REFERENCE GUIDE TO THE AMENDMENTS OF THE PRIOR AML/CFT GUIDELINES

Reference	Section	Rationale
N/A	Interpretation	An amendment was made to include the FATF definition for "beneficial owner" for compliance with the requirements of recommendation 10 of the FATF Recommendations.
3.2	Financing of Terrorism	The below was added to the section for consistency with fellow regulators: The FATF Recommendations places obligations on countries as it relates to terrorist financing in the context of national cooperation and coordination (Recommendation 2), confiscation and provisional measures (Recommendation 4), and targeted financial sanctions related to terrorism and terrorist financing (Recommendation 6). The latter is applicable to all United Nations Security Council resolutions (UNSCRs) applying targeted financial sanctions relating to the financing of terrorism. The Bank's role is to safeguard against access to financing by individuals and entities who may be involved in or supporting terrorism.
3.3	Financing of Proliferation of Weapons of Mass Destruction	Consideration was given to recommendations 7 and 11 of the FATF Recommendations. An amendment was made to include the FATF definition for proliferation financing. This section was also enhanced to include the Commission's role.
3.4	International Initiatives	The section was added to the section for consistency with fellow regulators: The **FATF Forty Recommendations** were revised in February 2012, and renamed the **International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations**. The Recommendations were since updated in February 2013 R.37 & R.40 (mutual legal assistance and other forms of international cooperation); October 2015 (Interpretative Note to R.5 on foreign terrorist fighters); June 2016 (R.8 and its Interpretative Note on non-profit organizations); October 2016 (Interpretative Note to R.5 on terrorist financing offence); June 2017 (Interpretive Note to R.7 on targeted financial sanctions related to proliferation); November 2017 (R.21 on tipping-off and

		confidentiality and Interpretive Note to R.18 on internal controls and foreign branches and subsidiaries); February 2018 (R.2 on national cooperation and coordination); and October 2018 (R.15 on new technologies). The FATF normally issues Guidance and Best Practices Papers to assist countries in implementing the Recommendations. The growing body of work includes Guidance on **AML/CFT-related Data & Statistics**; **Combating the Abuse of Non-Profit Organizations**; **Transparency and Beneficial Ownership**; Politically Exposed Persons; Risk Based Approach to Prepaid Card, Mobile Payments and Internet-Based Payment Services; Risk-Based Approach to Combating Money Laundering and Terrorist Financing; Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction; and Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Financial institutions should keep abreast of developments in the international standard and refine their programmes accordingly.
4.0	Legislative Framework	This section was enhanced to include relevant legislation and the following paragraphs updated for consistency with fellow regulators: The MLFTA indicates that a financial institution engages in money laundering if it fails to take reasonable steps to implement or apply procedures to control or combat money laundering, and it confers responsibility for the supervision of financial institutions[1] to the Authority, which was established in August 2000. A Financial Intelligence Unit (FIU) has been established as the office of the Authority. As the office of the Authority and as a member of the Egmont Group of FIUs, the FIU's responsibilities include: i. Receiving suspicious or unusual transactions reports from Financial Institutions (FIs) and Designated Non-Financial Business Entities and Professionals (DNFBPs); ii. Analysing suspicious or unusual transactions reports; iii. Instructing FIs and DNFBPs to take steps that would facilitate an investigation; and iv. Providing training to FIs and DNFBPs in respect of record keeping obligations and reporting obligations under the MLFTA.

[1] Offences and penalties under the MLFTA .

		Where a financial institution is uncertain about how to treat an unusual or suspicious transaction, it is strongly urged to speak directly to the FIU for preliminary guidance and then make a report as appropriate. Where the FIU suspects on reasonable grounds that a transaction involves the proceeds of crime, the FIU will send a report for further investigation to the Commissioner of Police.
5.0	The Role of the Board and Senior Management	The section was updated at the paragraphs highlighted below. Financial institutions must see AML/CFT & PF as part of their overall risk management strategy. Money laundering, terrorist financing and financing of proliferation expose a financial institution to transaction, compliance and reputation risk. For financial institutions convicted of money laundering or terrorist financing, there are considerable costs. Financial institutions therefore must establish an effective AML/CFT & PF programme that minimises these risks and potential costs. The Board of Directors has ultimate responsibility for the effectiveness of the financial institution's AML/CFT & PF framework. Section 5(2)(b) of the MLFTA establishes that a financial institution engages in money laundering where the financial institution fails to take reasonable steps to implement or apply procedures to control or combat money laundering. Section 4 of the Anti-Terrorism (Amendment) Act, 2019 establishes the circumstances where a financial institution engages in terrorism financing. Directors and senior management must be aware that: i. The use of a group wide policy does not absolve directors of their responsibility to ensure that the policy is appropriate for the financial institution and compliant with Barbadian law, regulations and guidelines. Failure to ensure compliance by the financial institution with the requirements of the MLFTA may result in significant penalties for directors and the financial institution. This includes information and analysis of transactions and activities which appear unusual (if such analysis was done). Similarly, branches and subsidiaries should receive such information from these group level functions when relevant and appropriate for risk management; ii. Subsidiaries and branches of financial institutions including those domiciled outside of Barbados are expected to, at a minimum, comply with the requirements of Barbados MLFTA and this guideline; iii. Where some of a financial institution's operational

