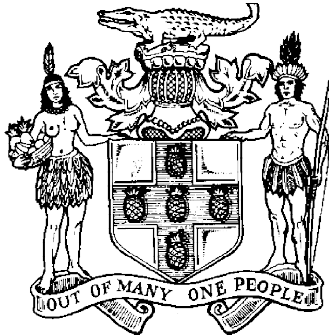




THE

JAMAICA GAZETTE

EXTRAORDINARY

911

Vol. CXLIX

WEDNESDAY, JUNE 17, 2026

No. 277

The following Notification is, by command of His Excellency the Governor-General, published for general information.

DWAYNE HILL, JP (MAJOR)
Governor-General's Secretary and
Clerk to the Privy Council.

GOVERNMENT NOTICE

MISCELLANEOUS

No. 383

BANK OF JAMAICA



(2026)

GUIDANCE NOTES ON THE PREVENTION OF MONEY LAUNDERING AND COUNTERING THE
FINANCING OF TERRORISM, PROLIFERATION AND MANAGING RELATED RISKS — 2026

This publication of the Guidance Notes is available on the Bank of Jamaica's website <http://www.boj.org.jm/>.

Initial Reissue August 2004

1st Update February 2005

2nd Update March 2005

3rd Update June 2005

4th Update March 2007

5th Update March 2009

(Revised June 2005, February, March and June 2007, and March 2009)

(Revised 2025 and 2026)

Second Reissue April 2017

Gazette Publication June 2018

Bank of Jamaica 2026. All rights reserved.

NO REPRODUCTION OR TRANSLATION OF THIS PUBLICATION MAY BE MADE

WITHOUT THE PRIOR WRITTEN PERMISSION OF THE BANK OF JAMAICA.

APPLICATIONS FOR SUCH PERMISSION, FOR ALL OR PART OF THIS

PUBLICATION SHOULD BE MADE TO:

THE BANK OF JAMAICA

NETHERSOLE PLACE,

KINGSTON, JAMAICA

(TELEPHONE 876-922-0750-9; FAX 876-922-2519 OR EMAIL FISDFEEDBACK@BOJ.ORG.JM)

TABLE OF CONTENTS

	Pages
Glossary	913 - 914
FOREWORD	915
SECTION I — PRELIMINARY PROVISIONS APPLICABILITY AND LEGAL STATUS OF THESE GUIDANCE NOTES	915
OBJECTIVE	916
APPLICABILITY OF THESE GUIDANCE NOTES	916
LEGAL STATUS OF THESE GUIDANCE NOTES	917
SECTION IA — BACKGROUND	918
MONEY LAUNDERING.....	918
TERRORIST FINANCING.....	919
FINANCING THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION	920
MUTUAL LEGAL ASSISTANCE	920
SECTION II — AML/CFT/CPF LEGISLATIVE AND REGULATORY FRAMEWORK — Competent Authority, Applicable and Other Relevant Legislation	921
COMPETENT AUTHORITY	921
APPLICABLE LEGISLATION	921
THE PROCEEDS OF CRIME ACT (POCA)	921
STATUTORY AML OBLIGATIONS UNDER THE POCA AND POC(MLP) REGULATIONS	931
THE POC (MLP) REGLUTATIONS, 2007	933
TERRORISM PREVENTION ACT, 2005 (“TPA”)	937
AREAS OF ENFORCEMENT UNDER THE TPA	939
TERRORISM PREVENTION (REPORTING ENTITIES) REGULATIONS, 2010 AMENDED IN 2013 AND 2019	942
FINANCIAL INVESTIGATIONS DIVISION ACT, 2010	943
CRIMINAL JUSTICE (SUPPRESSION OF CRIMINAL ORGANIZATIONS) ACT, 2014	944
DANGEROUS DRUGS ACT, 1948 (LAST AMENDED 2021)	944
THE FIREARMS (PROHIBITION, RESTRICTION AND REGULATION) ACT, 2022	944
LAW REFORM (FRAUDULENT TRANSACTIONS) (SPECIAL PROVISIONS) ACT, 2013	944
CYBER CRIMES ACT, 2015	945
OTHER OFFENCES (RELATING TO FRAUD, DISHONESTY, AND CORRUPTION	945
THE PREVENTION OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION	946
UNITED NATIONS SECURITY COUNCIL RESOLUTION IMPLEMENTATION ACT.....	947
AREAS OF ENFORCEMENT UNDER UNSEC IMPLEMENTATION ACT, 2013. FURTHER AMENDED IN 2019, UNSCRIDPRK — SANCTIONS REGIME) REGULATIONS, 2021 AND UNSCRI (REPORTING ENTITIES) REGULATIONS, 2019	950
SECTION III — REGULATORY REQUIREMENTS	952
INTERNATIONAL REGULATORY REQUIREMENTS	952
DOMESTIC REGUATORY REQUIREMENTS	957
SECTION IV — RISK-BASED FRAMEWORK	958
SECTION V — “KNOW YOUR CUSTOMER” (KYC), “KNOW THE TRANSACTION COUNTERPARTY” AND “CUSTOMER DUE DILIGENCE” (CDD)	963
INTERPRETATION	963
GENERAL REQUIREMENTS FOR KNOW YOUR CUSTOMER (“KYC”) AND “CUSTOMER DUE DILIGENCE” (“CDD”)	965

POLICIES AND PROCEDURES FOR KYC AND CDD	966
BANKS, MERCHANT BANKS, BUILDING SOCIETIES, CREDIT UNIONS, MICROCREDIT INSTITUTIONS, CAMBIOS AND REMITTANCE COMPANIES	968
GENERAL REQUIREMENTS FOR KNOW YOUR CUSTOMER (“KYC”) AND CUSTOMER DUE DILIGENCE (“CDD”)	968
UPDATING KYC AND CDD RECORDS	971
NATURAL PERSONS	972
CUSTOMER IDENTIFICATION FOR NATURAL PERSONS (WHETHER RESIDENT IN THE JURISDICTION OR NOT)	974
SELF-EMPLOYED PERSONS AND SOLE PROPRIETORS	975
TRANSACTION COUNTER-PARTIES	980
VERIFICATION OF CDD, KYC & TRANSACTION DETAILS	980
FINANCIAL INCLUSION	983
SIMPLIFIED AND ENHANCED DUE DILIGENCE — IDENTIFICATION AND KYC REQUIREMENTS	983
INTRODUCED BUSINESS	987
TRUST ACCOUNTS	988
ACCOUNTS OPENED BY PROFESSIONAL INTERMEDIARIES	988
PRIVATE BANKING/PRIVATE WEALTH MANAGEMENT/WEALTHMANAGEMENT/ HIGH-NET-WORTH CLIENTS	989
TRANSFERRING CLIENTS	989
POLITICALLY EXPOSED PERSONS (PEPS)	989
NON FACE-TO-FACE CUSTOMERS/REMOTE ON-BOARDING	991
EMERGING TECHNOLOGY	991
CORRESPONDENT BANKING	995
SHELL BANKS	998
COUNTRIES WITH INADEQUATE AML/CFT/CPF FRAMEWORKS	998
TRANSACTIONS UNDERTAKEN FOR OCCASIONAL CUSTOMERS.....	1000
CUSTODY ARRANGEMENTS	1000
ELECTRONIC FUNDS TRANSFERS (WIRE TRANSFERS, MONEY TRANSFERS etc.) ACTIVITIES	1000
ANONYMOUS ACCOUNTS/ACCOUNTS IN FICTITIOUS NAMES/NUMBERED ACCOUNTS	1002
Specific ADDITIONAL Guidance for Cambios, (Exchange Bureaux) and Money Transfer and Remittance Agents and Agencies (Remittance Service Providers (RSPs)/Remittance Companies)	1002
KYC GUIDANCE	1003
SECTION V(A)—SPECIAL GUIDANCE REGARDING TREATMENT OF LISTED ENTITIES	1007
SECTION V(B)—SPECIAL GUIDANCE - UNSEC RESOLUTIONS ON THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION	1008
SECTION V(C)—ADDITIONAL GUIDANCE - FINANCIAL HOLDING COMPANIES	1009
SECTION V(D)—ADDITIONAL GUIDANCE - BRANCHES AND SUBSIDIARIES	1009
SECTION V(E)—ADDITIONAL GUIDANCE-AGENT BANKS	1010
SECTION VI—THE NOMINATED OFFICER REGIME	1010
REPORTING OBLIGATIONS AND THE APPOINTMENT OF NOMINATED EMPLOYEES/OFFICERS	1010
SECTION VII—COMPLIANCE MONITORING	1012
INTERNAL COMPLIANCE PROGRAMME	1012
SECTION VIII—BOARD RESPONSIBILITY AND EMPLOYEE INTEGRITY AND AWARENESS	1014
BOARD RESPONSIBILITY	1014
EMPLOYEE INTEGRITY AND AWARENESS	1015

EDUCATION AND TRAINING	1016
SECTION IX — TRANSACTION MONITORING AND REPORTING	1018
REQUIRED DISCLOSURES-RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS AND FINDINGS IN RELATION TO UNUSUAL TRANSACTIONS	1018
SECTION X	1023
RECORD KEEPING	1023
SECTION XI — CONCLUSION	1024
SECTION XII — APPENDICES	1024
APPENDIX I —	1024
CRITERIA FOR DESIGNATION AS A ‘PERMITTED PERSON’ UNDER SECTION 101A OF THE POCA	1024
APPENDIX II — ADVISORY ISSUED BY BOJ IN MAY 2014	1025
APPENDIX III — DESIGNATION ORDERS (PARAGRAPH 96)	1026
APPENDIX IV — BASIC DUTIES AND RESPONSIBILITIES OF THE NOMINATED OFFICER	1046
APPENDIX V	1047
EXAMPLES OF UNUSUAL /SUSPICIOUS ACTIVITIES	1047
APPENDIX VI	1048
MANDATORY OBLIGATIONS	1048
APPENDIX VII	1049
BANK OF JAMAICA’S SPECIFIED TERRITORIES SUPERVISORY AUTHORITY NOTICE	1049
APPENDIX VIII	1051
i. BOJ’S INTERNAL PROCEDURE FOR LISTING ENTITY DESIGNATIONS UNDER SECTION 14 OF THE TPA	1051
ii. UNSCR SANCTIONS LIST AS AT JUNE 2025	1052
APPENDIX IX	1056
ADVISORY TO LICENSEES ON THE MANAGEMENT OF CYBER-RISKS	1056
APPENDIX X	1056
FORMAL ORDER UNDER SECTION 3A OF UNSCRIA RE: IRAN	1056

Glossary			
AML	—	Anti-Money Laundering	
ARA	—	Asset Recovery Agency	
BOJ/the <i>Bank</i>	—	Bank of Jamaica	
BOJA	—	Bank of Jamaica Act ¹	
BSA	—	Banking Services Act	
CDD	—	Customer Due Diligence	
CFATF	—	Caribbean Financial Action Task Force	
CFT	—	Counter Financing of Terrorism	
CPF	—	Counter Proliferation Financing of Weapons of Mass Destruction (also used for Combatting the financing of proliferation of weapons of mass destruction)	
CT	—	Counter Terrorism	
CTD	—	Chief Technical Director (Financial Investigations Division) ²	
DNFBP	—	Designated Non-Financial Businesses & Professions	
DNFI	—	Designated Non-Financial Institution	
DPP	—	Director of Public Prosecutions	
DPRK	—	Democratic People’s Republic of Korea	
DTI	—	Deposit Taking Institutions	
EFT	—	Electronic Funds Transfers	
ERSP	—	Electronic Retail Service Provider	
FI	—	Financial Institution	
FIA	—	Financial Intelligence Agency	
FID	—	Financial Investigations Division	
FIU	—	Financial Intelligence Unit	
FRSR	—	Fundamental Rules and Supplemental Rules	
FSC	—	Financial Services Commission	
FSRB	—	FATF Style Regional Bodies	
FT	—	Financing of Terrorism	
IOSCO	—	International Organization of Securities Commissions	
JMD	—	Jamaican Dollars	
KYC	—	Know Your Customer	
MFAFT	—	Ministry of Foreign Affairs and Foreign Trade	
MCA	—	Microcredit Act	
MCI	—	Microcredit Institution	
ML	—	Money Laundering	
MOFP	—	Ministry of Finance and the Public Service	
NIRA	—	National Identification Registration Authority	
NPO	—	Non-profit Organisation	
NPPS	—	New Payments Products and Services	
NRA	—	National Risk Assessment	
OFAC	—	Office of Foreign Assets Control	
POCA	—	Proceeds of Crime Act	
POC (MLP) Regulations	—	Proceeds of Crime (Money Laundering Prevention) Regulations ³	

¹ And all of its amendments.

² Pursuant to the Civil Service Establishment (General) Order, 2023, the post of Chief Technical Director of the Financial Investigations Division has been retitled as Director General with effect from April 1, 2023.

³ And all of its amendments.

PF	—	Proliferation Financing
STR	—	Suspicious Transaction Report
SOP	—	Standard Operating Procedures
TF	—	Terrorism Financing
TPA	—	Terrorism Prevention Act
TPR/TP (Rep. Ent.) Regs	—	Terrorism Prevention (Reporting Entities) Regulations ⁴
TTR	—	Threshold Transaction Report
UNSCRIA	—	United Nations Security Council Resolution Implementation Act ⁵
UNSCRI (DPRK Sanctions Regime) Regulations	—	United Nations Security Council Resolutions Implementation (Democratic People’s Republic of Korea Sanctions Regime) Regulations, 2021
UNSCRI (Rep. Ent.) Regs	—	United Nations Security Council Resolutions Implementation (Reporting Entities) Regulations, 2019
USD	—	United States Dollars
VASP	—	Virtual Asset Service Provider

⁴ And all of its amendments.

⁵ And all of its amendments.

FOREWORD

These Guidance Notes have been substantially revised to reflect the 2019 amendments to the AML/CFT/CPF Laws in Jamaica, amendments to the United Nations Security Council Resolutions Implementation Act and the Reporting Entities Regulations, 2019, updates to the FATF 40 Recommendations (issued 2012, last updated December 2025) and revised FATF Guidance on matters covered in the FATF Recommendations.

