundering, terrorist financing or proliferation financing".

---

*The Explanation to section 46 of the principal Code of Practice is amended in paragraph (iii), by inserting at the end of the last sentence, before the full-stop, the words, ", allowing the entity or professional to have access to the records, whenever necessary".*

---

**Section 47 amended**

**51.** Section 47 of the principal Code of Practice is amended

(a) in subsection (1)(a), by deleting the words "money laundering and terrorist financing" and substituting the words, "money laundering, terrorist financing and proliferation financing";

(b) in subsections (2) and (3), by deleting the words "anti-money laundering and terrorist financing" and respectively substituting the words, "anti-money laundering, terrorist financing and proliferation financing";

(c) in subsection (4), by deleting paragraph (c) and substituting the following paragraph

"(c) an entity that is a fund or private investment fund registered or recognised under the Securities and Investment Business Act, Revised Edition 2020, or an approved or incubator fund under the Securities and Investment Business (Incubator and Approved Funds) Regulations, Revised Edition 2020; or"; and

(d) in subsection (5)(b)(i), by deleting the words, "a restricted Class II or Class III trust licence" and substituting the words, "a restricted Class II trust licence or restricted Class III licence".

---

*The Explanation to section 47 of the principal Code of Practice is amended*

*(a) in paragraphs (i) and (ii), by deleting the words, "money laundering and terrorist financing" and respectively substituting the words, "money laundering, terrorist financing and proliferation financing"; and*

*(b) in paragraph (iv), by inserting after the words "overseas training," the words, "virtual training, webinars,".*

**Section 48 amended**

**52.** Section 48(2)(b) and (d) of the principal Code of Practice is amended, by deleting the words "money laundering and terrorist financing" and respectively substituting the words, "money laundering, terrorist financing and proliferation financing".

*The Explanation to section 48 of the principal Code of Practice is amended*

*(a) in paragraph (ii), in the closing paragraph, by inserting after the words "face to face arrangement" the words, "or through virtual means"; and*

*(b) in paragraph (iii), by deleting the second sentence and substituting the following sentence*

*"For the purposes of this Part of the Code and the AMLR, training or re-training must be afforded at least once every year, and entities or professionals that operate in sectors that are most vulnerable to money laundering, terrorist financing and proliferation financing activities may undertake training on a more frequent basis."*

**Section 49 amended**

**53.** Section 49 of the Code of Practice is amended

(a) by revoking subsection (2) and substituting the following subsection

"(2) Where an entity or a professional

(a) terminates or dismisses an employee on account of the employee's competence with respect to compliance with anti-money laundering, terrorist financing and proliferation financing requirements,

(b) terminates, dismisses or disciplines an employee on account of his or her probity, or

(c) discovers, after an employee had ceased to be an employee of the entity or professional (whether through resignation, retirement, transfer, exchange, or otherwise), that the employee had, while employed with the entity or professional, been engaged in an activity which raises questions about the employee's probity,

the entity or professional, as the case may be, shall, within 7 days of the occurrence or discovery of the event mentioned in paragraph (a), (b) or (c), notify in writing the Commission (in the case of entities or professionals regulated by the Commission), or the Agency (in the case of entities or professionals supervised by the Agency), of that fact providing the name and address of the employee or former employee and detailed information as would enable the Commission or the Agency to fully understand the circumstances and reason for the occurrence of the event.";

(b) by inserting after subsection (2), the following new subsections

(2A) The Commission or the Agency shall establish a system for recording and maintaining the names of employees or former employees of an entity or a professional in relation to whom a notification has been made under subsection (2).

(2B) The Commission or the Agency may use the system established under subsection (2A), including the names recorded or maintained in the system, for purposes of

(a) in the case of the Commission, discharging its functions under the Financial Services Commission Act, Revised Edition 2020, or any other enactment;

(b) in the case of the Agency, discharging its functions under the Financial Investigation Agency Act, Revised Edition 2020; or

(c) in any other case, ensuring that appropriate steps are taken to prevent an employee or a former employee who has been the subject of a notification under subsection (2) from further engaging in any conduct or activity that led to his or her name being notified to the Commission or the Agency.

