VIRGIN ISLANDS

ANTI-MONEY LAUNDERING AND TERRORIST FINANCING (AMENDMENT) (NO. 2) CODE OF PRACTICE, 2018

ARRANGEMENT OF SECTIONS

Section

VIRGIN ISLANDS

STATUTORY INSTRUMENT 2018 NO. 36

Proceeds of Criminal Conduct Act, 1997
(No. 5 of 1997)
Financial Services Commission Act, 2001
(No. 12 of 2001)

Anti-Money Laundering and Terrorist Financing (Amendment) (No. 2) Code of Practice, 2018

[Gazetted 19th July, 2018]

The Financial Services Commission, pursuant to the powers conferred by section 27 (1) of the Proceeds of Criminal Conduct Act, 1997 (No. 5 of 1997) and in exercise of the powers granted by section 41A of the Financial Services Commission Act, 2001 (No. 12 of 2001) 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, 2008.

Citation and commencement

1. (1) This Code may be cited as the Anti-Money Laundering and Terrorist Financing (Amendment) (No. 2) Code of Practice, 2018.

(2) This Code shall come into force on the 1st day of August, 2018.

Section 23 amended

2. Section 23 of the Anti-Money Laundering and Terrorist Financing Code of Practice, 2008 (hereinafter referred to as the "Code of Practice") is amended by inserting after subsection (6), the following subsections –

"(6A) For purposes of verification of identity under this Code, an entity or a professional may use such electronic or digital means as it considers appropriate to carry out the verification.

(6B) Where, for the purposes of subsection (6A), an entity or a professional relies on the electronic or digital or other data of an organisation to carry out verification, it shall ensure that the organisation –

(a) is independently established and operates independently;

(b) uses a range of positive information sources that can be called upon to link an applicant or a customer to both current and historical data;

(c) accesses negative information sources such as databases relating to fraud and deceased persons;

(d) accesses a wide range of alert data sources;

(e) has transparent processes that enable an entity or a professional to know what checks have been carried out, what the results of those checks were and to be able to determine the level of satisfaction provided by the checks;

(f) has not been convicted of a criminal offence or sanctioned for breach of data or providing misleading data; and

(g) is independent of the person to whom the verification relates.

(6C) In addition to the requirements outlined in subsection (6B), the entity or professional must be satisfied that the information obtained and stored by the organisation is sufficiently extensive, accurate and reliable.

(6D) In the case of electronic or digital verification of identity in relation to a non-face to face transaction, an entity or a professional need not treat an applicant for business or a customer as high risk unless it or he or she is satisfied that the applicant or customer presents a high risk or is otherwise engaged in money laundering or terrorist financing.".

[Explanation:

The Explanation to section 23 of the Code of Practice is amended as follows:

(a) After the reference to "Explanation", the following sub-heading should be inserted: "*General Verification*";

(b) Paragraphs *(iii), (iv), (v)* and *(vi)* are deleted and the following paragraphs substituted:

"*Specific Verification*

(iii) This Code makes provision for verification of the identities of individuals and legal persons who are applicants for business or customers of an entity or a professional. Section 24 specifically deals with verification requirements pertaining to an individual applicant for business or customer. The verification requirements relating to a legal person are dealt with in section 25 which also outlines information that is required with respect to a company and a partnership. Section 27 outlines the obligation for verification of underlying principals of legal persons, while section 28 deals with verification with respect to trusts. The obligation outlined in respect of each section must be complied with.

Methods of Verification

(iv) The methods by which verification may be carried out will generally vary, depending on the type, nature, size and complexity of business concerned, including origin of the applicant or customer. The purpose of verification is primarily to establish identity of individuals and legal persons and legal arrangements and other related matters outlined in the sections. It is designed to confirm that persons are who they claim to be and documents presented in that and other regards support whatever claim is made.