In examining, the 2019 updates to the AML/CFT/CPF legislation, these Guidance notes provide additional special guidance on the subject of Targeted Financial Sanctions, highlights obligations which will attract sanctions under the AML/CFT/CPF Rules that will be issued under the Banking Services and Bank of Jamaica Acts, provides general guidance on new technologies specific to virtual currencies and highlights additional sectors such as the Microcredit industry which have been brought under the AML/CFT/CPF framework.

The Guidance Notes seek to encourage financial institutions (as defined herein) to apply a risk based approach to their respective AML/CFT/CPF policies and procedures; outlines the regulatory expectations in relation to the matter of scenarios classified as high risk and low risk; expands discussions on financial inclusion, simplified and enhanced due diligence measures, KYC and CDD considerations; provides additional guidance on the matter of agent banking and responsibilities for group wide AML/CFT/CPF approaches, incorporates discussions on emerging issues such as the cash transaction limit requirements of the POCA and promotes a refocused approach to PEPS.

These Guidance notes support the application and interpretation of the law and serve as a guide for the minimum standards expected under the relevant laws. Therefore FIs should be guided by the law, the Guidance Notes and any other relevant directive or standards issued by the Bank as Supervisor/Regulator.

SECTION I — PRELIMINARY PROVISIONS

APPLICABILITY AND LEGAL STATUS OF THESE GUIDANCE NOTES

Preliminary Provisions—

1. Interpretation

“applicable legislation” means—

- The Bank of Jamaica Act
- The Banking Services Act;
- The Charities Act;
- The Financial Investigations Division Act;
- The Microcredit Act⁶;
- The National Identification Registration Act;
- The Proceeds of Crime Act (POCA);
- The Proceeds of Crime (Money Laundering Prevention) Regulations;
- The Revenue Administration Act;
- The Terrorism Prevention Act (TPA);
- The Terrorism Prevention (Reporting Entities) Regulations;
- The United Nations Security Council Resolution Implementation Act;
- The United Nations Security Council Resolutions Implementation (Democratic People’s Republic of Korea Sanctions Regime) Regulations, 2021⁷;
- The United Nations Security Council Resolutions Implementation (Reporting Entities) Regulations;
- The United Nations Security Council Resolution Implementation Regulations (enacted from time to time);
- The AML/CFT/CPF Rules (under the Banking Services Act and the Bank of Jamaica Act); and all applicable amendments to these legislation.

“competent authority” has the meaning assigned:—

In the Proceeds of Crime Act (‘POCA’), competent authority is defined at section 91(g) for anti-money laundering purposes in relation to its functions set out at section 91A⁸. In 2007, Bank of Jamaica was designated by the Minister of National Security, as the competent authority for the financial institutions it regulates;

⁶ The Micro Credit Act was passed in 2021 making BOJ the regulatory authority for licensing and monitoring microcredit institutions.
⁷ Please note that as of March 16, 2026, the United Nations Security Council Resolution Implementation (Asset Freeze — Democratic People’s Republic of Korea) Regulations as of March 16, 2026, have been revoked and replaced with the UNSCRI (DPRK — Sanctions Regime) Regulations.
⁸ See 2019 amendment which includes the continuous assessment of risk of money laundering and terrorist financing.

In the Terrorism Prevention Act (‘TPA’), competent authority for counter financing of terrorism is defined at section 18(5) of the TPA. Formal designation to the Bank of Jamaica of the role of competent authority was effected by way of letter dated 15th May, 2015 by the Minister of Finance and Planning;

In the United Nations Security Council Resolutions Implementation (Reporting Entities) Regulations, competent authority for proliferation financing is defined at regulation 2.⁹ Bank of Jamaica was formally designated as Competent Authority on 23rd of February, 2021 by the Minister of Foreign Affairs and Foreign Trade.

“designated authority” means the Chief Technical Director of the Financial Investigations Division for the purposes of the POCA, TPA and the United Nations Security Council Resolution Implementation Act 2013;

“designated non-financial institution” has the meaning set out in the Fourth Schedule of the POCA;

“enforcing authority” has the meaning set out in the POCA section 2;¹⁰

“financial institution” for the purposes of these Guidance Notes means a financial institution which falls under the AML/CFT/CPF jurisdiction of the Bank of Jamaica defined as follows—

- (a) a financial holding company (as defined in the Banking Services Act (‘BSA’);
- (b) a commercial bank;
- (c) a merchant bank;
- (d) a building society;
- (e) a co-operative society carrying on business as a ‘credit union’¹¹;
- (f) a person licensed under the Bank of Jamaica Act to operate an exchange bureau (i.e. a “cambio”);
- (g) a microcredit institution licensed under the Microcredit Act;
- (h) a money transfer and remittance agent and agency as defined in section 2 of the Bank of Jamaica Act¹²;
- (i) any other financial institution which falls under the supervisory jurisdiction of the Bank of Jamaica;

“financial service” has the meaning assigned in the BSA.

“regulatory authority” has the meaning assigned in the Microcredit Act.

OBJECTIVE

2. The objective of these Guidance Notes is to outline the minimum standards for;
- (i) the effective management of financial institutions’ ML/TF/PF risks,
 - (ii) expected behaviour with regard to FFs responsibilities under the applicable legislation, and
 - (iii) to outline the best practices in the areas of Anti-Money Laundering (‘AML’) and Counter-Financing of Terrorism (‘CFT’) and Counter Proliferation Financing (‘CPF’) techniques, to include a Risk-based Approach.

These Guidance Notes will be reviewed periodically and amended as deemed necessary, to ensure their continued usefulness, efficacy, relevance and adherence to international standards.

These Guidance Notes were initially circulated in this form in January and April 2004, replacing the previous versions issued in July 1995 and August 2000. The most recent version of these Guidance Notes was updated and published in 2018.

APPLICABILITY OF THESE GUIDANCE NOTES

3. These Guidance Notes shall apply to entities as defined by the POCA, TPA and UNSCRIA which are regulated by the Bank of Jamaica and fall within the remit of the Banking Services Act and the Bank of Jamaica Act. They are as follows:
- (i) a bank licensed under the BSA;
 - (ii) a merchant bank licensed under the BSA; (in) a building society licensed under the BSA;
 - (iii) a building society licensed under the BSA;
 - (iv) an FHC licensed under the BSA;
 - (v) a society registered under the Co-operative Societies Act and which undertakes credit union business;
 - (vi) persons who with the approval of the Minister, operate as an exchange bureau pursuant to BOJA;
 - (vii) approved money transfer and remittance agents and agencies as defined by section 2 of the BOJA;

⁹ The UNSCRIA and its regulations for Reporting Entities was last amended in 2019.
¹⁰ As amended by the Proceeds of Crime (Amendment) Act 2019, Section 2.
¹¹ Please note the Cooperative Societies Act and attendant Regulations which govern co-operative societies registered under that Act generally.
¹² On 15 January 2002 Money Transfer and Remittance Agents and Agencies were designated financial institutions for the purposes of the Money Laundering Act by Ministerial Order. Subsequently on 12 February 2004, the BOJ Act was amended to formally establish the regulatory regime for money transfer and remittance agents and agencies and the requisite Operational Directions for these persons was issued on 5 July 2005.

- (viii) a microcredit entity licensed under the MCA; and
- (ix) any other financial institution which falls under the supervisory jurisdiction of the Bank of Jamaica.

(i) Agent Banking Services

Persons who operate deposit taking institutions (DTIs) which have obtained the authorisation of BOJ to extend banking services through agents, are subject to the requirements in these Guidance Notes in relation to the agent banking services offered. Each deposit taking institution is charged with the responsibility to ensure that its agent has adequate AML/CFT/CPF controls, policies and procedures in place for the permissible offering of banking services through the agent’s operations.

Accordingly, to avoid losing the authorisation to offer banking services through agents, deposit taking institutions must ensure that their Agents’ operations through which the banking services are provided, are compliant with these Guidance Notes.

(ii) Retail Payment Service Providers

Persons who obtain authorisation to offer retail payment services as outlined or defined in the BOJ’s Regulatory Sandbox, 2020 (which replaced the “Electronic Retail Payment Services Guideline”), will be expected to inform themselves of the requirements in these Guidance Notes in so far as the services or products offered will involve or require interfacing, on any level, with or within, the operating space of a deposit taking institution (i.e. commercial bank, merchant bank or building society)¹³.

These Guidance Notes are informed by:—

- (a) The FATF Revised Forty (40) Recommendations, 2012 (last updated December 2025) (and related FATF generated Guidance and Best Practice Papers);
- (b) The Applicable Legislation (as defined in the interpretation section to these Guidance Notes); and
- (c) Other AML/CFT/CPF related international requirements, applicable to the financial institutions defined in these Guidance Notes.

LEGAL STATUS OF THESE GUIDANCE NOTES

- 4. These Guidance Notes have been re-issued pursuant to section 91(1)(g)(ii) of the POCA, Regulations 3 and 20 of the TP (Reporting Entities) Regulations and Regulation 3 of the UNSCRI (Reporting Entities), Regulations, 2019 and section 14A of the UNSCRIA.
- 4A. Further, sections 132(1) of the BSA, 34F (6) of the BOJA and 59(1)(c) of the MCA give the BOJ the authority to make supervisory rules in relation to combatting money laundering, terrorism financing and the proliferation of weapons of mass destruction¹⁴.
- 5. This authority is supported by the fact that the AML/CFT/CPF laws¹⁵ reflect that in determining whether a person committed an offence under the POCA, or its Regulations, or under the TPA or its Regulations or complied with any of the requirements contained in the UNSCRI (Rep, Ent.) Regs, **a court shall consider any relevant supervisory or regulatory guidance issued by the competent authority which has jurisdiction over an entity which is charged with an offence under the POCA or under the (MLP) or (TP) or (UNSCRI) regulations indicated.**

The Attorney General’s Chambers has opined that the import and effect of this wording, is that it makes compliance with these Guidance Notes compulsory. Section 18(4) of the TPA further requires entities to consult with the competent authority for the purpose of carrying out their obligations to establish regulatory controls to enable them to fulfil their counter-financing of terrorism duties.

Mandatory Obligations

The mandatory obligations under these Guidance Notes, are set out in the areas pertaining to the subject matters itemized below on¹⁶—

- (a) Risk-based Framework — Section IV;

¹³ The entities eligible to participate in the regulatory sandbox are regulated under existing regime as obtains with DTIs, remittance and cambios with the exemption of payment service providers (PSPs) for which a framework is being developed.

¹⁴ When finalized and promulgated, the supervisory rules will, among other things, codify the risk-based examinations and oversight processes pertaining to the AML/CFT/CPF oversight functions of the Bank of Jamaica that were established in 2014 and expressly mandate the compliance of licensees under the BSA, MCA and BOJA, with the certain measures outlined in the BOJ Guidance Notes. Accordingly, non-compliance with these aspects of the Guidance Notes will amount to a breach of the Rules and subject to regulatory directions and prosecution, if there is non-compliance with the directions. This approach extends the sanctioning options available to BOJ to address non-compliance and therefore also means BOJ would not need to demonstrate that non-compliance with these Guidance Notes is engaging in unsafe or unsound business practice, before such non-compliance can be punished.

¹⁵ Section 94(7) of POCA and Regulation 2(3) of the POC (MLP) Regulations; TP (Reporting Entities) Regulations, Regulation 3, UNSCRI (Reporting Entities) Regulations, Regulation 3.

¹⁶ Please note that these aspects of the Guidance Notes will be directly enforceable under the BOJ’s AML/CFT/CPF Ruies when the Rules take effect. Currently these aspects are enforceable under the general supervisory mechanisms of preventing unsafe and unsound business practices and there are aspects that are already subject to criminal penalties.

- (b) Know Your Customer Requirements — Section V;
 - (c) Customer Due Diligence — Section V;
 - (d) Special guidance — Listed Entities (Section V(B)& UNSEC Resolutions Section V(C);
 - (e) Nominated Officer Regime - Section VI;
 - (f) Compliance Monitoring - Section VII;
 - (g) Board Responsibility and Employee Integrity and Awareness — Section VIII;
 - (h) Transaction Monitoring and Reporting — Section IX;
 - (i) Record Keeping — Section X; and
 - (j) Special and Additional guidance — Listed Entities & UNSEC Resolutions.
6. Additionally, for a licensee under the BSA, a breach of its statutory obligations under the applicable legislation may be viewed as operating in a manner that constitutes unsafe or unsound practices for the purposes of paragraph 2 of Part A to the Fifth Schedule to the BSA, therefore, constituting a basis on which enforcement under the BSA is triggered in this regard. The ineffective or inadequate implementation of policies and procedures and controls (including any case of-inadequate policy(ies); inadequate assessment or analysis of risks; insufficient training sessions; inconsistent application of policies and procedures) is another example of a circumstance that could constitute unsafe or unsound practices.
7. If a licensee under the BSA is assessed to be operating in an unsafe or unsound manner, it can be subject to any one or more of the following penalties under section 109 of the BSA-
- Warning letter;
 - Voluntary Board Undertaking;
 - Supervisory directions; or
 - Cease and desist order

Failure to comply with any such requirement, undertaking, direction or order constitutes an offence for which a person on conviction in a Parish court can be fined up to \$5million and/or imprisoned for a term not exceeding one year.

In addition to these penalties, this does not exclude the licensee from being subject to the issuance of a fixed penalty notice (where applicable) and/or criminal sanction where the action warrants same.

- 7A. For a licensee under the Microcredit Act, non-compliance with their respective AML/CFT/CPF obligations *including these **Guidance Notes*** may result in the imposition of regulatory sanctions, such as, warnings, directions suspension or revocation of the licence pursuant to sections 25, 26 and 27. Further the licensee may be subject to the issuance of a fixed penalty notice (where applicable) and/or criminal sanction where the action warrants same.
- 8 In the case of Money Transfer and Remittance Agents and Agencies (“remittance companies”) and Bureaux de Change (“cambios”), non-compliance with their respective AML/CFT/CPF obligations, *including these **Guidance Notes***, may result in the imposition of regulatory sanctions, such as, being placed on probation and subject to enhanced monitoring or oversight, or the suspension or revocation of the licence.
9. A conviction for an offence under any of the applicable legislation can also adversely impact a person’s ability to be deemed as ‘fit and proper’ and to continue to operate within the sectors regulated by the BOJ.
10. Similar powers to take regulatory action for AML/CFT/CPF breaches will be applicable to credit unions when they become subject to regulation by the Bank of Jamaica. Additionally, credit unions must be aware that their level of compliance with the applicable legislation and these Guidance Notes will be amongst the matters considered in the review and assessment process for licence applications once the licensing regime has commenced. Currently where breaches of these Guidance Notes or the AML/CFT/CPF laws are identified in the operations of a credit union, both the credit union which is the subject of the breach, as well as the statutory regulator (i.e. The Registrar of Cooperative and Friendly Societies) are notified.