(2C) Subsection (2B)(c) is without prejudice to an employee's or former employee's right, at any time, to make representations to the Commission or the Agency regarding

(a) the circumstances and reason for the termination of, or dismissal from, his or her employment, or the initiation of disciplinary action against him or her by his or her former employer; and

(b) why his or her name should not be included in, or should be removed from, the system established under subsection (2A) for the recording of names of employees or former employees; or

(c) in the case of a former employee to whom subsection (2) applies, why his or her name should be included in, or should be removed from, the system established under subsection (2A) for the recording of names of employees or former employees.

---

*The Explanation to section 49 of the principal Code of Practice is deleted and substituted by the following Explanation*

***(i)*** *Competence and probity are critical to the efficient and effective functioning of an AML/CFT regime. Persons whose competence fall short of the desired standards after having been trained and whose continued employment is likely to pose potential AML/CFT risks, having regard to their specific area of employment, must be closely monitored. In addition, an employee who has questionable integrity may be willing to forego the AML/CFT obligations of the entity or professional or facilitate ML/TF activities through the entity or professional. Where as a consequence of inadequate competence and integrity their employment is terminated, this must be notified immediately to the Commission (for entities or professionals regulated by the Commission) or the Agency (for entities or professionals supervised by the Agency) . An*

*entity or a professional must not shield such an employee by failing to notify the Agency or the Commission, notwithstanding any internal settlement that might have been reached; to do so will constitute an offence and criminal proceedings may be instituted against the entity or professional concerned.*

***(ii)*** *The situation may also arise where an employee commits a fraud or other offence or commits a breach of an entity's or a professional's internal control systems to engage in questionable transactions and then resigns, retires, or is transferred or exchanged (for example to or between a parent entity and a subsidiary). The later discovery of such conduct or activity should be reported to the Commission or Agency, as the case may be. This will apply to any other conduct or activity bordering on probity, irrespective of whether the conduct or activity was discovered whilst in employment or after the cessation of employee.*

***(iii)*** *The Commission and the Agency are required to establish a system in which they record and maintain the names of employees or former employees whose conduct or activity is reported to the Commission or the Agency. The system established may be in the form of creating a watch list or through some other mechanism. The important thing is that a record should exist within the Commission or the Agency of the reports made to it. Each report should be sufficiently detailed to enable the Commission or the Agency to understand and have a full appreciation of the nature and circumstances of the conduct or activity for which a report is made to the Commission or the Agency. The details provided may not necessarily be uniform across the board, but must at a minimum contain the date of occurrence or discovery of the event reported, the employee's or former employee's name, address, date of employment, status within the entity or professional as at the date or termination, suspension, dismissal, discipline, resignation, retirements, etc., nature of the conduct or activity, the internal control systems that were breached and how such systems were breached, possible oversight failures, action taken or being taken, to whom reports have been made, etc. This list is simply a guide and is not exhaustive. Each entity or professional submitting a report must include in the report every detail that will assist a better understanding of the subject of the report.*

***(iv)*** *Furthermore, both the Commission and the Agency have a responsibility for properly guarding the financial perimeter of the Territory. That means taking necessary steps to prevent reported employees from occupying positions of responsibility within an entity or a professional in the Territory where the Commission or the Agency considers such steps necessary and justified. This may include publishing the name of a reported person whose conduct or activity has resulted in a conviction, disclosing the name of a reported person to a judicial authority or law enforcement agency, or simply sharing with a competent authority or licensee the facts relative to an employee or former employee as reported to the Commission or the Agency.*

***(v)*** *However, consideration must be given to an employee's or former employee's right to due process. Ideally, where the Commission or the Agency is aware of the employee's or former employee's presence in the Territory at the time he or she is reported, he or she should be notified of the report and invited to make such representation to the Commission or the Agency, as the case may be, as he or she deems fit. The Commission or Agency may, after receipt and proper consideration of any representation made, determine whether to include the employee's or former employee's name as provided*

*under section 49(2A). If, on the other hand, the employee or former employee cannot be reached, that does not prevent him or her from making representation to the Commission or Agency at any time.*

***(vi)*** *These steps shall, however, not prevent the Commission or Agency from including a reported employee's or former employee's name on the system (list) established and maintained by the employer. The Commission or Agency may, at any time after reviewing an employee's or former employee's representation, remove his or her name from the system if it determines that such removal is justified.***"**

---

**Section 50 amended**

**54.** Section 50 of the principal Code of Practice is amended

(a) in subsection (1)