(v) Accordingly, verification of information received or required by an entity or professional may be carried out in physical paper form or by electronic/digital means. This may include the use of propriety software and/or programme by an entity or a professional to conduct electronic/digital verification. The reference to "electronic/digital means" (including variations of the term) in this Code should be given a broad interpretation to include verification by digital, electrical, magnetic, optical, electromagnetic, biometric and photonic form. The requirement for verification refers to the process of checking reliable, independent source documentation, data or information to confirm the veracity of any identifying information that an entity or a professional obtains during the process of identification. Accordingly, wherever in this Code verification of identity is required, such verification may be carried out by electronic/digital means in accordance with the Explanation in this section.

(vi) It is not sufficient for an entity or a professional to rely on an applicant's or customer's claim as to who he or she is; further verification procedures must be put in motion to truly establish the actual existence of the applicant or the customer. In that regard, reliance on verification may be placed on reliable independent source documentary or other tangible or acceptable evidence. Effort must be made to test the reliability of the source of evidence. That means a check should be made of the reliability, integrity, independence and authority of the source of the evidence and of the evidence itself, bearing in mind that documentary evidence may be susceptible to forgery.

(vii) As part of the verification process, additional measures may be adopted to check against fraud and other criminal behaviour, such as those routinely undertaken by entities and professionals in their business relationships. These measures may include:

- *requiring the first payment to be carried out through an account in the applicant's or customer's name with a regulated banking or financing institution in the Virgin Islands or based in a recognised jurisdiction listed in Schedule 2 of this Code, or with an assessed low risk jurisdiction;*

- *verifying such additional aspects of the applicant's or customer's identity as is required under this Code and as the entity or professional may consider necessary;*

- *telephone contact with the applicant or customer, prior to opening an account, on a home or business number which has been verified electronically, digitally or otherwise, or a "welcome call" to the applicant or customer before a business transaction is permitted, using it to verify additional aspects of personal identity information that have been previously provided during the establishment of the business relationship or setting up of the account;*

- *communicating with the applicant or customer at an address that has been verified (which may take the form of a direct mailing of account opening documentation to him or her which, in full or in part, is required to be returned completed or acknowledged without alteration);*

- *internet sign-on following verification procedures where the applicant or customer uses security codes, tokens and/or other passwords which have been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address;*

- *other card or account activation procedures; and*

- *requiring copy documents to be certified by an appropriate person, bearing in mind the provisions of section 30 of this Code and the Explanation thereto.*

(viii) In circumstances where verification relates to a person, other than an individual, the identity of the person may be verified electronically/digitally by relying on documentation that is directly sourced from an officially established institution (such as a registry or other body designated or established under law or recognised by a government) with which the person is incorporated or registered and/or an organisation that the person is a member of or has other affiliation with. In that context, it is important that an entity or a professional seeks to verify the identity of the individual or individuals connected with the person being verified by electronic/digital means or by reference to

documents that are independently sourced. The entity or professional must be able to demonstrate that it has both verified that the person exists and the individual seeking to establish the business relationship on behalf of that person is in fact that individual.

(ix) An entity or a professional may conduct an electronic/digital verification of a person by relying on the electronic/digital and other data of an organisation, but only if the conditions outlined in section 23 (6B) and (6C) are satisfied. Where such reliance is made, it is important that the entity or professional records its satisfaction of the conditions being met by the organisation. This may be carried out on a one-off basis and need not be carried out on each occasion that reliance is placed on the same organisation. However, the entity or professional must engage in an ongoing monitoring process to keep track of any changes in the stipulated conditions and to act accordingly. The ongoing monitoring may be measured on a cyclical basis whereby the entity satisfies itself of compliance or non-compliance with the stipulated conditions at least once every three years. The record maintained by the entity or professional will serve as evidence of compliance in the event of an inspection or other regulatory requirements.