SECTION IA— BACKGROUND

MONEY LAUNDERING

11. The term ‘money laundering’ refers to all procedures, methods, and transactions designed to change the identity of illegally obtained proceeds of criminal activity so that it appears to have originated from a legitimate source.

It is recognized that cash lends anonymity to, and is therefore the normal medium of exchange for many forms of criminal activities, in particular, drug and arms trafficking, human trafficking, offences committed against persons (e.g. murder/ assassination/kidnapping), as well as all criminal activities involving fraud, dishonesty and corruption (e.g. tax evasion, extortion, infringement of copyrights or dealings with illicit recordings). The extent and impact of these criminal activities globally have required countries to make concerted efforts to defend their institutions, financial systems, economies

and citizens by criminalizing the proceeds of these crimes. Thus, in keeping with FATF Recommendation 3, POCA criminalizes any benefit derived directly or indirectly from any criminal conduct.

One of the most critical features of any AML regime is the protection of the financial system. Thus, apart from ensuring that financial institutions do not commit the offence of money-laundering, they are placed under further statutory obligations to ensure that they take active, effective and ongoing steps to detect and prevent money laundering¹⁷.

TERRORIST FINANCING

12. Terrorist financing refers to the act of accommodating or facilitating financial transactions that may be directly or indirectly related to terrorists, terrorist activities and/ or terrorist organizations. Once the financial institution knows or suspects or reasonably suspects that an individual or group is associated with any terrorist activity or group, a financial institution (in carrying out a transaction for or with that individual or group), may be considered to be facilitating terrorist activity whether or not the institution knows the specific nature of the activity facilitated, or whether any terrorist activity was actually carried out.

Terrorist financing offences extend to any person who wilfully provides or collects funds or other assets by any means, directly or indirectly, with the unlawful intention that they are used, or with the knowledge that they are to be used, in full or in part (a) to carry out a terrorist act(s); or (b) by a terrorist organisation or (c) by an individual terrorist (even in the absence of a link to a specific terrorist act or acts).

Additionally, these offences include financing the travel of individuals who travel to another jurisdiction for the purpose of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training. Offences also extend to any funds or other assets whether from a legitimate or illegitimate source.

It is not required for terrorist financing offences that the funds or other assets were actually used to carry out or used to attempt a terrorist act(s) or be linked to a specific terrorist act(s)¹⁸. Terrorist financing offences must be inferred from objective factual circumstances based on intent and knowledge required to prove the offence.¹⁹

A financial institution must also be aware, that business relationships with terrorists and terrorist organizations can expose it to significant legal, operational and reputational risks. These risks increase exponentially if the terrorist or terrorist related person or organization involved is later shown to have benefited from a lack of effective monitoring or wilful blindness on the part of the financial institution and is found to have carried out, supported or facilitated acts of terrorism. Accordingly, financial institutions are placed under further statutory obligations to ensure that they take active, effective and ongoing steps to detect and prevent terrorist financing²⁰. It may be difficult to detect funds linked to terrorist activities owing to the fact that terrorists or terrorist organizations often obtain financial support from legal sources. Other factors contributing to the difficulty of detection may also be the size and nature of transactions as these can be non-complex and in very small amounts.

Any financial institution that carries out transactions, knowing that the funds or property involved are owned or controlled by terrorists or terrorist organizations, or that the transaction is directly or indirectly linked to, or likely to be used in, terrorist activity, may be committing a criminal offence under the laws of many jurisdictions. Such an offence in many instances may exist regardless of whether the assets involved in the transaction were the proceeds of criminal activity or were derived from lawful activity but intended for use in support of terrorism.²¹ Additionally, some states have included in their legislation provisions intended to extend their local criminal jurisdiction beyond state borders. This is grounded on the premise that a person, who commits a terrorist offence in a jurisdiction other than his own jurisdiction, can in fact be prosecuted by the local jurisdiction for the commission of a terrorism offence, so long as such offence if committed in the local jurisdiction would have been a terrorism offence. The TPA also provides that for the purpose of conferring jurisdiction, any offence committed outside of Jamaica will be deemed to have been committed in Jamaica where the offender may be domiciled for the time being in Jamaica, if such offence, when committed in Jamaica, would have been a terrorism offence²².

13. A key issue for financial institutions therefore is to be able to identify any unusual and/or suspicious transaction that merits additional scrutiny and to record and report such transactions accordingly. In this regard, financial institutions must pay particular attention to:—
- (a) The nature of the transaction itself;

¹⁷ See Regulation 5 of POCA (MLP) Regulations.

¹⁸ The banking sector is an attractive means for terrorist organisations seeking to move funds globally because of the speed and ease at which they can move funds internationally. The low value of funds often used by terrorist financiers, and the sheer size and scope of financial flows gives terrorist organisations and their financiers the opportunity to blend in with normal financial activity.

Taken from FATF’s Terrorist Financing Risk Assessment Guidance, paragraph 55, page 37

¹⁹ Revision to FATF Recommendation 5 and update to the interpretive note to FATF Recommendation 5.

²¹ Section 18 (20) TPA.

²¹ FATF R 5 on Terrorism Financing was revised to include wilfully providing or collecting funds ‘or other assets by any means’ whether directly or indirectly with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); or (b) by a terrorist organisation or by an individual terrorist (even in the absence of a link to a specific terrorist act or acts.)

²² Section 46 TPA.

- (b) The parties involved in the transaction; and
- (c) The pattern of transactions or activities on an account over time.

See Appendix V, for examples of suspicious transactions which may be evidence of money laundering and/ or terrorist financing. Special attention must be given to elements of varying transactions which could indicate that the funds involved relate directly or indirectly to money laundering or terrorist financing. The list is not exhaustive and entities should be alert to evolving money laundering and/or terrorist financing techniques, patterns and typologies.

FINANCING THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

- 13A. Weapons of mass destruction (WMD) proliferation refers to the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes)

Proliferation financing refers to the act of raising, moving, or making available funds or financial services, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation to include their means of delivery or related materials (including both technologies and dual use goods for non-legitimate purposes).²³

This may be done within the framework of their existing targeted financial sanctions and/or compliance programmes. There is no requirement to duplicate processes for proliferation financing risk assessment or mitigation.

TARGETED FINANCIAL SANCTIONS (TFS) RELATED TO TERRORISM AND
TERRORIST FINANCING AND PROLIFERATION²⁴

- 13B. The FATF standards mandate countries to implement Targeted Financial Sanctions (TFS) related to terrorism and terrorist financing and proliferation financing in relation to designations made pursuant to United Nations Security Council Resolutions (UNSCRs)²⁵ and UN Sanctions regimes and to develop mechanisms for effective national cooperation and coordination to combat terrorism and the financing of terrorists²⁶ and the financing of proliferation of weapons of mass destruction²⁷.

While any deficiency in a country’s AML/CFT/CPF framework can pose a potential vulnerability, a weakness in the implementation of TFS, amongst other things, may be linked to TF vulnerabilities for financial institutions.

Recommendation 7 applies to both the Democratic People’s Republic of Korea (DPRK) and as of September 27, 2025 via the ‘snapback mechanism’ of United Security Council resolution 2231 has been reapplied to Iran²⁹ and requires countries to freeze without delay the funds or other assets of, and to ensure that no funds and other assets are made available, directly or indirectly to or for the benefit of (a) any person or entity designated by the United Nations (UN), (b) persons and entities acting on their behalf or at their direction, (c) those owned or controlled by them.

MUTUAL LEGAL ASSISTANCE

14. The United Nations Resolution 1373 and the revised FATF Recommendations (R.36-40) require that states must have the ability to provide mutual assistance to each other whether through the exchange of information, or facilitating the freezing and forfeiture of assets used to aid the commission of a crime or of a terrorist offence in another jurisdiction. In Jamaica the Mutual Assistance (Criminal Matters) Act of 1995, The Sharing of Forfeited Property Act of 1999, the Maritime (Drug Trafficking) Act, the Interception of Communications Act, and the Extradition Act, permit Jamaica to extend assistance to other countries that are in the process of investigating and/or prosecuting criminal matters, seeking to apprehend those charged or convicted of a crime or enforcing judgments or forfeiture proceedings, for a range of offences including drug related, revenue, money laundering and terrorist offences.

²³ Proliferation Financing Risk refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7.

²⁴ FATF Recommendations 6 and 7.

²⁵ Recommendation 6

²⁶ Recommendation 2.

²⁷ *ibid*.

²⁸ As included in the operative paragraphs (OPs) of relevant UNSCRs, it is the obligation of member states to impose targeted financial sanctions on designated persons and entities, as well as persons and entities acting on their behalf, at their direction, or owned or controlled by them.

²⁹ Pursuant to UNSCR 2231 (2015) the TFS measures in resolutions 1696(2006), 1737(2006), 1747(2007), 1803(2008), 1835(2008) and 1929(2010) have been reapplied in the same manner to Iran as they applied before the adoption of resolution 2231 (2015). See Appendix X with UN Order reinstating in Jamaica the obligations relative to proscribed persons and entities of Iran. FATF’s position is that the triggering of the snapback mechanism activates obligations that already exist under Recommendation 7 and does not result in any substantive changes to the FATF methodology, it only affects the natural and legal persons to whom TFS are applied (i.e. the names on sanctions lists.)

SECTION II — AML/CFT/CPF LEGISLATIVE AND REGULATORY FRAMEWORK — Competent Authority, Applicable and other Relevant Legislation

{The following summaries do not constitute a legal interpretation by the Bank of Jamaica of the sections of the Acts or Regulations referred to, accordingly independent legal advice must be sought thereon.}

COMPETENT AUTHORITY

15. The competent authority is the person designated under the POCA and TPA and UNSCRIA³⁰ as the authority with statutory responsibility to monitor compliance of FIs and DNFI with their respective statutory responsibilities under these statutes. Initially, the mandate of the competent authority was expressed as monitoring compliance with statutory obligations and issuing guidance to assist with compliance. This mandate has expanded over the years to reflect the ongoing assessments being taken in relation to the country’s risk profile as well as to strengthen the powers of the competent authority. There is also an express exclusion of disclosures to the competent authority from the tipping-off provisions in the POCA and to the disclosure prohibition pertaining to TTRs³¹.

The amendments effected to the POCA in 2013 strengthened the oversight powers of the competent authority. These 2013 amendments have been bolstered by amendments in 2019.

Section 91A outlines the additional functions of the competent authority which are:—

- (a) requiring the regulated business to comply with registration and reporting procedures (if any) developed by the competent authority and issued by written notice;
- (b) undertaking inspections or verification procedures (either directly or through a third party);
- (c) issuing directions to take certain measures to either prevent, detect or reduce the risk of money laundering or terrorism financing;
- (d) examining and making copies of information or documents in the possession or control of the regulated business and relating to the operations of that business;
- (e) sharing information pertaining to examinations conducted by the competent authority with the competent authority’s regulatory counterpart, a supervisory authority, or the designated authority either in Jamaica or in another jurisdiction. This ability to cooperate is—
 - (i) restricted to information which is not subject to protection from disclosures (such as matters that are covered by legal professional privilege); and
 - (ii) not meant to operate in contravention of the prohibitions regarding ‘tipping off’.
- (f) continually assess money laundering and terrorist financing risks relating to businesses in the regulated sector and tailor its activities (whether through directions or requirements or measures or procedures that may be issued/established)³².

Non-compliance with the directives/requirements of the competent authority is a criminal offence and subsections (5) (a) and (b) of section 91A provide for penalties, which are \$3,000,000.00 JMD on summary conviction in the Parish Court; or on conviction on indictment before a Circuit Court to a fine.³³ Further subsection 6 of section 91A states that a conviction under subsection 5 shall be deemed to constitute grounds on which administrative action may be taken by the competent authority, such as the suspension or revocation of an operating licence.

It should be noted that the pre-POCA position under the financial legislation, which pre existed the BSA, was that the BOJ³⁴), through the Supervisor of Banks, has leval access to all records of the banks, merchant banks and building societies including STR related information. POCA. has therefore synchronized the position under the AML laws with that under the financial legislation then and that status quo is maintained under the BSA. This now extends to FHCs under the BSA as well as microcredit institutions under the MCA.

APPLICABLE LEGISLATION

The Proceeds of Crime Act (POCA)

16. POCA came into effect on the 30th day of May, 2007 and repealed and replaced the Money Laundering Act (‘MLA’) and the Drug Offences (Forfeiture of Proceeds) Act (‘DOFPA’).

³⁰ Competent authority is defined in Regulation 2 of UNSCRIA ((Reporting Entities) Regulations, 2019 as the authority authorized to monitor compliance by any type of business in the regulated sector and issue guidelines regarding effective measures to prevent ML.
³¹ POC(A)A, 2019 Sections 97(2)(e), 100 and Regulation 3(4) of the POC (MLP) Regulations).
³² POCA amendment 2019 section 3 amending section 91A.
³³ The Circuit (Supreme) Court being one of unlimited jurisdiction, the fine to be imposed is subject to the discretion of the Court in accordance with precedence and other relevant sentencing principles to include the overarching consideration of fairness.
³⁴ BOJ is the designated competent authority for banks, merchant banks, building societies, credit unions, microcredit institutions, cambios and remittance service providers.

POCA represents an all crimes approach to dealing with money laundering and generally the proceeds of crime. Money laundering is any specified activity amounting to dealings with criminal property³⁵. Criminal property is any property that constitutes a benefit derived wholly or partially from criminal conduct. Criminal conduct³⁶ means any conduct constituting an offence in Jamaica, or if committed outside Jamaica, conduct that would constitute a crime in Jamaica if that act had been committed in Jamaica.

17. The POCA comprises seven parts as follows:—

- (a) Part I treats with the Assets Recovery Agency provisions. Assets Recovery Agency under section 3 means the Financial Investigation Division (‘FID’) of the Ministry of Finance and Public Service (‘MOFPS’) or any other entity so designated by the Minister by Order. (See sections 2 and 3).