(i) by inserting after the words "The Agency and the Commission shall", the words ", as far as possible, jointly"; and

(ii) by deleting the words "money laundering and terrorist financing" and substituting the words, "money laundering, terrorist financing and proliferation financing";

(b) in subsection (2)

(i) in paragraph (a), by deleting the words "money laundering and terrorist financing" and substituting the words, "money laundering, terrorist financing and proliferation financing";

(ii) in paragraph (b), by inserting after the words "Anti-terrorism (Financial and Other Measures) (Overseas Territories) Order," the words, "Counter-Terrorism Act, No. 33 of 2021, Proliferation Financing (Prohibition) Act, No. 20 of 2021"; and

(iii) in paragraph (d), by deleting the words "money laundering or terrorist financing" and substituting the words, "money laundering, terrorist financing or proliferation financing";

(c) in subsection (3)

(i) by deleting paragraph (b), and substituting the following paragraph

"(b) Her Majesty's Customs;";

(ii) by deleting paragraph (f) and substituting the following paragraph

"(f) the BVI Airports Authority;";

(iii) by deleting paragraph (h) and substituting the following paragraph

"(h) the Virgin Islands Shipping Registry;";

(iv) by deleting paragraph (i) and substituting the following paragraph

"(i) the Department of Trade and Consumer Affairs";

(v) in paragraph (j) by deleting the words, "money laundering and terrorist financing" and substituting the words "money laundering, terrorist financing and proliferation financing".

---

*The Explanation to section 50 of the Code of Practice is amended*

*(a) in the third sentence, by inserting after the words "the 2002 Order" the words, ", PFPA, CTA"; and*

*(b) in the fourth sentence, by deleting the words, "money laundering and terrorist financing" and substituting the words "money laundering, terrorist financing and proliferation financing".*

---

**Section 51 amended**

**55.** Section 51(2)(a) and (b) of the principal Code of Practice is amended, by deleting the words "money laundering and terrorist financing" and substituting the words, "money laundering, terrorist financing and proliferation financing".

*The Explanation to section 51 of the principal Code of Practice is amended in paragraphs (i) and (ii), by deleting the words "money laundering and terrorist financing" and substituting the words, "money laundering, terrorist financing and proliferation financing".*

**Section 52 revoked**

**56.** Section 52 of the principal Code of Practice is revoked.

**Section 53 amended**

**57.** Section 53 of the principal Code of Practice is amended

(a) in subsection (1)

(i) by deleting the words, "that is regulated in the Virgin Islands" and substituting the words, "or a professional"; and

(ii) by inserting after the word "subsidiaries", wherever it appears, the word, ", agencies";

(b) in subsection (1A)

(i) by inserting after the words "An entity", the words "or a professional";

(ii) by inserting after the word "subsidiaries", the word ", agencies"; and

(iii) by deleting the words "anti-money laundering and terrorist financing" and substituting the words, "anti-money laundering, terrorist financing and proliferation financing";

(c) in subsection (2)

(i) by inserting after the words "the entity's", the words "or professional's";

(ii) by inserting after the word "subsidiaries", wherever it appears, the word ", agencies"; and

(iii) by inserting after the words "the entity", the words "or professional";

(d) in subsection (3)

(i) by inserting after the words "an entity", the words "or a professional";

(ii) by inserting after the word "subsidiaries", wherever it appears, the word ", agencies";

(e) by deleting subsection (3A) and substituting the following subsection

"(3A) An entity or a professional that has branches, subsidiaries, agencies or representative offices operating in foreign jurisdictions shall notify the Agency (in the case of an entity or a professional supervised by the Agency) or the Commission (in the case of an entity or a professional licensed by the Commission) in writing if any of the entity's or professional's branches, subsidiaries, agencies or representative offices is unable to observe appropriate anti-money laundering, terrorist financing and proliferation financing measures on account of the fact that such observance is prohibited by the laws, policies or other measures of the foreign jurisdiction in which it operates."; and

(f) by deleting subsection (3B) and substituting the following subsection

"(3B) Where a notification is provided pursuant to subsection (3A), the entity or professional shall apply appropriate additional measures to manage the risks related to the operation of its or his or her branches, subsidiaries, agencies or representative offices in that foreign jurisdiction.".