(x) It is acceptable for an entity or a professional to rely on and accept from a person that is the subject of verification an offer to access electronic/digital data or source with which the person is affiliated if the data or source is reliable and independent of the person in terms of its collection, administration and management and is in the custody of an organisation that meets the criteria set out in paragraph (ix) above. However, the entity or professional must weigh any potential or perceived drawbacks that may taint the independence and integrity of the data or source and determine whether it should accept such an offer. The entity or professional only needs to ensure that the appropriate checks on reliability, independence and accuracy of the data or source have been satisfied whilst complying with the conditions stipulated in section 23 (6B) and (6C).

(xi) Determining the reliability and independence of electronic/digital data or source may not always be a straightforward matter. To assist an entity or a professional to make the proper judgment calls, it is important that account is taken of the following matters (although additional factors may apply which should, in such a situation, be taken into account as well):

- *accuracy of the information provided;*
- *security of the electronic/digital data or source;*
- *method used in collecting, storing and maintaining the information;*
- *level of privacy attached to the electronic/digital data or source;*

- *whether the electronic/digital data or source is reviewed and updated regularly;*

- *whether the electronic/digital data or source has incorporated a mechanism to determine that the person who is the subject of verification can be linked to the claimed identity;*

- *whether the information is maintained by a government, statutory body or pursuant to a specific enactment; and*

- *whether the information has been additionally verified from another reliable and independent source.*

(xii) Reliance on electronic/digital verification, as in physical paper verification, may disclose both positive and negative information concerning an applicant or a customer. Positive information will generally confirm the existence of a person (individual or legal) by providing confirmation of name, current address and date of birth. Negative information may relate to some wrong-doing (such as criminal conviction, ongoing criminal investigation, identity fraud, sanctions breach, etc.) connected to an applicant or customer. These are all important markers in the electronic/digital verification process and their discovery may assist in mitigating the possibility or potential for impersonation fraud and other types of criminal activity relative to money laundering and/or terrorist financing. It is therefore important that where reliance is placed on electronic/digital data of an organisation that the organisation has available to it the ability to be immediately notified and/or become aware of any changes in the source data that may impact the original assessment of the applicant for business or customer.

(xiii) Where an entity or a professional uses the medium of electronic/digital verification to verify the identity of an applicant or a customer, the entity or professional assumes (as with physical verification of information) full responsibility if there is failure to make any significant discovery in relation to the applicant or customer which could otherwise have been discovered with care and diligence at the time the verification was undertaken or when the applicant's or customer's information was being updated. It is therefore important that an entity or a professional sets out in writing the steps it has taken in engaging the electronic/digital verification process as regards an applicant or a customer. Consideration might be given to including in the entity's or professional's identification and verification procedures (required under the AMLR) the forms of electronic/digital identity verification methods used or relied upon during a verification process.

(xiv) Where reliance is placed on electronic/digital verification, it is important that an entity or a professional seeks (as with the physical verification of information)

confirmation of the matter being verified from a multiplicity of sources as is considered necessary. This may also be satisfied by relying on a single source that has relied on a multiplicity of other sources to acquire and retain its identity verification data. In circumstances where supplemental information is required for verification purposes, reliance may be placed on social media sources, but caution must be exercised as regards the reliability of such sources, especially in cases where information contained in such sources can be accessed and altered. It is therefore prudent that an entity or a professional should adopt qualitative checks which enable a proper assessment of the strength of the information sourced and received.

(xv) An entity or a professional may not rely on an electronic/digital record in certain circumstances. These will include situations where the relevant information contained in the record is not capable of being displayed in a legible form, the electronic/digital record appears to be damaged, altered or incomplete, or an electronic/digital signature or other kind of authentication accompanying or included with the electronic/digital record appears to be altered or incomplete. There may be other circumstances discernible on the face of an electronic/digital record which may require a proper assessment before reliance is placed on the record; it is for each entity or professional engaging electronic/digital means of identity verification to carefully consider and make an appropriate judgment call on.