The Director under POCA means the Chief Technical Director (‘CTD’) of the FID or where another entity is designated, the person in charge of the operations of that entity. (See section 3(2)).

- (b) Parts II, III and IV treat with enforcement and investigatory tools such as Forfeiture Orders, Pecuniary Penalty Orders and Restraint Orders, Disclosure Orders, Search and Seizure Warrants, Customer Information Warrants and Account Monitoring Orders and the criminal lifestyle regime. (See paragraph 20-21 below for more details).
- (c) Part V treats with the issue of money laundering, required disclosures, and offences under the POCA. Under POCA, money laundering is any act which—
 - (i) constitutes an offence under section 92 or 93; (See Section 91(l)(b)(i));
 - (ii) amounts to an attempt, conspiracy or incitement to commit an offence at section 92 or 93; (See Section 91(l)(b)(ii)); and
 - (iii) amounts to aiding, abetting, counselling, or procuring the commission of an offence under Section 92 or 93. (See Section 91(l)(b)(iii)).
- (d) Part VI treats with investigations and other offences under the POCA. The offences addressed under this aspect of the Act are in relation to investigations being conducted.
- (e) Part VII treats with matters general in nature such as regulation making powers under POCA, the fixed penalty regime, the repeal of the MLA and DOFPA and consequential amendments to other enactments.

SPECIFIC AREAS OF CONCERN UNDER POCA SECTION V (MONEY LAUNDERING) AND
UNDER SECTION VI (INVESTIGATIONS) TO FINANCIAL INSTITUTIONS

18. Offences under Section V (Money Laundering) are as follows:—

- (a) Section 92(1) of the POCA, creates an offence where a person:—
 - (i) engages in a transaction that involves criminal property; (section 92(l)(a)) or
 - (ii) conceals, disguises, disposes of, or brings into Jamaica, criminal property; (section 92(l)(b)) or
 - (iii) converts, transfers or removes criminal property from Jamaica, (section 92(l)(c)),

and that person knows or has reasonable grounds to believe at the time he does any act referred to at (a) (b) or (c), that the property is criminal property. (Section 92(1)).

Financial institutions should note that the successful prosecution of an offence under the AML regime does not only require proof of knowledge on the part of the person charged with the offence. It is sufficient if it can be proven that there was wilful blindness on the part of the person so charged. That is to say, it need only be proved that in the circumstances, there were reasonable grounds for the person charged to believe or know that the property being dealt with was in fact criminal property.

Under the POCA, criminal property is property that constitutes a person’s benefit (whether in whole, partially, directly or indirectly) from criminal conduct. It is immaterial who carried out or benefited from the conduct. (Section 91(l)(a))

- (b) Section 92(2) of the POCA creates an offence where a person enters into or becomes involved in an arrangement that the person knows or has reasonable grounds to believe facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another.

Financial institutions must pay particular attention to this category of offence since this offence can be committed whether or not a transaction (in the traditional sense of the term), takes place. For instance, an offer of any kind or type of service, such as custodian or asset safe keeping services (e.g. safety deposit boxes) provided for property that is later viewed as criminal property; or the issue of letters of credit on behalf of persons who proceed to use these arrangements to acquire property which is later deemed to be

³⁵ POCA section 91(1), 92 and 93.

³⁶ POCA section 2.

criminal property. Both of these examples pose a significant risk to financial institutions and increase their exposure to prosecution and liability under POCA. Other services in respect of which caution should be applied include cheque cashing, arrangements facilitating the movement of funds to accounts held (i.e. gift certificate arrangements); and changing out large bills to smaller bills or vice versa.

Financial institutions shall ensure that their mandates with customers and contractual arrangements entered into in the course of the regulated business permits the legal termination of the transaction, arrangement or business relationship if the institution conducting the transaction or facilitating the commercial arrangement forms the view that criminal activity is taking place and to continue with the arrangement, relationship or transaction would expose that institution to legal or reputational risks due to the suspected criminal activity.³⁷ In such cases the FI should be able to give reasonable notice to terminate the banking relationship and should report in the manner and form prescribed by POCA;

- (c) Section 93(1) of the POCA makes it an offence where a person acquires uses or has possession of criminal property and the person knows or has reasonable grounds to believe that the property is criminal property;
- (d) Section 94(2) makes it an offence for failing to make the requisite disclosure within the stipulated timeframe (i.e. within fifteen days after the information or matter comes to a person’s attention) (s. 94(2)(c)) in circumstances where there is knowledge or belief that another person has engaged in a transaction that could constitute or be related to money laundering (s. 94(2)(a)), and this knowledge or belief arose in the course of a business in the regulated sector (s. 94(2)(c)); (Suspicious Transaction Report (‘STR’) obligation);

Importantly section 94(4) requires that a business in the regulated sector shall in relation to each customer make and retain for a period of not less than seven years or such other period specified in writing by the supervisory authority a record of all complex, unusual or large business transactions carried out with the customer by the business and unusual patterns of transactions whether completed or not which appear to be inconsistent with the customer’s normal transactions or business.

- (e) Section 94(A) makes it an offence where a business in the regulated sector in respect of all its business relationships and transactions with customers domiciled, resident or a body corporate incorporated in a specified territory³⁸, fails to apply enhanced due diligence procedures, ensure that the background and purpose of all such relationships and transactions are examined and places those findings in writing³⁹ and limits those business relationships or one-off transactions, in accordance with enhanced money-laundering counter-measures set out in the regulations.
- (f) Section 95 makes it an offence where there is a failure of the nominated officer⁴⁰ to make the requisite disclosure within the stipulated timeframe (i.e. within fifteen (15) days after the information or matter comes to the nominated officer’s attention) in circumstances where there is knowledge or belief on the part of the nominated officer that another person has engaged in a transaction that could constitute or be related to money laundering, and this knowledge or belief arose in the course of a business in the regulated sector; (STR obligation);
- (g) Section 97 makes each of the following matters a ‘tipping off’ offence—
 - (i) disclosing information with the knowledge or having reasonable grounds to believe⁴¹ that a protected or authorized disclosure has been or is to be made under section 100; (s. 97(1)(a))

Disclosures in this regard refer to disclosures by regulated businesses (via nominated officer regime) and disclosures to an authorized officer; (refer to section 100(4)(a))
 - (ii) Disclosing information or any other matter with the knowledge or having reasonable ground to believe that the Agency, the DPP or an authorized officer⁴² is acting or proposing to act in connection with a money laundering investigation that is being, or is about to be conducted; (s. 97(1)(b))

³⁷ NCB v Olint Corp Ltd. — Privy Council Appeal No. 61 of 2008 [2009] UKPC 16. Per Lord Hoffman at paragraph 1 “Their Lordships have no doubt that in the absence of express contrary agreement or statutory impediment a contract by a bank to provide banking services to a customer is terminable upon reasonable notice: Paget’s Law of banking 13th Ed (2207) p. 153.

³⁸ This section was inserted pursuant to the POC (Amendment) Act. 2019. Specified territory means a territory specified in a list, published by notice in the Gazette, by a supervisory authority, as being a territory in respect of which there is a greater associated risk of money laundering or terrorist financing.

³⁹ Which are to be made available on request to the designated authority, supervisory authority or competent authority.
See section 94A (2)(c).

⁴⁰ See discussion below in Section VI on the Nominated Officer.

⁴¹ As amended in 2019.

⁴² As amended in 2019.

- (h)

Section 101 makes it an offence for failing to make a report where cash (which includes bearer-negotiable instruments⁴³) exceeding US\$10,000 or the equivalent amount in any other currency, is being taken into or out of Jamaica (s. 101(2)). The FID has introduced a standard reporting form which can be found on its website at www.fid.gov.jm.
- (i)

Section 101A makes it an offence for a person to pay or receive cash in excess of the prescribed amount⁴⁴ for the purchase of property or services or for the payment or reduction of any indebtedness, accounts payable or financial obligation or to artificially separate a single activity or course of activities to circumvent the prescribed amount but which in the aggregate exceeds the prescribed amount.

19. Offences under Section VI — Investigations are as follows:

- (a)

Disclosing information or any other matter with the knowledge or reasonable grounds to believe that an investigation (whether regarding forfeiture; money laundering or civil recovery) is about to be or is being conducted or falsifying, concealing or destroying or disposing or permitting either the falsification, concealment, destruction or disposition of documents that are relevant to the investigation (section 104(2) (a) and (b));
- (b)

Failure by the financial institution without reasonable excuse, to comply with a disclosure order (section 112);

It is also an offence under section 112(3) if in purported compliance with a disclosure order a statement is made or is recklessly made, that is false or misleading in a material particular.
- (c)

Failure by the financial institution without reasonable excuse, to comply with a customer information order (CII) (section 122(1));
- (d)

The financial institution in purported compliance with a CII making a statement that it knows to be false or misleading in a material particular (section 122(3)(a));
- (e)

The financial institution in purported compliance with a CII recklessly making a statement that is materially false or misleading (section 122(3)(b)).

20.

The responsibility for enforcing the provisions of the POCA is shared amongst the FID (in its capacity as the ARA and as designated authority through its CTD); the DPP; the Police; Jamaica Customs; the competent authority, and any other person designated by the Minister. The responsibility for monitoring compliance with the obligations of the POCA is placed with the competent authority, which for financial institutions as defined in these Guidance Notes is the BOJ.

AREAS OF ENFORCEMENT UNDER POCA & POC (MLP) REGULATIONS

Areas of Enforcement	Section of Act/Regs.	Responsible Authority	Additional Information
Threshold reporting	Reg. 3	CTD of the FID	
Required disclosure (SIR)	Sections 94 and 100	CTD of the FID	
Account Monitoring Orders ⁴⁵	Section 126	ARA + (Constable; Officer designated by the Commissioner; Customs Officer; or any other person designated by the Minister)	These persons are collectively referred to as the “Appropriate Officer”.
AML Guidance and implementation of AML measures and monitoring compliance with the AML laws and guidance.	Sections 91 and 91A	Competent Authority	BOJ for licensees under the BSA, MCA, credit unions, cambios and remittance companies;

⁴³ Section 101(1) POCA. In 2013 the penalty on conviction for an offence under section 101, was revised from J\$10,000 to J\$250,000 — refer section 12 of the POCA as amended in 2013.

⁴⁴ One million dollars or its equivalent in any currency or such other amount as the Minister may prescribe.

⁴⁵ Section 126 of the POCA refers to an account monitoring order as an order directing a financial institution to give such information and documents as the Appropriate Officer requires in his application for this order. The order requires a financial institution to produce documents and/or information obtained by or that are under the control of the financial institution about transactions conducted through accounts held by a particular person with the financial institution.

Areas of Enforcement	Section of Act/Regs.	Responsible Authority	Additional Information
			FSC for non-DTIs (i.e. Securities dealers, Insurance Companies; Pension Funds Managers; Collective Investment Schemes, Trust and Corporate Service Providers); The Public Accountancy Board for Accountants; General Legal Council for Attorneys ⁴⁶ ; The Real Estate Board for Real Estate Dealers; The Betting, Gaming and Lotteries Commission for the gaming sector; The Casino Commission for casinos.
Forfeiture & Pecuniary Penalty Orders	5-32	ARA The DPP	
Restraint Orders	33	ARA The DPP	
Seizure of realizable property ⁴⁷ that is subject to Restraint Order	36	A Constable; Customs Officer; An officer of the ARA/ Agency; Any other person designated by the Minister	These persons are collectively referred to as “Authorized Officers”
Recovery Orders pursuant to the Civil	57	ARA	
Forfeiture Regime		The DPP	
Disclosure Orders	105	Appropriate Officer	ARA + (Constable; Officer designated by the Commissioner; Customs Officer; any other person designated by the Minister)
Ancillary Orders	110	Appropriate Officer	
Search & Seizure Warrants	115	Appropriate Officer	
Customer Information Orders	119	Appropriate Officer	

⁴⁶ The AG v JAMBAR; The GLC v JAMBAR [2023] UKPC 6 has now decided that the AML obligations under POCA is applicable to Attorneys practising in Jamaica.

⁴⁷ “Realizable property” is any free property held by the defendant for the purposes of the criminal lifestyle and civil forfeiture regimes; or any free property held by the recipient of a tainted gift.

21. The tools used for enforcement and investigation are Forfeiture Orders, Pecuniary Penalty Orders, Restraint Orders, Disclosure Orders, Search and Seizure Warrants, Customer Information Orders, Account Monitoring Orders and the issuance of Fixed Penalties⁴⁸.

- (a) A forfeiture order is an order by the court, made upon the application of the Agency or the DPP where a person is convicted for any offence in proceedings before the court or committed to the Supreme Court, for any property used in or in connection with the offence concerned to be forfeited to the Crown. In making a forfeiture order the Court shall (amongst other things) determine:
 - (i) whether the person convicted of the offence has a criminal lifestyle⁴⁹ and that person has benefited from his general criminal conduct, or
 - (ii) if the Court determines that the defendant does not have a criminal lifestyle, determine whether or not he has benefited from his particular criminal conduct⁵⁰; AND
 - (iii) identify any property used in or in connection with the offence concerned and make a forfeiture order for the property identified. (Section 5)
- (b) A pecuniary penalty order is an order by the court, made upon the application of the Agency or the DPP where a person is convicted for any offence in proceedings before the court or committed to the Supreme Court, to pay to the Crown an amount equal to the value of the benefits derived by that person from his/her criminal conduct.⁵¹ An order of this nature would usually be made in circumstances where the property representing the benefit from criminal conduct cannot be made subject to an order for forfeiture. (Section 5(3)(b));
- (c) A restraint order is an order by the court made upon the application of the Agency or the DPP, prohibiting any person from dealing with any realizable property held by a specified person or transferred to the specified person after the order is made. (Sections 32 and 33) Realizable property as defined in section 2, means any free property held by the person who is the subject of the order; or held by the recipient of a tainted gift and includes any realizable property transferred to the specified person after the order is made. (Section 33 (3)(b)).
- (d) A search and seizure warrant is a warrant authorizing:
 - (i) The entry and search of premises specified in the warrant; and
 - (ii) The seizure and retention of any information or material found which is likely to be of substantial value, whether by itself or not, to the investigation in respect of which the search warrant has been issued. (Section 115(3)).