		functions are outsourced, the financial institution retains full responsibility for compliance with local laws, regulations and guidelines; and iv. AML/CFT programmes must include adequate safeguards on the confidentiality and use of information exchanged, including the prevention of tipping-off.
5.1	Risk-Based Approach	The section was updated at the paragraphs highlighted below. The FSC recognises the diversity of the institutions it regulates and it will seek to establish that, overall, processes appropriate to institutions are in place and operating effectively. Notwithstanding the risk rating framework highlighted above, all registered entities should therefore design an AML/CFT & PF framework that satisfies the needs of their institution, taking into account: i. The nature and scale of the business; ii. The complexity, volume and size of transactions; iii. The degree of risk associated with each area of operation; iv. Type of customer (e.g. whether ownership is highly complex, whether the customer is a PEP, whether the customer's employment income supports account activity, whether customer is known to other members of the financial group); v. Type of product/service (e.g. regular savings, one-off transaction, mortgage, annuity contract, brokerage account); vi. Delivery channels (e.g. whether internet business, wire transfers to third parties, remote cash withdrawals); vii. Geographical area (e.g. whether business is conducted in or through jurisdictions with high levels of drug trafficking or corruption, whether the customer is subject to regulatory or public disclosure requirements); viii. The ML/FT national risk assessment of Barbados; ix. The internal audit and regulatory findings; and x. Value of account and frequency of transactions.
6.0	Customer Due Diligence	The below was added to the section for consistency with fellow regulators: Where there is a suspicion that a transaction relates to money laundering or the financing of terrorism, financial institutions should be cognizant of tipping off a customer when conducting due diligence. The financial institution should make a business decision whether to open the account or execute the transaction as the case may be, but a suspicious

		report should be submitted to the Authority.
6.4	Enhanced Due Diligence	The below was added to the section for consistency with fellow regulators: Financial institutions should observe the Public Statements issued by the FATF and CFATF as it relates to business relationships and transactions with natural and legal persons, and financial institutions from listed countries. Financial institutions are also required to observe the list of countries published by any competent authority which lists countries that are non-compliant or do not sufficiently comply with FATF recommendations. In order to mitigate the risks, financial institutions should apply appropriate countermeasures to any country that appears on the list or when called upon to do so by FATF and CFATF. Such countermeasures may include: 1. Requiring financial institutions to apply specific elements of enhanced due diligence; 2. Prohibiting financial institutions from establishing subsidiaries, branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant subsidiary, branch or representative office would be in a country that does not have adequate AML/CFT & PF systems; 3. Limiting business relationships or financial transactions with the identified country or persons in that country; 4. Prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the CDD process; 5. Requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned; and 6. Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.
6.4.7	Corporate Vehicles	The section was updated at the paragraphs highlighted below for consistency with fellow regulators. Barbados law prohibits companies from issuing shares in bearer form. Where a financial institution decides that companies with nominee shareholders represent an acceptable business risk, they must exercise care in conducting transactions. Financial institutions must ensure they can identify the beneficial owners of such companies and must immobilise bearer shares and bearer share warrants

		as a means of monitoring the identity of such companies by, for example, requiring custody by:… *A bearer share warrant was defined in a footnote as a document issued by a company certifying that the bearer is entitled to a certain amount of fully paid stock shares.*
6.4.8	Virtual Asset Service Provider (VASP)	The section was added due to revisions to the FATF Recommendations and for consistency with fellow regulators: The FATF defines: "Virtual asset" as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations; and "VASP" as any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: a) Exchange between virtual assets and fiat currencies; b) Exchange between one or more forms of virtual assets; c) Transfer of virtual assets; d) Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and e) Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset. When establishing and maintaining relationships with VASP, a financial institution should: a) Adequately assess account risk and monitor the relationship for suspicious or unusual activity; b) Understand the intended use of the account, including the anticipated transaction volume, products and services used, and geographic locations involved in the relationship; and c) Obtain the identity of the beneficial owners of the client funds where it is not satisfied that the intermediary has in place due diligence procedures equivalent to the standard of this Guideline.
6.8	Reduced Customer Due Diligence	The section was amended to remove reference to the International Financial Services Act and circumstances which may warrant reduced due diligence measures, for consistency with fellow regulators.