(xvi) It may not be in every situation that a non-face to face business relationship or transaction presents a high risk thereby requiring treating an applicant or a customer as high risk. The extent of verification in such a situation will depend on the nature and characteristics of the product or service requested and the assessed money laundering or terrorist financing risk presented by the applicant or customer. There may be instances where the applicant or customer is not physically present which, in itself, would not necessarily increase the risk that may attach to the transaction or activity. This will be the case, for example, in many wholesale markets or instances of purchase of some types of collective investments. It is important, therefore, that an entity or a professional should take account of such instances in developing their AML/CFT systems (internal risk assessment procedures).

(xvii) An entity or a professional may adopt or deploy additional measures which may include assessing the possibility that an applicant or a customer may be deliberately avoiding face-to-face contact. It is, therefore, important that the entity or professional is clear on and adopts the appropriate approach in such circumstances, ensuring full compliance with its or his or her risk assessment mechanisms in evaluating the risk presented by the applicant or customer.

<u>Documentation for Identity Verification</u>

(xviii) As already noted above, 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 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's or customer's full name and photograph and either his or her residential address or his or her date of birth;*

  - *a government, court or local authority-issued document (without a photograph) which incorporates the applicant's 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.*

(xix) For purposes of the first bullet point under paragraph (xviii) 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 identity card;*

- *a national insurance card; and*

- *a valid student identity card.*

(xx) For purposes of the second bullet point under paragraph (xviii) above, a government-issued document 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.*

(xxi) 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 regulated by the Commission or another financial institution in a recognised jurisdiction listed in Schedule 2 of this Code. Where current bank statements or credit/debit card statements are issued by a regulated institution in a non-listed jurisdiction, the entity or professional should have regard to the ML/TF risks posed by that jurisdiction in determining whether the statements are acceptable. 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).

(xxii) It should be noted that some applicants 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 class 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.

(xxiii) Notwithstanding what is provided in the above paragraphs, an entity or a professional may, where it or he or she assesses an applicant 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.]"

Explanation to section 26 amended

3. The reference in Explanation *(ii)* to section 26 of the Code of Practice to "*paragraph (v) of the Explanation to section 23*" is amended to read "*paragraphs (viii), (ix) and (xi) of the Explanation to section 23*".

Section 29 amended

4. Section 29 of the Code of Practice is amended –

(a) in subsection (2) by deleting the words "Where an entity of a professional" and substituting the words "Subject to this section, where an entity or a professional";

(b) in subsection (3) by inserting after "section 19 (7)", the words "but subject to subsections (5) and (6)";

(c) in subsection (4) by deleting the words "identity is verified electronically or";

(d) by adding after subsection (4), the following subsections –

"(5) Subject to subsection (6) and having regard to appropriate risk assessment, where identity is verified by electronic or digital means in relation to a non-face to face application for business or one-off transaction, additional verification checks are not required where the entity or professional is satisfied of the authenticity of the documentation being relied on.

(6) The entity or professional shall, for the purpose of electronic or digital verification of identity, use such multiple electronic or digital sources as the entity or professional considers appropriate and necessary.".

[Explanation:

The Explanation to section 29 of the Code of Practice is amended by deleting the last paragraph after the last bullet point to paragraph (v) and substituting the following:

"(vi) In establishing a business relationship through reliance on copies of documents, additional verification checks are not required to verify the identity of an applicant for business or customer where the entity or professional assesses that applicant or customer as presenting a low risk, pursuant to section 19 (7) of this Code. This would normally be the case, for instance, in relation to applicants for business or customers that are known to the entity or professional or that emanate from recognised jurisdictions listed in Schedule 2 of this Code. Where the applicant for business or customer emanates from a non-listed jurisdiction, the entity or professional must have regard to the ML/TF risks posed by that jurisdiction in determining whether additional verification checks are required. It should be noted that dispensing with the requirement for additional verification does not mean dispensing with the basic CDD requirements of identification and verification, which continue to apply where an applicant for business or a customer (or a business relationship) is assessed as low risk.