The Act states that this warrant does not confer the right to seize any information or material in respect of which production can be refused on the grounds of legal professional privilege in proceedings in the Supreme Court (section 117);

- (e) A disclosure order is an order by the court that requires the person on whom it is served to either produce or grant access to an appropriate officer, information or material or answer questions at once or at a place or time specified in the order (Section. 105(3)). The Act states that this order does not require production of or access to information that can be refused, that is, “excluded material”⁵² or information or material that can be refused on the grounds of legal professional privilege in proceedings in the Supreme Court⁵³ (See section 108);

⁴⁸ Section 138 of the POC Amendment Act, 2019

⁴⁹ Expounded on more below at paragraph 22.

⁵⁰ The principles enunciated at (i) and (ii) are also relevant for the Court’s consideration in making a pecuniary penalty order.

⁵¹ This has been coined as a ‘recoverable amount’ and is assessed in accordance with the relevant provisions of the POCA.

⁵² “Excluded material” per section 103 of POCA means:—

- (a) medical records;
- (b) human tissue or fluid which has been taken for the purpose of diagnosis or medical treatment and which a person holds in confidence.

⁵³ Legal professional privilege according to (Gilbert Law Summaries Dictionary of Legal Terms) is a person’s privilege to refuse to disclose and to prevent others from disclosing anything said in confidence to that person’s Attorney. Legal professional privilege very broadly applies to—

- (i) matters that come within the ordinary scope of professional employment of an attorney and which are received in the attorney’s professional capacity, either from a client or on the client’s account, and for the client’s benefit in the transaction of the client’s business; or
- (ii) communications from the client received by the attorney in the course of employment with the client and which relate to matters which the attorney becomes aware only through the professional relationship with the client. (See The Queen v. Cox and Railton — (1884) QBD 153 C.A.(see also Bowman v Fels [2005] EWCA 226/[2005] All ER (D) 115.

This principle was also reaffirmed in the Jamaican Court of Appeal decision JAMBAR V AG & GLC [2020] JMCA Civ 37.

For the purposes of Section V of the POCA, information comes to an Attorney in privileged circumstances where—

- (i) it is given by the client directly or indirectly in connection with his giving legal advice to the client;
- (ii) it is given directly or indirectly by a person seeking legal advice; or
- (iii) it is given by a person in connection with legal proceedings or contemplated legal proceedings. (s. 94(8)).

Provided that this does not apply to information or other matter that is communicated or given with the intention of furthering a criminal purpose.

- (f) A customer information order is an order by the court for information on whether a person holds/held (solely or jointly) any account with a financial institution or has during a specified period conducted any transaction with a financial institution, (Section 119). Note the particular information required in the case of individuals—
- (i) account/transaction number;
 - (ii) full name and date of birth;
 - (iii) TRN (see section V on KYC for further guidance);
 - (iv) most recent address and previous addresses;
 - (v) date on which the individual began to hold the account;
 - (vi) date on which the individual ceased to hold the account;
 - (vii) transaction date and description of transaction type;
 - (viii) identity obtained by the financial institution under or for the purposes of any ML enactments;
 - (ix) full name, date of birth, most recent and previous addresses of any current or previous joint holder(s) of the account;
 - (x) account number of any other accounts to which the individual is a signatory and details of the persons holding those accounts.

Note the Particular information required in the case of non-individuals—

- (i) account number;
 - (ii) entity’s full name;
 - (iii) description of the business carried on by the entity;
 - (iv) country or jurisdiction of incorporation or establishment;
 - (v) TRN (see section V on KYC for further guidance);
 - (vi) current and previous registered office or place of business (in or outside of Jamaica);
 - (vii) date on which the entity began to hold the account;
 - (viii) date on which the entity ceased to hold the account;
 - (ix) evidence of the entity’s identity obtained by the financial institution under or for the purposes of any ML enactments;
 - (x) full name, date of birth, most recent and previous addresses of any person who is a signatory to the account;
- (g) An Account Monitoring Order is an order by the court to a financial institution to provide the account information specified in the order to an appropriate officer in the manner which it is requested and for the period or by the time or times specified in the order. (Section 126(5)).

For these purposes, account information means information relating to an account held at, or a transaction conducted with, the financial institution specified in the order, by the person specified in the order, whether solely or jointly with another. (Section 126(4)). Under the POCA an accounting monitoring order has effect notwithstanding any restriction on the disclosure of information, however imposed. (Section 126(7)).

Criminal Lifestyle Principle

22. This concept of criminal lifestyle was introduced by the POCA. Once a person has been convicted of any offence before the Supreme Court or has been committed to the Supreme Court from the Parish Court⁵⁴ for a determination to be made in relation to an application for either a forfeiture order or pecuniary penalty order, the Court at that point is required to decide on the issue of criminal lifestyle⁵⁵.

- (a) Under the POCA a person shall be deemed as having a criminal lifestyle if—
- (i) the person is convicted of an offence specified in the Second Schedule;
 - (ii) the offence for which he is convicted or committed (by a Parish Court whilst in custody or on bail) constitutes conduct forming part of a course of criminal activity, from which the person obtains a benefit; or

⁵⁴ Formerly Resident Magistrates’ Court. Renamed by virtue of section 3 of the Judicature (Parish Courts) Act.
⁵⁵ Section 5(1) POCA. That is whether or not the person has been proven to have a criminal lifestyle or and benefited from his general/particular criminal conduct.

- (iii) the offence for which he is convicted or committed (by a Parish Court whilst in custody or on bail) was committed over a period of at least one month and the person has benefited from the conduct constituting the offence. (Section 6(1)).
- (b) A court’s assessment of the determination of the “criminal lifestyle” issue as stated above will look at—
 - (i) whether there is a criminal lifestyle and whether there has been some benefit from the general criminal conduct. If the determination is that there has been some benefit from criminal conduct, the court will then identify the property that represents that benefit, and either make an order for the property to be forfeited to the Crown; or make an order for the payment of an amount equal to the value of the benefit obtained; (section 5(3))
 - (ii) if the determination at (a) is in the negative then the determination will be as to whether there has been any benefit from the particular criminal conduct (for which the person was convicted); and
 - (iii) identification of any property used in or in connection with the offence concerned and make an order for same to be forfeited to the Crown;(section 5(2))

A person benefits from conduct if he obtains a benefit as a result of or in connection with the conduct. (Section 7(1)). Benefit is given a wide interpretation and speaks to:

- (i) benefit from conduct which constitutes the offence (section 6 (3) (a)(i)); or
- (ii) benefit from any other conduct which forms part of the course of criminal activity and constitutes the offence of which the defendant is convicted) (section 6 (3)(a)(ii) and b(i)); or
- (iii) benefit from conduct which constitutes an offence that has been or will be taken into consideration by the Court in sentencing the defendant (section 6 (3)(a)(iii) and b(ii)).

For the purpose of making a forfeiture order, a person’s benefit is the property obtained as a result of or in connection with the conduct. For a pecuniary penalty order a person’s benefit is the value of the benefit obtained as a result of or in connection with the conduct. (Section 7(4)(a) and (b)).

- (c) Statutory safeguards to the above powers of forfeiture include the following:
 - (i) In considering whether a forfeiture order should be made the Court must take into account—
 - third Party rights and interests in the property;
 - the gravity of the offence concerned;
 - any hardship that might reasonably be expected to be caused by the order;
 - the use that is ordinarily made of the property or the intended use of the property; (section 5(4))
 - (ii) Not less than fourteen days written notice of an application for a forfeiture or pecuniary penalty order must be given by the enforcing authority to the Defendant and any other person it is believed to have an interest in the property targeted for forfeiture. Additionally, a copy of the notice must be published in a daily newspaper printed and circulated in Jamaica; (section 5(11)).
 - (iii) Persons claiming an interest in the property targeted for forfeiture may apply to the court for an order (section 5(12)) declaring the nature, extent and value of their interest in the property. Before such an order is made the court must first be satisfied that the applicant was not in any way involved in the commission of the offence; that the person acquired his interest for sufficient consideration and without knowing or having reasonable grounds to suspect that at the time the property was acquired, it was tainted property; (section 5(13)).
- (d) The offences to which the criminal lifestyle regime applies can be found at the Second Schedule to the POCA (i.e. offences that include drug trafficking, money laundering, murder, kidnapping, arms trafficking, forgery, infringements of intellectual property rights, larceny, embezzlement, extortion, terrorism offences and inchoate offences (conspiracy, aiding, abetting, counselling etc.)).

CIVIL RECOVERY IN THE SUPREME COURT

- 23. POCA allows for civil recovery of property in the Supreme Court.
- 23A. Under sections 57-71 of the POCA, the Enforcing Authority (i.e. the ARA or the DPP) can apply to the Supreme Court to recover in civil proceedings recoverable property which is property believed to be obtained through unlawful conduct. Where the Court is satisfied that any property is recoverable the Court shall make a recovery order vesting the property in the Agency subject to certain conditions and exceptions (section 57).

For these purposes, property includes cash (including postal orders; bankers’ drafts, cheques of any kind, monetary instruments of any kind designated by the Minister), real property believed to be obtained directly or indirectly by or in return for or in connection with unlawful conduct (i.e. conduct that is unlawful under the criminal law of Jamaica);

Flowing from this power a Court may either make or refuse to make an order for provision out of recoverable property (i.e. property subject to a recovery order). Where all four of the conditions below are met a Court shall not make an order for provision unless it is just and equitable to do so. They are:

- (a) whether the respondent obtained the recoverable property in good faith;
- (b) whether steps were taken after obtaining the property that would not have been taken if the respondent had not obtained the property; or whether steps were taken before the property was obtained which steps would not have been taken if the respondent did not believe that he would obtain the property;
- (c) when the steps at (b) were taken the respondent had no notice that the property was recoverable; and
- (d) if a recovery order is made, then by virtue of the steps taken by the respondent at (b) the order would be detrimental to the respondent. (Section. 58(3) & (4), (5)).

Conversely, in deciding whether it is just and equitable to make such a provision the court must take into account—

- (a) the degree of detriment that would be suffered if the provision was made; and
- (b) the enforcing authority’s interest in receiving the realized proceeds of the recoverable property;

CIVIL FORFEITURE IN THE PARISH COURT

23B. POCA also allows for civil forfeiture in the Parish Court.

- (a) The authorized officer⁵⁶ who has reasonable grounds for suspecting that there exists in the scenarios outlined below, cash, which is obtained through unlawful conduct whether directly or indirectly or intended for use in unlawful conduct⁵⁷ AND not less than the statutory minimum⁵⁸ of J\$100,000, can take the following actions:
 - (i) search of premises where it is believed cash is kept (section 72(1));
 - (ii) search of a person or of any article in that person’s possession whom it is believed is carrying cash (section 72(3)); (a person may be detained for as long as is required for the exercise of these powers - section 72(4));
 - (iii) seizure of any cash (section 75) (initial detention period is 72 hours which period may be extended on application to a Parish court⁵⁹ (section 76);
 - (iv) apply to the court for the cash seized to be forfeited to the Crown (section 79).
- (b) Statutory safeguards to the above powers of civil forfeiture include—
 - (i) requirements that the Officer must be lawfully on the premises and must have reasonable grounds for suspecting that there is cash on the premises before a search under section 72 can be done; (see section 72(1)); and
 - (ii) the officer must act in accordance with a search warrant or the approval of a senior officer if action is taken in the absence of a warrant (section 73(1));
 - (iii) additionally, POCA mandates the Minister to establish a code of practice in connection with the exercise of powers conferred under section 72 which shall be taken into account as evidence in any relevant civil or criminal proceedings. (See section 74).

Amendments effected to the POCA since its passage in 2007

24. Since its passage in 2007 POCA has been amended to extend the list of predicate offences and offences in respect of which an assumption of criminal lifestyle can be made, to include offences under the Child Pornography (Prevention) Act, part II of the Cybercrimes Act; specified offences under the Sexual Offences Act; offences under the Law Reform (Fraudulent Transactions) (Special Provisions) Act which targets activities such as lottery scamming and related inchoate offences of aiding and abetting; incitement etc.

- (a) In October 2013 further amendments were passed in Parliament to the POCA to, among other things:
 - (i) clarify the suspicious transactions reporting requirements (section 94(4))⁶⁰;

⁵⁶ Any of the following individuals may be considered an authorized officer — a constable, customs officer or the Minister’s designate. (Section 55(1).
⁵⁷ Please see sections 84-86 of POCA.
⁵⁸ Section 55(1).
⁵⁹ The maximum period for detention is two years. A Justice of the Peace may exercise the power of the Parish Court to make an order first extending the period no longer than three months beginning with the date of the order.
⁶⁰ See 2019 Amendments discussed below which expanded on these requirements.

- (ii) outline the powers that competent authorities designated under the POCA have in relation to their role of monitoring compliance with the AML requirements under the POCA. Accordingly, competent authorities therefore, among other things, have the power to—
 - conduct examinations; request information and direct an entity to comply with the requirements of the Act or regulations. The competent authority has enforcement powers to ensure compliance with such directions; and
 - share information with regulatory counterparts and law enforcement agencies, both locally and internationally. (Section 91A);
 - (iii) Extend the obligations placed on a financial institution to an entity that has corporate responsibility for the development and implementation of group wide AML/CFT/CPF prevention, policies and procedures for the group of companies of which the financial institution forms a part. (One e.g. of such an entity would be a financial holding company as defined in the BSA); (Paragraph 1(1) of the Fourth Schedule to the POCA);⁶¹
 - (iv) Introduce a cash transaction limit of JMD One Million, beyond which it is illegal for transactions to be undertaken in cash unless such transactions are undertaken with permitted persons (such as banks). (Section 101A) (Refer also to paragraph 25 below);
 - (v) Refine the provisions applicable to law enforcement activity to, for e.g. allow for the disposal of seized assets which are in danger of depreciating in value before the substantive case is determined in the courts with provision being made for the safe custody of the proceeds of disposal to be available at the conclusion of the case to the Party adjudged by the court to be the Party entitled to those proceeds;
 - (vi) Effect several amendments to POC (MLP) Regulations discussed further at paragraph 29 below.
- (b) In October 2019 further amendments were made to the POCA Regulations discussed at paragraph 29 below. Following on these amendments, in November 2019 further amendments were made to the POCA which in relevant part are:
1. Imposing via statute a mandatory duty on the competent authority to continually assess the risks of money laundering and terrorist financing relating to businesses in the regulated sector and tailor its activities which includes directions etc accordingly. (Section 91A(f)).
 2. Requiring the application of enhanced due diligence procedures documented in writing in relation to all the business relationships and transactions with any customer resident or domiciled (in the case of a body corporate) in a specified territory. (Section 94A (1)).
 3. Granting the Minister power to prescribe programmes, policies etc to be implemented by businesses to extend to the enhanced monitoring procedures to be applied in respect of specified territories (Section 102).
 4. Requiring the supervisory/competent/designated authority to keep statistical records which will be utilized in measuring the overall effectiveness of AML and TF measures taken under POCA. (Section 137A).
 5. Introduction of the Fixed Penalty Regime for specified offences which allows the competent authority to impose administrative fines in conjunction with or instead of other enforcement measures to include criminal sanction. (Sections 138-139).