---

*The Explanation to section 53 of the principal Code or Practice is amended*

*(a) in the first sentence of the paragraph, by inserting after the words "An entity", the words "or a professional";*

*(b) by inserting after the word "entity's", wherever it appears in the paragraph, the words "or professional's"; and*

*(c) by inserting after the words "the entity", wherever they appear, the words "or professional".*

---

**Section 53A inserted**

**58.** The principal Code of Practice is amended by inserting after section 53, the following new section

**"Financial groups**

**53A.** A financial group shall implement group wide policies, procedures and controls against money laundering, terrorist financing and proliferation financing which are

applicable to all branches and subsidiaries of the financial group, and these policies and procedures shall include

(a) policies, procedures and controls required under Part II (Establishing Internal Control Systems), Part III (Establishing Customer Due Diligence Measures), Part VI (Record Keeping Requirements) and Part VII (Employee Training);

(b) policies and procedures for sharing information required for the purposes of customer due diligence and money laundering, terrorist financing and proliferation financing risk management;

(c) the provision, at group-level compliance, audit and AML/CFT functions, of customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT purposes; and

(d) adequate safeguards on confidentiality and use of information exchanged.".

**Section 54 amended**

**59.** Section 54 of the principal Code of Practice is revoked and substituted by the following section

**"Application of counter-measures**

**54**. (1) This section applies in relation to

(a) the Commission only with regard to entities and professionals that are licensed or supervised by the Commission; and

(b) the Agency only with regard to entities and professionals that are supervised by the Agency for compliance with the laws relating to money laundering, terrorist financing and proliferation financing.

(1A) Where the FATF, CFATF or any other similar organisation advises that measures should be undertaken in relation to a jurisdiction, or the Agency or the Commission forms the opinion that a jurisdiction with which the Virgin Islands engages in business or the provision of any service through an entity or a professional poses a significant money laundering, terrorist financing or proliferation financing risk, the Agency or the Commission may

(a) issue advisories advising entities and professionals of the weaknesses in the AML/CFT system of the jurisdiction and that transactions with individuals, legal persons and legal arrangements in the jurisdiction may run the risk of money laundering, terrorist financing or proliferation financing; or

(b) require entities and professionals to apply counter-measures, proportionate to the risks, in relation to that jurisdiction.

(2) The counter-measures referred to in subsection (1) in relation to a jurisdiction may include requiring entities and professionals to undertake any of the following

(a) apply stringent requirements for the identification and verification of applicants for business or customers in the jurisdiction, including

requirements for the establishment of beneficial owners of legal persons and legal arrangements before any business relationship is established;

(b) enhance reporting mechanisms or systematic reporting of financial transactions on the basis that such transactions with the jurisdiction are more likely to be suspicious;

(c) limit business relationships or financial transactions with the jurisdiction or persons within that jurisdiction; and

(d) discontinue from engaging in any kind of business relationship emanating from or relating to such jurisdiction.

(3) Where the Agency or the Commission requires the application of a counter-measure pursuant to subsection (1), an entity or a professional that contravenes or fails to comply with the counter-measure commits an offence and is liable to be proceeded against under section 27(4) of the Act.

---

***[Explanation:***

*This section seeks to implement the FATF Recommendation in relation to jurisdictions that do not apply or insufficiently apply the FATF Recommendations and/or have weaknesses in their AML/CFT systems. The FATF, CFATF and/or other international organisation with similar functions issue advisories in relation to jurisdictions that do not apply or insufficiently apply FATF Recommendations. These advisories require entities and professionals to apply particular counter measures when engaging in business with customers and counterparts in those jurisdictions. Entities and professionals must comply with the advisories when issued. In addition, the Commission based on their own evaluation, or receiving input from other authorities responsible for AML/CFT in the Territory, may also deem that certain jurisdictions pose significant ML/TF risks and require entities and professionals to undertake certain counter measures in engaging in business with the named jurisdictions. The essence of such measures is simply to protect entities and professionals against dealings in possible money laundering, terrorist financing or proliferation financing activities with persons (legal or natural) in such jurisdictions, in addition to assuring the reputation of the Virgin Islands. Accordingly, it is expected that entities and professionals will be vigilant and ensure that the jurisdictions with or in which they form business relationships have in place AML/CFT measures; where these are considered insufficient, an entity or a professional must, as a first step, employ enhanced customer due diligence measures to identify and verify the relevant applicant for business or customer.]"*

---

**Section 55 amended**

**60.** Section 55(1) of the principal Code of Practice is amended in the opening paragraph, by inserting after the words "submitted in writing", the words "(including in electronic form)".