7.0	Unusual & Suspicious Tractions	The section was updated at the paragraph highlighted below for consistency with fellow regulators. Suspicious transactions are business transactions that give rise to reasonable grounds to suspect that they are related to the commission of a money laundering or terrorism offence.
7.2	External Reporting	The section was updated at the paragraphs highlighted below for consistency with fellow regulators. Financial institutions are required by law to report promptly to the FIU where the identity of the person or entity involved, the transaction or any other circumstance concerning that transaction lead the financial institution to have reasonable grounds to suspect that a transaction: i) Involves proceeds of crime to which the MLFTA applies; ii) Involves terrorist financing; iii) Involves the financing of proliferation; iv) Is of a suspicious or an unusual nature; or v) Is conducted by, or relates to, a person or entity against whom a terrorist designation order is in force or relates to the property of such a person or entity. Where a suspicious report has been filed with the FIU, and further unusual or suspicious activity pertaining to the same customer or account arises, financial institutions must file additional reports with the FIU.
7.3	Freezing and Unfreezing	The section was updated at the paragraphs highlighted below for consistency with fellow regulators. In addition, pursuant to the United Nations Resolutions on terrorist financing and the financing of proliferation, financial institutions must freeze any funds or other assets held for individuals or entities so designated by a terrorist designation order or counter-proliferation order in respect of listed persons. Orders will be communicated electronically or in the Official Gazette and local newspapers. Financial institutions are required to submit a report to the identified Competent Authority which should include the total sum of frozen assets. The obligation to freeze is extended to all funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, of designated persons or entities, as well as funds or assets of persons and entities on behalf of, or at the direction of, designated persons or entities. Where a terrorist designation order or counter-proliferation

		order has been lifted. Financial Institutions should have a mechanism in place to release the assets previously frozen. See the detailed Guidelines on TF and PF Financial Sanctions obligations. A footnote was included which advises that this Refer to Omnibus Guidelines on Terrorist Fin. Sanctions for FIs to be issued by the AMLA in conjunction with Supervisors. Reports must be in the format determined by the FIU (**See www.fsc.gov.bb**). However, where a matter is considered urgent, an initial report may be made by contacting the FIU by telephone or e-mail.
9.1	Internal and External Records	The section was updated at the paragraph highlighted below for consistency with fellow regulators. In accordance with section 18.2 of the MLFTA, financial institutions must maintain records related to unusual and suspicious transaction reports. These must include: i. All reports made by staff to the Compliance Officer; ii. The internal written findings of transactions investigated. This applies irrespective of whether a suspicious report was made; iii. Consideration of those reports and of any action taken; iv. Reports by the Compliance officer to senior management and board of directors. v. Reports to the Authority on positive screening results in relation to terrorist financing and the financing of proliferation; and vi. Reports to the Authority on the total amount of frozen assets in relation to terrorist financing and the financing of proliferation.
12.1	Insurance	Consideration was given to recommendation 10 and 12 of the FATF Recommendation and Immediate Outcome 4. This section was enhanced to include the requirement for the beneficiaries of life insurance policies to be vetted to identify whether the ultimate beneficiaries are Politically Exposed Persons; as detailed below: Life insurers/ long term insurers are required to conduct CDD on beneficiaries of life insurance policies before the payout of the policy. Life insurers/ long term insurers are also required to vet the beneficiaries of life insurance policies to identify whether they are higher risked, including PEPS, and whether EDD measures are applicable. Where high risks have been identified, financial institutions must inform the senior management before the payout of the policy and conduct EDD on the whole business relationship.

		Additionally, where appropriate, financial institutions shall consider filing a Suspicious Activity or Transaction Report. Thereafter all additional due diligence measures would apply including those set out at paragraph 6.4.6 entitled Politically Exposed Persons."
N/A	Appendices	Appendices 1 thru 9 were removed; as well as references to the Appendices in the Guidelines. The Commission noted that the information therein may be updated on a regular basis to reflect legislative amendments and/or revision to the FATF Recommendations and Immediate Outcomes. On this basis, this information would be best placed in guidance notes and/or information circulars. Where necessary, forms previously housed in the AML.CFT Guidelines will be made available on the Commission's website.
N/A	Financing of Proliferation	General reference to the financing of proliferation was otherwise included in the Guidelines as necessary.