Cash Transaction Limits (Section 101A POCA)

25. POCA has a transaction limit in respect of transactions conducted in cash (i.e. notes and coins issued by BOJ or issued by the authority responsible for the issue of notes and coins in another jurisdiction⁶²).

- (a) Section 101A of POCA states that, a person shall not carry out a cash transaction in excess of JMD\$1,000,000.00 or its equivalent (at the date of the relevant transaction) in any other currency, unless such transaction is undertaken with a permitted person.⁶³

A ‘permitted person’ is defined as a licensed deposit taking institution regulated by Bank of Jamaica; a person licensed under the Bank of Jamaica Act to operate an exchange bureau; or any other person that may be designated by the Minister as a ‘permitted person’ by Ministerial Order.⁶⁴ A person or transaction can also be exempted from the cash transaction limit by Ministerial Order. Pursuant to section 101A(3) as amended, this is a two-stage test That is, after written consultation with the designated authority and competent authority which is the BOJ. The competent authority shall submit a written money laundering and terrorist financing risk assessment regarding the person or transaction concerned AND the Minister is satisfied that it is in the public interest to grant this exemption⁶⁵.

⁶¹ POCA section 2.
⁶² Section 101A(6) POCA.
⁶³ This section also prohibits artificially separating a single activity/transaction into more than one which aggregate exceeds the prescribed amount.
⁶⁴ Section 101A(6) POCA.
⁶⁵ As amended in 2019.

Meaning of ‘permitted person’ and exempted person or exempted transaction

- (i) The permitted person category includes commercial banks, merchant banks, building societies, cambios, credit unions, and persons so designated by virtue of an order from the Minister of National Security;
 - (ii) A person or transaction can be exempted from the cash transaction prohibition by virtue of an order made by the Minister of National Security as outlined above;
 - (iii) The order by which a designation as ‘permitted person’ is done or by which exempt status is conferred, is subject to Affirmative Resolution.⁶⁶ If therefore a person conducting business with a licensed deposit taking institution, attempts to conduct a transaction in excess of the statutory limit on the basis of having received a designation as ‘permitted person’ or exemption status, the licensed deposit taking institution shall ensure it has sight of and retain a copy of the gazette copy of that order of exemption prior to proceeding;
- (b) Permitted persons may carry out cash transactions in excess of the prescribed amount with any person. It should be noted that the prohibition does not apply to a payment made to, or by, a permitted person (Section 101A (2)⁶⁷).
- (c) Permitted persons must therefore not refuse to carry out a cash transaction solely on the basis that it exceeds the prescribed amount. However, in facilitating cash transactions, permitted persons remain obliged to be reasonably sure that they do not facilitate a financial crime or other breaches of the law. (An advisory to this effect was issued by the BOJ in May 2014 — refer to Appendix II).
- (i) Licensed deposit taking institutions and cambios therefore still need to be alert for circumstances in which cash transactions are conducted by persons connected with each other which each meet or is below the statutory transaction limit, but which collectively exceed such limit, as these could amount to a single transaction being conducted in a manner designed to avoid the cash transaction limit prohibition. It is important to note that the ability to accept cash above the prescribed limit does not obviate the obligation to conduct CDD.
 - (ii) ‘Connected’ for this purpose could mean — persons connected with each other by virtue of having the same residential or business address, familial bonds, same contact details or contact persons, or persons connected with each other by virtue of the existence of common principals, common shareholders; common trustees; or connected through the use of funds derived from the same source.
- (d) Once a cash payment is being made to a permitted person by a person other than a permitted person, or payment is being received by a permitted person from a person other than a permitted person, then the permitted person shall ensure that it employs the requisite checks (appropriate in the circumstances) to satisfy itself that its services are not being used to allow a non-permitted person to circumvent the prohibition on dealings/transactions exceeding the prescribed amount.

See Appendix I for the matters considered by the Ministry of National Security in reviewing an application for designation as a permitted person.

STATUTORY AML OBLIGATIONS UNDER THE POCA & POC (MLP) REGULATIONS

26. Other statutory AML obligations under the POCA regime can be found in Section V of the POCA and in the POC (MLP) Regulations and require the following:—
- (a) filing required disclosures where this is applicable in the circumstances and manner prescribed and related record keeping obligations (ss94-96 and 100);
 - (b) filing TTRs (s. 102 & reg. 3(1)) (refer also to paragraph 29 below);
 - (c) complying with the directions of the designated authority in relation to required disclosures and TTRs (reg. 3(6));
 - (d) complying with a requirement or direction issued by the competent authority (section 91 A(5));
 - (e) making the required cross border currency report in the manner indicated by the designated authority (s. 101)(2) (reporting threshold is USD 10,000); and
 - (f) complying with other AML/CFT/CPF operational and regulatory controls under the POC (MLP) Regulations, 2007 and its amendments. (Refer to Paragraph 29 below).

⁶⁶ The Interpretation Act defines ‘regulations’ as including, inter alia, orders and, further states that, unless otherwise indicated, regulations come into effect, on the date of publication in the gazette. (Refer to sections 3 and 31).

⁶⁷ As amended in 2013.

27. Suspicious Transaction Reports (STRs) (Sections 94 - 96 & 100 POCA)
- (a) Section 94 makes it an obligation for a person to make a required disclosure as described in the circumstances outlined below:
 - (i) there is knowledge or belief or reasonable grounds to know or believe that another person has engaged in a transaction that could constitute or be related to money laundering (Section 94(2)(a)); and
 - (ii) the information or matter on which the knowledge or belief is based or which gave reasonable grounds for such knowledge or belief, was obtained in the course of a business in the regulated sector (section 94(2)(b));
 - (b) The required disclosure is a disclosure to the nominated officer; or a disclosure to the designated authority in the form and manner prescribed by the POCA legislation⁶⁸ (Section 94(3))⁶⁹.
28. Where the conditions stipulated at paragraph 27 above exist giving rise to the need for a STR to be filed, financial institutions should further note that:
- (a) there is a maximum thirty (30) day period for institutions to file a report with the designated authority (i.e. maximum fifteen days from the date on which the suspicion is formed, meaning, for the person who forms the suspicion to report to the nominated officer and maximum fifteen days within receiving the report for the nominated officer to file the report with the designated authority);⁷⁰
 - (b) in guiding the determination of whether a required disclosure is to be made, a business in the regulated sector must in relation to each customer identify all—
 - (i) complex, unusual or large business transactions carried out with the business; and
 - (ii) unusual patterns of transactions, whether completed or not, which appear to be inconsistent with the normal transactions carried out by that customer with the business⁷¹;

These transaction records referred to at (a) and (b) must be retained for a period of not less than seven years. (Section 94(4)).

- 28A. Additionally, a business in the regulated sector must in relation to ALL of its business relationships and transactions with any customer resident or domiciled or in the case of a body corporate incorporated in a specified territory apply enhanced due diligence procedures, examine the background and purpose of all relationships and transactions and set out these findings in writing. These writings should be made available upon request to the designated/supervisory/competent authority. (Section 94A).
- 28B. For persons not included in the regulated sector, the POCA provides protection for disclosure of information.
- Section 100(1) to (3) addresses disclosure of information or any other matter obtained or discovered in the course of the reporting person’s trade, profession, business or employment, resulting in the knowledge or reasonable grounds for knowing or believing that another person has engaged in money laundering.
- Section 100(4) authorizes disclosure where information or any other matter is disclosed in circumstances where there are reasonable grounds for knowing or believing that property is criminal property and this disclosure is made either before the person does the prohibited act or the disclosure is made after the person does the prohibited act but there is a reasonable excuse for failing to make the report before and when the disclosure is made it was on the person disclosing own initiative and as soon as it was reasonably practicable for him to make it.
- This disclosure is protected or authorized where it is made to an authorized or nominated officer as soon as is reasonably practicable.
- 28C. For both financial institutions and designated non-financial institutions, required disclosures are to be made using Form 1⁷².

⁶⁸ See Form 1 in the Schedule, POC (MLP) Regulations, 2007.

⁶⁹ goAML, September 1, 2018.

⁷⁰ S94(3) and S95 as amended in 2013 provides for the maximum period allowed.

⁷¹ S 94(4)(b) as amended in 2019.

⁷² POC(MLP) Regulations, Regulation 17 — goAML filing solution is a web portal now used for filing required disclosures (go AML Reporting Solution — Financial Investigations Divisions).

THE POC (MLP) REGULATIONS, 2007

29. The bulk of the AML operational and regulatory control requirements can be found in these Regulations which were last amended in October 2019.⁷³ The operational controls and requirements are discussed below and include the following:—

(a) Threshold Transaction Reporting (‘TTR’)

- (i) Regulation 3(1)⁷⁴ sets out the threshold reporting requirements for financial institutions to report to the designated authority all cash transactions involving the “prescribed amount as per the limits which have been tiered in relation to financial institutions.⁷⁵ (See paragraph 29(a)(iv) below). This report shall be done within fifteen days after the end of the month and the duty to report exists even where no transactions have been carried out during the relevant month.⁷⁶

Cash transaction reporting requirements are not applicable to cash transactions carried out by a Ministry, Department of Government, statutory body or authority; a company in which the Government or an agency of Government is in a position to influence the policy of the company; an Embassy, High Commission, consular office or organization to which the Diplomatic Immunities and Privileges Act apply or any organization in relation to which an order is made under Section 3(2) of the Technical Assistance (Immunities and Privileges) Act;

- (ii) Pursuant to regulation 3(8) the threshold reporting limits⁷⁷ for financial institutions are as follows:—
 - 1. Financial institutions other than cambios — US\$15,000 or more or the equivalent amount in any other currency;
 - 2. Cambios and bureau de change — US\$8,000 or more or the equivalent amount in any other currency;
 - 3. Remittance companies — US\$5,000 or more or the equivalent amount in any other currency.
- (iii) Regulation 4(1)A Financial Institution may apply to the Minister responsible for Finance for an exemption in relation to a transaction or series of transactions to be carried out by a customer for the requirements of Regulation 3.

Regulation 4(2) allows the Minister to grant this exemption to established customers (defined as customers with whom the institution has done business for at least 12 months immediately preceding the application), where he is satisfied having regard to the following circumstances:

- 1. the transaction or series of transactions involve the deposit into or withdrawal of monies held by such an established customer from an account in a financial institution;
 - 2. the customer carries on:—
 - ✓ a retail business, not including the sale of motor vehicles, vessels, farm machinery or aircraft; or
 - ✓ a business declared by the Minister by order to be an entertainment business or a hospitality business for the purposes of this Regulations;
 - 3. the account through which the transactions are conducted is maintained for the purpose of such business; **and** critically,
 - 4. the amount of money involved is not over and above an amount that is reasonably commensurate to the lawful activities of the customer.
- (iv) Financial institutions shall be required to apply appropriate due diligence mechanisms to ensure that their transactions do not breach the threshold transaction reporting (TTR) limits. It should also be noted that the passage in 2013 of the amendments to the POCA which introduced the cash transaction limit of JMD 1 million coupled with the current exchange rate (JMD 159.7315⁷⁸ to USD1 as at 12/09/2025), have the resulting effect of a cash transaction that amounts to, or exceeds approximately USD 6,261 breaching section 101A of the POCA if that transaction is not conducted with a permitted person as discussed above at the paragraph (29(a)(ii)) on cash

⁷³ A number of amendments were made to these Regulations most recently through the Proceeds of Crime (Money Laundering Prevention) (Amendment) Regulations, 2019.
⁷⁴ Last amended in 2019.
⁷⁵ Regulation 3(8).
⁷⁶ In these circumstances the report should indicate that no such transactions have been carried out.
⁷⁷ POC (MLP) Regulations, 2007 regulation 3(7) & (8) as amended in 2019 where fine is increased to not exceeding \$1,000,000.00.
⁷⁸ BOJ weighted average sell rate as at 12/09/25.

transaction limits. FIs therefore need to be mindful of this situation.

(v) Under the TTR regime the designated authority can request information from financial institutions on any of the following persons exempted under the TTR regime — i.e. a Ministry, department or agency of Government; a statutory body or authority or a Government company. (Refer Regulation 3(3)). Additionally, the designated authority has the power under the regime to issue directions to a regulated business in relation to matters arising from TTRs and STRs filed⁷⁹. These directions can be issued in relation to:—

1. previous or current reports;
2. the provision of information regarding a report at 1.;
3. the provision of additional information in response to queries concerning specific matters arising from a report at 1. including:
 - ✓ due diligence procedures followed in relation to a specific transaction;
 - ✓ persons authorized to sign on a specific account;
 - ✓ errors identified in the report; and
 - ✓ such other matters specified in the directions. (Regulation 3(6)⁸⁰)

(i) KYC/ Customer Due Diligence (‘CDD’) requirements

(i) Risk Profile

Businesses in the regulated sector are required to establish a risk profile regarding its operations generally AND a risk profile regarding all its business relationships and one-off transactions with a view to determining the level of risk for each. Once these assessments are completed the business must employ mitigation measures commensurate with the risks identified. (Regulation 7A⁸¹).

The basis on which such profiles are established shall be guided by the respective risk assessments undertaken as discussed in these Guidance Notes at Section IV below. ‘High risk’ relationships or transactions which require the application of enhanced due diligence procedures are categorized in the law at paragraph 2 of regulation 7A and include the following—

1. Politically Exposed Persons (‘PEPs’);
2. Trustees;
3. A person who is not ordinarily resident⁸² in Jamaica;
4. A company having nominee shareholders, or shares held in bearer form;
5. Where the applicant for business is not the ultimate beneficial owner of the assets concerned in the business relationship or one-off transaction⁸³;
6. A member of such other class or category of persons as the supervisory authority may specify by notice published in the gazette.