**Section 56 amended**

**61.** Section 56(1) of the principal Code of Practice is amended, by deleting the words, "money laundering or terrorist financing" and substituting the words, "money laundering, terrorist financing or proliferation financing".

**Schedule 1 revoked and substituted**

**62**. Schedule 1 of the principal Code of Practice is revoked and substituted by the following Schedule

**"SCHEDULE 1**

*[Section 4A (8)]*

**BEST PRACTICES FOR NPOs**

***A. Introduction***

It is generally recognised globally that the set-up and operation of NPOs are susceptible to misuse for money laundering, terrorist financing and proliferation financing purposes. While taking on different forms (such as association, organisation, foundation, corporation, committee for fund raising or community service, limited guarantee company and unlimited company, all of which may be formed pursuant to the BVI Business Companies Act or some other enabling enactment) to provide services for charitable, educational, cultural, religious, community, social and fraternal purposes, recent developments have shown that NPOs have become convenient conduits for facilitating the laundering of ill-gotten gains and for providing funding to organisations that carry out or facilitate the carrying out of terrorist activities, as a result of the trust placed in them. Accordingly, it is essential that every NPO exercises vigilance in its dealings with persons who present themselves or appear to be friends of and benevolent givers of donations for general or specific activities.

It is therefore significant that every NPO understands and appreciates its objectives and adopt appropriate measures designed to protect it from misuse for money laundering, terrorist or other financial criminal activities. These Best Practices are not designed to prevent or discourage NPOs from sourcing and accepting funds from reliable and legitimate sources. Rather, they are designed to assist NPOs to better insulate themselves against abuse for money laundering, terrorist financing, proliferation financing and other financial crime activities.

In this vein, NPOs should note that there may be business relationships or transactions their organisations may be concerned with which their managers may not be fully aware or have full appreciation of. The same may apply to donors who give out in good faith (whether through solicitation or otherwise), just to have their donations channelled for unlawful or other unintended purposes. Thus it becomes incumbent on everyone (NPOs, their employees, donors and supervisors or regulators) to guard the perimeter against abuse and misuse.

***B. Guiding Principles***

These Best Practices are guided by the following principles

1. NPOs will be encouraged to promote, encourage and safeguard within the context of the laws of the Virgin Islands the practice of charitable giving and the strong and diversified community of institutions through which they operate.

2. The effective oversight of NPOs and their activities is a cooperative undertaking which requires the effective participation of the Agency, Commission, Government, charity supporters (donors and other philanthropic persons) and the persons whom NPOs serve.

3. The Agency (as supervisor or any other body replacing the Agency as such) and NPOs must at all times seek to promote transparency and accountability and, more broadly, common social welfare and security goals with respect to the operations of the NPOs.

4. While small NPOs by their operations do not engage in raising significant amounts of money in excess of $50,000 per annum from private and public sources or which merely concentrate on redistributing resources among their members may not pose serious threats to money laundering, terrorist financing or proliferation financing activity and therefore not require regular and enhanced oversight, they must recognise that they are susceptible to unlawful laundering and financing activity and adopt appropriate measures to protect themselves and the reputation of the Virgin Islands.

5. In particular, NPOs must establish transparency, accountability and probity in the manner in which they collect, transmit or distribute funds.

6. All NPOs must recognise that no charitable endeavour must be undertaken that directly or indirectly supports money laundering, terrorist financing, proliferation financing or other financial crime, including actions that may serve to induce or compensate for participation in such activity.

7. While NPOs are (until otherwise replaced by an overriding enactment) supervised by the Agency pursuant to section 5C(2) of the Financial Investigation Agency Act, Revised Edition 2020, they are encouraged to develop, maintain and strengthen mechanisms for self-regulation as a significant means of decreasing the risks associated with money laundering, terrorist financing, proliferation financing and other financial crimes.

## *C. <u>Adopting Preventive Measures</u>*

The measures outlined hereunder must be viewed as supplementing the provisions of the Code and are not designed to derogate from the intent, objectives or obligations of the Code.