(vii) An entity or a professional may carry out non-face to face verification of an applicant or customer by electronic or digital means. In this case, an applicant or customer should only be treated as presenting a high risk where the entity or professional, as part of its risk assessment, considers that the applicant or customer indeed presents a high risk. In addition, enhanced customer due diligence verification measures are not required where –

- *an entity or a professional relies on the electronic/digital data of an organisation which complies with the requirements and guidelines for electronic/digital verification outlined in section 23 of this Code; or*
- *is satisfied with the authenticity of verification documents; and*
- *has no concern regarding an applicant for business or a customer.*

However, where the applicant for business or customer is considered to present a high risk, the entity or professional must engage the enhanced customer due diligence requirements outlined in this Code.

(viii) Account should also be taken of the requirements for utilising multiple sources for verification by electronic/ digital means as outlined in paragraph (xiv) of the Explanation to section 23.]"

Section 30 amended

5. Section 30 of the Code of Practice is deleted and substituted by the following –

"(1) Where an entity or a professional, in the establishment of a business relationship or conduct of a one-off transaction with an applicant for business or a customer, relies on a copy of a document presented by the applicant or customer which the entity or professional, having regard to appropriate risk assessment, considers may not be authentic or may be doubtful or generally has concern with, the entity or professional shall ensure that the copy of the document is properly certified.

(2) For the purposes of subsection (1), a copy of a document is properly certified if the certification is made by a person who is competent and has authority to certify the document and bears –

(a) the name and address of the person certifying the document;

(b) the date of the certification; and

(c) the signature or seal of the person certifying the document.

[Explanation:

The Explanation to section 30 of the Code of Practice is deleted and substituted by the following –

"[Explanation:

(i) Every entity and professional has a legal obligation under the AMLR and this Code to risk assess its or his or her business relationships, including any transactions involving an applicant for business or a customer. In carrying out identification and verification requirements, reliance may be placed on copies of a document. These copies need not be certified in every case, particularly where the entity or professional does not have any doubt with regard to the source or authenticity of the information contained in the document. Certification must, however, be insisted upon where the entity or professional has some doubt regarding the authenticity or source of the document or any information contained in the document. Such certification will aid the verification process undertaken by the entity or professional. Any certification must include the information outlined in section 30 (2).

(ii) The onus is on the entity or professional to determine whether the person making a certification is competent and has the authority to provide reliable certification. A person that is acting in a professional capacity and is subject to some rules of professional conduct promulgated and enforced by the professional

body to which he or she belongs, is most likely to provide reliable certification. This is also the case for a person operating within a statutory system in his or her jurisdiction that provides for specific compliance measures and the application of penalties for breaches of those measures. Examples of persons that are competent and have the authority to certify reliable documents are as follows:

- *a judicial officer or a senior public officer, including a senior police officer, customs officer or immigration officer with responsibility within his or her organisation for issuing certified documents (for example, a registrar responsible for deeds, land matters, etc.);*
- *an officer of an embassy, consulate or high commission of the country of issue of documentary evidence of identity;*
- *a legal practitioner or medical practitioner, or an accountant, actuary or other professional who belongs to a recognised professional body with established rules of professional conduct;*
- *a notary public who is governed by established rules of professional conduct or statutory compliance measures;*
- *a director, manager or senior officer of a licensed entity, or of a branch or subsidiary of a group headquartered in a recognised jurisdiction under Schedule 2 of this Code or other well-regulated jurisdiction that applies group standards to subsidiaries and branches worldwide and tests the application of and compliance with such standards.]"*

Explanation to section 31 amended

6. The last sentence in brackets in Explanation *(iv)* to section 31 of the Code of Practice is amended by adding after the words "*section 19 of the Code*", the words "*and the Explanation to section 23*".

Issued by the Financial Services Commission this 12th day of July, 2018.

[Sgd]: Robert Mathavious
Managing Director/CEO