It should be noted that where the applicant for business ceases to be a person considered not ordinarily resident in Jamaica, FIs are mandated to determine whether the level of risk of money laundering

⁷⁹ Regulation 3(6) of the POC(MLP) Regulations.

⁸⁰ Failure to comply with these directions is a criminal offence subject to a one million dollar fine before the Parish Court; Reg. 3(7).

⁸¹ POC(MLP) Regulations 2013 as amended in 2019.

⁸² Ordinarily resident is not defined in legislation. Applying its ordinary dictionary meaning it would mean someone who is usually or normally resident in Jamaica. Further guidance may be found in the definition of “resident of Jamaica” as contained in the Income Tax Act which states that: The Income Tax Act, S 29, describes for tax purposes a person who is ordinarily resident in Jamaica versus one who is resident for a temporary purpose as:

an individual who is in the island for a period aggregating six (6) months or more in any tax year. Where there remains a lack of clarity further Supervisory Guidance may be sought.

⁸³ POC(MLP) Regulations 7A(2), 2019.

involved nevertheless requires the application of enhanced due diligence procedures. (Regulation 7A (2) (f)).

Pursuant to Regulation 7B where the customer is a member of a class or category of persons specified by the Supervisory authority by notice in the gazette the competent authority is empowered to direct businesses in the Regulated sector to carry out additional actions such as providing reports at more frequent intervals and imposing limits on the business relationships or transactions.

(ii) Reasonable Due Diligence

Financial institutions are mandated by regulation 7A(3) to carry out reasonable due diligence in the conduct of every transaction to ensure the transaction is consistent with an institution’s knowledge of the transacting Party’s—

- 1. business, trade or profession;
- 2. risk profile; and
- 3. stated source of funds involved in the transaction.

In addition to the foregoing, financial institutions are also mandated in this regulation in relation to each transaction conducted, to verify the identity of the transacting party as well as the source of funds involved in the transaction.

Regulation 7(5) contains the following definition of “customer information”, “Customer information includes applicant for business’s full name, current address, taxpayer registration number or other reference number, date and place of birth and mother’s maiden name (in the case of an individual)⁸⁴, where applicable, the information referred to in regulation 13(1) (c) and any other information used to verify the applicant’s identity or nature of the business’s trade, profession or source of funds. (See also section 120(1) & (2) POCA) which outlines the KYC information a financial institution must be in a position to provide pursuant to customer information orders.

(iii) Simplified Due Diligence⁸⁵

Regulation 7A(5A) speaks to businesses in the regulated sector being allowed to apply simplified due diligence procedures (SDD) where a business relationship or one-off transaction is determined to be low-risk and they have met certain conditions as outlined in 7A(5B) to include conducting a proper evaluation of the risk which justifies the adoption of SDD, identified and documented the risks of money laundering involved and implemented appropriate controls and systems to reduce or mitigate those risks and reviewed the risks and controls and systems on an ongoing basis and taking into account any guidance issued by the competent authority on aspects relevant to the determination of this matter.

(iv) In addition to the foregoing, the POC (MLP) Regulations, 2007 require the following—

- 1. Periodic updates of customer information must be carried out at least once every seven years or at more frequent intervals as warranted by the risk profile of the business relationship; this is applicable to existing and new customers. (Regulation 7(1)(c) and (d) and 19(3)⁸⁶).

Where customer information is not updated the business relationship shall not proceed any further and the business

⁸⁴ Regulation 7(5) was amended in 2019.
⁸⁵ Discussed further in Section IV below.
⁸⁶ Existing customers transactions dating back to March 2007.
⁸⁷ That is, disclosures as to transactions which could constitute or be related to money laundering.

is required to make ALL required disclosures under section 94 of POCA.⁸⁷;

2. Transaction verification procedures⁸⁸ must be applied particularly in the circumstances specified in regulation 7(3) which include cases where — the transaction meets the TTR; transactions appear to be linked; wire transfer transactions are being conducted; a required disclosure (STR) is to be made; or there is doubt about the accuracy of any previously obtained evidence of identity;
3. KYC details must be retained for electronic funds transfers. This includes relevant information throughout the payment process and chain such as correct name, address and account number (if any), reference number assigned to the transaction and any other relevant reference numbers and instructions given in relation to the transfer. This information should identify and verify the identity of the recipient of the funds transferred where the amount exceeds USD 500 or its equivalent. Critically the financial institution should have in place risk-based policies and procedures for determining “whether to execute, reject or suspend the transfer” where the identification is not made or unverifiable. (Regulation 9 (1) as amended in 2019)

Further in respect of transfers which exceed USD500⁸⁹ or the equivalent amount in any other currency, the KYC details must include—

- ✓ a national identification number;
- ✓ the customer identification number; or
- ✓ the date and place of birth of the person who places the order for the transfer and the holder of the account that is the source from which the funds are transferred. (Regulation 9(2A)⁹⁰);
- ✓ the law reflects that the business from which the transfer originates must provide the KYC details to the business to which the funds are transferred within three days of being requested so to do by the business to which the funds are transferred. (Regulation 9(2B)).
4. Procedures must be in place to ensure that the identities of both principals and agents are obtained in the case of transactions being conducted by a person on behalf of another; (Regulations 11,12 and 13)⁹¹;
5. Procedures must be in place to ensure that the identities of the beneficiaries and ultimate beneficial owner of the property or funds which are the subject of the transaction and/or business relationship are obtained; (Regulation. 11, and 13)⁹²;
6. Financial institutions must ensure the retention of records not only for identification records, but also for transaction records⁹³; (Regulation 14)⁹⁴)
7. Financial institutions must adhere to the prohibition against maintaining anonymous, fictitious or numbered accounts; (Regulation 16);

⁸⁸ Taking such measures specified in the procedures of a regulated business that will produce satisfactory evidence as to the purpose of and intended nature of the business relationship or one-off transaction — (POC (MLP) Regulations, 2007 — regulation 7(2)(a)).

⁸⁹ POC(MLP) Regulation 9(2A) as amended in 2019.

⁹⁰ FATF Recommendation 16 (Wire Transfers) and the related Interpretive Note. See POC(MLP) amendment in 2019.

⁹¹ POC (MLP) Regulations, 2007 as amended in 2019.

⁹² POC (MLP) Regulations, regulation 11 and 13 - First Schedule to the POC (Amendment) Act, 2013.

⁹³ As amended in 2019. A record should also be kept of all correspondence and analysis undertaken in relation to each transaction and business relationship which can facilitate the reconstruction of transactions and the provision of information to the competent authority. Additionally, all account files must be kept in relation to each customer containing all pertinent information in respect of each of the customer’s accounts with the regulated business (including customer information etc.)

⁹⁴ As amended in 2019.

8. Financial institutions must ensure that the CDD updated requirements are applied to existing customers. (Regulation 19)

- ✓ Financial institutions must ensure that required disclosures are filed on the statutory STR Form 1 (See Form I in the Schedule to these Regulations)

Financial Institutions other than remittance services, can apply a de minimis transaction amount of US\$250.00 below which the regulation 7 identification procedures will not be required unless the nature of the transaction is suspicious (See Regulation 8) and (see paragraph 156 below);

- 30. Financial institutions should note that the above AML obligations comprise specific FATF requirements for jurisdictions to have in place in order to be considered as having effective KYC/CDD regimes. In complying with obligations under POCA and its Regulations financial institutions should consult with their respective legal advisors.
- 30A. A breach of the relevant Regulations is a criminal offence attracting significant penalties. As stated above a conviction for a criminal offence may have serious implications for the continuance of operations of a licensee.
- 30B. Section 138 of the POCA MLP Regulations amendment 2019 has introduced the option for the Regulator to exercise its discretion to impose an administrative sanction of a fixed penalty. This approach allows for a more efficient and robust regulatory response to the statutory AML preventative measures in the legislation. The application of a fixed penalty may be done instead of or in conjunction with any additional enforcement measures. Currently the fixed penalty regime is available to specified offences as outlined in Part I of the Second Schedule to include offences found in Regulation 7, 7A and 7B as discussed above.

Terrorism Prevention Act, 2005 (“TPA”)

- 31. The TPA was passed in 2005, and amended in 2010, 2011, 2013 and the latest amendments came into effect November 2019. The Act outlines the following as terrorist financing offences:—
 - (A) directly or indirectly, wilfully and without lawful justification or excuse collecting property, providing or inviting a person to provide, or make available property or other related services,—
 - (a) intending that they be used, or knowing that they will be used in whole or in part—
 - (i) for the purpose of facilitating⁹⁵ or carrying out terrorist activity, or
 - (ii) for the benefit of any entity known to be committing or facilitating any terrorist activity;
 - (b) knowing, that in whole or in part, they will be used by or will benefit a terrorist group (section 4);
 - (B) Facilitating or carrying out a terrorist activity by—
 - (i) using property directly or indirectly, in whole or in part; or
 - (ii) possessing property intending that it be so used or knowing that it will be so used directly or indirectly in whole or in part (section 5).
 - (C) Dealing directly or indirectly in or with any property that is owned or controlled by or on behalf of a terrorist group or derived or generated from property owned or controlled by or on behalf of a terrorist group (section 6 (1)(a));
 - (D) Entering into or facilitating, directly or indirectly, any transaction in respect of property owned or controlled by or on behalf of a terrorist group (section 6(1)(b));
 - (E) Providing any property referred to in section 6(1)(a) or financial or other related services in respect of that property for the benefit of or at the direction of a terrorist group (section 6(1)(c));
 - (F) Converting any such property or taking any steps to conceal or disguise the fact that the property is owned or controlled by or on behalf of a terrorist group. (Section 6 (1)(d))⁹⁶;
 - (G) Providing any financial or other services to facilitate any person leaving or attempting to leave Jamaica in order to carry out a terrorism offence. (Section 8(3)(b)).

The TPA states that a person who commits any of these listed offences⁹⁷, is liable on conviction, in the case of an individual, to life imprisonment, and in the case of a body corporate, to a fine.

⁹⁵ By virtue of section 4(3) the meaning of facilitating terrorist activity shall be construed in accordance with section 8. Facilitating terrorist activity has been defined as including leaving or attempting to leave Jamaica to facilitate a terrorism offence or providing any financial or other services to facilitate any person leaving or attempting to leave Jamaica in order to carry out a terrorism offence.

⁹⁶ There shall be no civil liability whether for act or omission where a person took all reasonable steps to comply with sections 6(1)(a) - (d). Section 6(3) as amended in 2019.

⁹⁷ See section 2 for definition of terrorism offence which includes conspiring, attempting to commit, aiding or abetting, procuring or counselling.

32. The TPA defines the following terms in Section 2:—

- (a) ‘Applicable property’ — means any property wherever situated) derived, obtained or realized, directly or indirectly from the commission of a terrorism offence or that has been used, in whole or in part, to facilitate or carry out a terrorism offence, whether in the hands of the offender or the recipient of a tainted gift.

Specific rules have been set out to allow for identification of applicable property⁹⁸—

- (i) in which an interest is held — this constitutes property held by a person or property vested in a person as trustee in bankruptcy or liquidator;
- (ii) in which an interest is obtained — constitutes property obtained by a person; and in relation to property comprising land, this includes an interest involving any legal estate or equitable interest or power. In relation to property other than land, this includes a ‘right’ (such as a right to possession);
- (iii) in which an interest is transferred or granted — this constitutes property transferred to a person;
- (iv) in which a person is beneficially interested or in which a person would be beneficially interested if the property was not vested in another as trustee in bankruptcy or liquidator;

This definition ensures that property held by designated persons; terrorist organizations and other supporters of terrorism, by themselves or jointly with third parties, wherever situated, is subject to the tracking and enforcement mechanisms;

- (b) ‘terrorism offence’ and ‘terrorist activity⁹⁹’ to include conspiracies, or attempting to commit or inciting¹⁰⁰, aiding, abetting, procuring or counselling activities;
- (c) ‘tainted gift’ where an offender transfers property to another person for consideration which is significantly less than the value of the property. That property will constitute a tainted gift and the benefit gleaned will be calculated as the difference between the property value at the time of the transfer and the consideration,¹⁰¹ Further this applies to the giving of a gift by the offender at any time during or after the commission of the terrorism offence concerned.

Property that can be traced in this regard will either be property given to the recipient and being held by the recipient; or any property in the recipient’s hands which directly or indirectly represents the property given; or property given to and held by the recipient and any property in the recipient’s hands which directly or indirectly represents the other part of the property given.

- (d) ‘competent authority’ means the Minister of Finance or a person designated by him which additionally, are the Bank of Jamaica and FSC as of May 2015.
- (e) ‘designated authority’ means the Chief Technical Director of the FID.

33. The TPA also requires that financial institutions¹⁰²:—

- (a) determine on a continuing basis whether they are in possession or control of property owned or controlled by or on behalf of a listed entity. A listed entity is one which is either designated as a terrorist entity by the United Nations Security Council, or is an entity which the DPP has requested the court to designate as a listed entity on the basis of there being reasonable grounds to believe the entity has knowingly committed or participated in the commission of a terrorism offence; or is knowingly acting on behalf of, at the direction of or in association with such an entity or not being an individual is owned or controlled, directly or indirectly by a relevant entity; (section 14¹⁰³)
- (b) report all suspicious transactions to the designated authority¹⁰⁴, which under the TPA is, the DG of FID or such other person as the Minister may substitute by order, subject to Affirmative Resolution and published in the *Gazette*; (section 15¹⁰⁵)
- (c) make and retain a record for a minimum seven years of all complex, unusual or large business transactions and unusual patterns of transactions whether completed or not which are inconsistent with the normal transactions carried out by a customer with a reporting entity; (section 16)

⁹⁸ TPA Sections 2(2)-(7).
⁹⁹ Definition of terrorist activity in Section 2 of the TPA was amended in 2019.
¹⁰⁰ As amended in 2019.
¹⁰¹ Terrorism Prevention (Amendment) Act 2013 First Schedule (section 2).
¹⁰² Which was amended in 2019 to include life insurance businesses within the meaning of the Insurance act, or insurance intermediaries in respect of life insurance but does not include an insurance consultant or adjuster. Which was also amended in 2021 to include “a microcredit institution licensed under the Microcredit Act”. See MCA sixth schedule.
¹⁰³ As amended in 2019.
¹⁰⁴ In March 2006 the Minister designated the CTD of the FID the designated authority for the purposes of reporting obligations and other specific obligations outlined at sections 15-18 of the TPA. Section 15 TPA has been amended to indicate that the CTD of the FID is the designated authority,
¹⁰⁵ The Terrorism Prevention (Amendment) Act, 2013, new section 15(1) and new subsection (9).