***(a) NPOs must adopt measures that ensure transparency in their financial dealings. This must take into account the nature, volume and complexity of, as well as the risk that may be associated with, the financial dealings. In this respect, NPOs must, to the extent feasible and necessary, observe the following guidelines***

(i) prepare and maintain full and accurate programme budgets that reflect all programme expenses, including recording the identities of recipients and how funds are utilised;

(ii) adopt and maintain a system of independent auditing as a means of ensuring that accounts accurately reflect the reality of finances; and

(iii) maintain registered bank accounts in which to keep funds and to utilise formal channels for transferring funds, whether locally or overseas, and perform other financial transactions.

***(b) It is essential that every NPO adopts appropriate policies and procedures which ensure the adequate verification of their activities, especially where they operate foreign activities. This aids the process of determining whether planned programmes are being implemented as intended. The following guidelines must therefore be observed***

(i) every solicitation for a donation must accurately and transparently inform donors the purpose and intent for which the donation is being collected;

(ii) funds collected through solicitation and funds received through unsolicited donations must be utilised for the purpose for which they are collected or received;

(iii) in order to ensure that funds are applied for the benefit of intended beneficiaries, the following must be carefully considered

- whether the programme or project for which funds are provided have in fact been carried out;
- whether the intended beneficiaries exist;
- whether the intended beneficiaries have received the funds meant for them; and
- whether all the funds, assets and premises have been fully accounted for;

(iv) where, having regard to the nature, size and complexity of and risk associated with a programme or project, it becomes necessary to conduct direct field audits, this must be carried out in order to guard against malfeasance and detect any misdirection of funds; and

(v) where funds are delivered to an overseas location, appropriate measures must be adopted to account for the funds and make a determination as regards their use.

***(c) Central to the efficient and effective functioning of an NPO is the establishment of a robust administrative machinery that ensures the appropriate and routine documentation of administrative, managerial, compliance and policy development and control measures with respect to the operations of the organisation. Accordingly, the following guidelines must be observed***

(i) directors and/or managers (or persons appointed or deputed to perform such functions) must act with due diligence and ensure that the organisation functions and operates ethically;

(ii) directors and/or managers (or persons appointed or deputed to perform such functions) need to know the persons acting in the name of the organisation (such as executive directors, diplomats, fiduciaries and those with signing authority on behalf of the organisation);

(iii) directors and/or managers (or those appointed or deputed to perform such functions) must exercise due care, diligence and probity and, adopt where necessary, proactive verification measures to ensure that their partner organisations and those to which they provide funding, services or material support are not being penetrated or manipulated by criminal groups, including terrorists;

(iv) the directors and/or managers (or persons appointed or deputed to perform such functions) have responsibilities to

- their organisation and its members to act honestly and with vigilance to ensure the financial health of the organisation;
- their organisation and its members to diligently dedicate their service to the mandate(s) of the organisation;
- the persons, such as donors, clients and suppliers, with whom the organisation interacts;
- the Agency which has supervisory responsibility over the organisation; and
- the persons, including the Government, who provide donations or other forms of financial assistance to the organisation, whether on a regular basis or otherwise;

(v) where an NPO functions with a board of directors, the board must

- have in place adequate measures to positively identify every board member, both executive and non-executive;
- meet on a reasonably periodic basis, keep records of its proceedings (including the decisions taken);
- have in place appropriate formal arrangements regarding the manner in which appointments to the board are effected and how board members may be removed;
- adopt appropriate measures to ensure the conduct of an annual independent review of the finances and accounts of the organisation;
- adopt policies and procedures which ensure appropriate financial controls over programme spending, including programmes that are undertaken through agreements with other organisations;
- ensure that there is an appropriate balance between spending on direct programme delivery and administration; and
- ensure that there are appropriate policies and procedures to prevent the use of the organisation's facilities or assets to support or facilitate money

laundering, terrorist financing, proliferation financing or other financial crime."

**Schedule 2 revoked**

**63**. Schedule 2 of the principal Code of Practice is revoked.

**Schedule 4 revoked and substituted**

**64.** Schedule 4 of the principal Code of Practice is revoked and substituted by the following Schedule

**"SCHEDULE 4**

*[Section 57 (1)]*

**OFFENCES AND ADMINISTRATIVE PENALTIES**

| **COLUMN 1** ***Section of the Code creating offence.*** | **COLUMN 2** ***General nature of offence.*** | **COLUMN 3** ***Penalty (Corporate body)*** | **COLUMN 4** ***Penalty (Individual)*** |
|---|---|---|---|
| 4A (3), (5), (6) and (8) | Failure to comply with requirements of subsection (1), or carry out customer due diligence and record keeping measures, or accepting donations linked to money laundering, terrorist financing or proliferation financing | $100,000 | $80,000 |
| 11 | Failure to comply with the requirements of section 11 | $100,000 | $80,000 |
| 12 | Failure to carry out money laundering, terrorist financing and proliferation financing risk assessments | $100,000 | $80,000 |
| 14 | Failure to comply with the measures required under section 14 (2) | $100,000 | $80,000 |
| 15 | Failure by an employee to comply with the requirements under section 15 | - | $75,000 |
| 16 (3) | Failure to comply with the prescribed obligations in relation to a Reporting Officer | $65,000 | $60,000 |
| 18 (1) | Failure by an employee to report a suspicious activity or transaction | - | $80,000 |

| | | | |
|---|---|---|---|
| 19 (2), (4) and (5) | Failure to engage in or undertake customer due diligence, or additional customer due diligence in the case of a trustee of a trust or a legal person | $100,000 | $80,000 |
| 20 | Failure to engage in enhanced customer due diligence | $100,000 | $80,000 |
| 21 | Failure to undertake ongoing customer due diligence | $75,000 | $70,000 |
| 29 (2) and (4) | Failure to adopt relevant measures or additional measures or checks in non-face to face relationships | $100,000 | $80,000 |
| 30 (1) | Failure to ensure proper certification of document, or accepting certified document contrary to the section | $100,000 | $80,000 |
| 31 (2) and (5) | Failure to record an introduction of an applicant for business or a customer, or to ensure that an introducer reviews and maintains customer due diligence information as required | $70,000 | $65,000 |
| 31A (4) | Failure to amend or revise a written agreement within the prescribed period to comply with a condition stipulated in section 31A | $100,000 | $60,000 |
| 31B (1) | Failure to test a business relationship with a third party | $75,000 | $70,000 |
| 31B (5) | Failure to prepare a report of testing of business relationship with a third party or to provide copy of report to the Commission | $70,000 | $65,000 |

| | | | |
|---|---|---|---|
| 32 | Failure to take post verification steps required under the section | $65,000 | $60,000 |
| 36 | Failure by a correspondent bank to satisfy itself regarding necessary customer due diligence measures required to be undertaken by a respondent bank | $100,000 | $100,000 |
| 39 (1) and (3) | Failure to ensure transfer of funds accompanied by full originator information and full beneficiary information, or to verify full originator information | $80,000 | $75,000 |
| 39 (6) | Failure to keep records of full originator information on payer and full beneficiary information on the payee | $100,000 | $80,000 |
| 41 (2) and (5) | Failure to keep information received on payer with the transfer of funds, or to provide upon request within the specified time information on payer that the intermediary payment service provider has received | $80,000 | $75,000 |
| 41 (6) | Failure to keep records of information on payer and the payee for the specified period | $100,000 | $80,000 |
| 42 (2) | Failure to maintain records in the required form | $60,000 | $60,000 |
| 44 | Failure to maintain transaction records | $100,000 | $80,000 |
| 46 (2) | Entering into an outsourcing agreement for the retention of records whereby access to such records is impeded by | $100,000 | $80,000 |

| | | | |
|---|---|---|---|
| | confidentiality or data protection restrictions, or the outsourcing prevents or impedes the implementation of the Anti-money Laundering Regulations Revised Edition 2020, this Code or other enactment relating to money laundering, terrorist financing or proliferation financing | | |
| 47 (1) | Failure to train employees | $80,000 | $75,000 |
| 48 (1) and (2) | Failure to provide training at appropriate frequencies or to the desired level and standard | $80,000 | $75,000 |
| 55 (1) and (2) | Failure to make or submit a report in the proper form | $60,000 | $60,000 |
| Miscellaneous | The breach of or non-compliance with any provision for which a penalty is not specifically provided. | $60,000 | $60,000” |

Issued by the Financial Services Commission this 26th day of August, 2022.

(Sgd.) Kenneth Baker
Managing Director/CEO
Financial Services Commission