- (d)

in relation to all business relationships and transactions with any customer resident or domiciled or in the case of a body corporate, incorporated in a specified territory apply enhanced due diligence measures, ensure that the background and purpose of the relationships and transactions are examined and these findings set out in writing and limit the business relationships and one-off transactions in accordance with enhanced terrorist financing countermeasures; (section 16A);
- (e)

ensure that high standards of employee integrity are maintained, and that employees are trained on an ongoing basis regarding their responsibilities under the Act; (section 18);
- (f)

establish and implement programmes, policies, procedures and controls for enabling them to fulfil their duties under the TPA. Towards this end, financial institutions must designate a Compliance Officer at management level and arrange for independent audits to ensure that their compliance programmes are effectively implemented. (section 18)
34. Breaches of the obligations reflected in paragraph 33 are offences that will attract the following penalties:—

(a)

Under sections 15 and 16 an individual is liable on conviction in a Parish Court, to a fine not exceeding JMD\$1 million dollars or to imprisonment for a term not exceeding twelve months or to both fine and imprisonment, and in the case of a body corporate, to a fine not exceeding JMD\$3 million dollars.

(b)

Under section 17 where there are unauthorised disclosures by persons of information relating to actions or proposed actions of the designated authority relating to an investigation being conducted or about to be conducted in relation to a terrorism offence, unless such disclosure is made to an Attorney-at-Law for the purpose of obtaining legal advice, facilitating the investigation, or any proceedings which might be conducted following the investigation. An individual is liable on conviction, to imprisonment for a term not exceeding two years and/or a fine of not more than JMD\$2 million and in the case of a body corporate, to a fine not exceeding JMD\$6million dollars. (Section 17).

(c)

For breaches of sections 15(6) and 17(2), tipping off offences—

(i)

Disclosing the existence of a report under section 15(3) to any person other than the designated authority (refer to section 15(6)), the penalty on conviction in a Parish court in the case of an individual is a fine not exceeding JMD\$1 million and/or imprisonment for a term not exceeding 12 months; and in the case of a body corporate, the penalty on conviction is a fine not exceeding JMD 3 million.

(ii)

Knowing or suspecting that a report has been made to the designated authority and disclosing any information or matter relating to a report under section 15(3) or 16(3) (refer to section 17(2)), the penalty on conviction in a Parish court in the case of an individual is a fine not exceeding JMD 2million and/or imprisonment or a term not exceeding 2 years; and in the case of a body corporate, the penalty on conviction is a fine not exceeding JMD 6 million.
35. The following Table outlines the enforcement powers under the TPA.

AREAS OF ENFORCEMENT UNDER THE TPA

Areas of Enforcement	Section of Act/Regs.	Responsible Authority	Additional Information
Listed entity procedures	Sec. 14	DPP	
Duty of entities to report	Sec. 15	CTD of the FID (as of Mar. 2006) DPP (in 2005)	The Act now reflects the designated authority is the DG of the FID.
Duty to make and retain a record of complex or unusually large transactions	Sec. 16(2)	CTD of the FID (as of Mar. 2006) DPP (in 2005) BOJ (as of May 2015) FSC (as of May 2015)	”
Duty to file STRs	Sec. 16(3)	CTD of the FID (as of Mar. 2006) DPP (in 2005)	”

AREAS OF ENFORCEMENT UNDER THE TPA, *contd.*

Areas of Enforcement	Section of Act/Regs.	Responsible Authority	Additional Information
Tipping off	Sec. 15(3) Sec. 16(2) Sec. 17(2)	CTD of the FID (as of Mar. 2006) DPP (in 2005)	The Act now reflects the designated authority is the CTD of the FID.
Implementation of regulatory controls to prevent TF	Sec. 18 (supplemented by 18A)	Competent Authority ¹⁰⁶ BOJ (as of May 2015) FSC (as of May 2015). Minister of Finance or other person designated as Competent Authority. (2005)	
Monitoring Orders	Sec. 19 Sec. 20	Relevant Authority DPP (2005)	i.e. either the DPP or the CTD of the FID.
Examination and production orders	Sec. 21	Relevant Authority DPP (2005)	i.e. either the DPP or the CTD of the FID.
Search Warrant	Sec. 23	Physical execution is achieved by the Constable named in the warrant.	
Forfeiture orders ss. 28-32	Secs. 28-32	Relevant DPP (2005)	i.e. either the DPP or the Authority CTD of the FID.
Restraint orders	Secs. 34-43	Relevant Authority DPP (2005)	i.e. either the DPP or the CTD of the FID.
Disposal (i.e. resolution of) property seized, restrained etc.	Sec. 44	Relevant Authority DPP (2005)	i.e. either the DPP or the CTD of the FID.

¹⁰⁶ Prior to 2015 this function in practice — was undertaken by the BOJ for DTIs, FHCs, credit unions, cambios and remittance services and by the FSC for persons licensed or registered under the Insurance Act, the Securities Act and the Pensions Act.

36. Sections 19-44 of TPA treat with enforcement and investigatory tools such as Forfeiture Orders (section 28), Pecuniary Penalty Orders (section 28(5A)), Restraint Orders (sections 34-41), Search and Seizure Warrants (sections 23-27), Account Monitoring Orders (sections 19 and 20) and Examination and Production orders (sections 21 and 22).

The foregoing orders operate with similar effect to those described under the POCA subject to the following differences:—

(a) *Account Monitoring Orders*

These remain in effect for 3 months. The order may be extended on an application by the relevant authority (DPP or CTD of FID) prior to the ending of the initial three months.

Account information is not defined, but, as is the case with the POCA, the monitoring order is applicable to information and documents regarding transactions conducted through an account by a particular person with the institution. Reference to transactions conducted through an account includes the making of a fixed term deposit including the transfer of funds deposited or any part thereof at the end of the term, a financial investment, and the opening, existence or use of a deposit box held by the institution.

There is no express wording that reflects that the order takes effect regardless of any restriction on the disclosure of the information however imposed, as is the case under the POCA at section 126(7)¹⁰⁷.

(b) *Examination and Production Orders (sections 21 and 22)*

Where a terrorism offence has been, is being or is likely to be committed and an entity has possession or control of information or documents relevant to same, the DPP or the CTD of the FID can apply to the court for information or documents to be made available for examination or for a production order. The application is made ex parte in writing, and if granted, the subject entity would be directed by the Judge to make the information or documents available for examination by a Constable named in the order, or to produce the information or document to the constable. An order to produce does not require the Constable to remove or retain any accounting records (including ledgers, daybooks, cash books and account books) used in the ordinary business of banking). An order can provide for these documents to be examined or copied wherever they are located. An examination by a Constable may include him taking extracts from or making copies of the information or document or where the information or document is produced retaining same for as long as is reasonably necessary.

(c) *Statutory safeguards to the powers of forfeiture*

Statutory safeguards to the above powers similar to those discussed above in relation to the POCA are also included in the TPA as follows:

- (i) In considering whether a forfeiture order should be made the Court must take into account—
 - 1. third Party rights and interests in the property;
 - 2. the gravity of the offence concerned;
 - 3. any hardship that might reasonably be expected to be caused to any person by the order;
 - 4. the use that is ordinarily made of the property or the intended use of the property; (section 28(5)).
- (ii) Not less than fourteen days written notice of an application for a forfeiture order must be given by the enforcing authority (i.e. DPP or CTD of the FID) to the Defendant and any other person it is believed to have an interest in the property targeted for forfeiture. Additionally, a copy of the notice must be published in a daily newspaper printed and circulated in Jamaica; (section 28(2))
- (iii) The entity convicted of the terrorism offence and any other person who claims an interest in the property may appear and adduce evidence at the hearing;
- (iv) Persons claiming an interest in the property targeted for forfeiture may apply to the court for an order and the Court, if it is so satisfied, shall make an order declaring the nature, extent and value of the person’s interest in the property. Before such an order is made the court must first be satisfied that the applicant was not in any way involved in the commission of the offence; that the person acquired his interest for sufficient consideration and without knowing or having reasonable grounds to suspect that at the time the property was acquired, it was used in, or derived from, obtained or realized directly or indirectly from, the commission of a terrorist offence; (section 31(2)).
- (v) A person with an interest in any property for which a forfeiture order has been made may appeal this order. (Section 33).

¹⁰⁷ It should be noted that this is a Court order and the legal non-compliance with a Court order can only be achieved by another Court order from a Court of higher jurisdiction. For example, by way of an injunction. Where there is no such order the legal obligation remains to comply with the order made.

Terrorism Prevention (Reporting Entities) Regulations, 2010 amended in 2013 and 2019

37. Section 47 of the TPA allows for Regulations to be made for giving effect to the provisions of this Act. Regulations under the TPA are subject to Affirmative Resolution. The Terrorism Prevention (Reporting Entities) Regulations were promulgated in March 2010 and last amended in November 2019. Under these Regulations, reporting entities include the financial institutions to which these Guidance Notes apply. These Regulations outline the operational procedures that must be maintained by financial institutions particularly when contemplating the commencement of a business relationship or conducting a one-off transaction. These regulations therefore largely mirror the POC (MLP) Regulations and require financial institutions to establish and maintain appropriate procedures in relation to establishing a risk profile for all business relationships and one-off transactions, identification of customers (including identification of the agent, ultimate beneficial owner or person who ultimately controls a legal person), record-keeping (minimum 7 year retention period), internal controls, communication, and training of employees. These Regulations also prescribe the requisite Declaration Forms for transactions which the reporting entity knows or suspects may constitute a terrorism offence; and for the quarterly reports as to whether or not the reporting entity is holding property etc. in respect of a listed entity.

37A. In October 2013 the Regulations were amended to cover the following relevant areas:

- (i) Expansion of the requirements for identification procedures Regulation 5(b) requires that as regards every business relationship the reporting entity concerned “*shall keep all customer information under review with a view to ensuring its accuracy.*” Further 5(b)(i) has now reads that not only should this review be conducted at least once every five years during the course of the business relationship “or at more frequent intervals as warranted by the risk profile of the business relations hop as determined by the reporting entity in accordance with regulation 6A.
- (ii) Codification of the risk-based approach
The 2013 amendment introduced Regulation 6A which addresses the legal requirements for establishing risk profiles and ongoing due diligence in verification procedures. This is discussed further below in the 2019 amendments. Of note is that this regulation outlines enhanced due diligence procedures and the entities for which enhanced due diligence procedures are required. (See 6A(5) and (6)).
- (iii) Regulation 11 was amended to extend to body corporates, a settlement or trust or any other type of legal arrangement. Further Regulation 11(2)(a) was introduced which extends to beneficiaries, ultimate beneficial owners of the property or funds of the transaction concerned.
- (iv) Regulation 13 was expanded to address the identification procedures in transactions involving a settlement, trust or other type of legal arrangement, a person other than an individual, a body corporate listed on a stock exchange registered, licensed or authorised in any manner as required under the laws of the jurisdiction.
- (v) Finally, Regulation 14(5) was amended to increase the prescribed period to seven years or such other longer period as may be specified by the designated authority by notice in writing given to the reporting entity before the expiration of the period referred to in sub-paragraph (a).

37B. In November 2019 the Regulations were farther amended to cover the following relevant areas:

- (i) Provision of additional clarity around identification procedures
Regulation 5(2) as inserted now makes it clear that when establishing a potential customer’s identity “... evidence of the applicant’s identity is satisfactory if it is reliable evidence of the identity of a customer from an independent source.”¹⁰⁸
- (ii) Codifying the risk-based approach
In keeping with the amendments to the POCA (MLP) Regulations, Regulation 7A echoes the risk-based approach to be adopted by businesses in the regulated sector. FIs are mandated to establish a risk profile regarding operations generally and a risk profile regarding all its business relationships and one-off transactions with a view to determining the relationships and transactions that are high-risk. Consequent on this assessment FIS are further mandated to employ measures commensurate with the risks to effectively mitigate same. Simplified due diligence procedures are prohibited for relationships or transactions where the business knows or believes or has reasonable grounds for knowing or believing is related to money laundering or terrorist financing.
- (iii) Simplified due diligence Procedures¹⁰⁹
Regulation 6A(5A) speaks to businesses in the regulated sector being allowed to apply simplified due diligence procedures (SDD) where a business relationship or one-off transaction is determined to be low-risk and they have obtained the written approval of the competent authority to adopt this route¹¹⁰.

¹⁰⁸ See paragraphs 75G-I below addressing the leveraging of the National identification system.
¹⁰⁹ Discussed further at paragraph 157 below.
¹¹⁰ Reference BOJ’s letter dated August 27, 2020, sent to all DTIs titled “Operationalization of Stratified Due Diligence using a Tiered Know your Customer Approach and footnote 243 below. Please note the distinction for the requirement of written approval of the competent authority for matters falling under the TPA and these Regulations. Further guidance to supplement this letter of August 27 will be issued by the Bank on the approach to be taken under the TPA in this regard.

Regulation 5B outlines some of the considerations to be taken by the competent authority before granting this written approval and includes the CA being satisfied that the regulated business has identified and documented the risks of terrorist financing involved and gives certain undertakings such as to implement appropriate controls and systems to reduce or mitigate these risks.

- (iv) Updating identification procedures in relation to agent transactions

Regulation 11(1) now states that identification procedures satisfy the regulation where the entity takes reasonable measures¹¹¹ in identifying and verifying the identity of the principal and the agent and each beneficiary and the ultimate beneficial owner of the property or funds the subject of the transaction concerned.

38. Under the CFT framework, an institution is required to report whether:—

- (a) The institution is, or is not, in possession of property for a listed entity (section 15); or
- (b) The institution is, or is not, in possession of property for a person included on the UN consolidated listing of individuals and entities pertaining to Al-Qaida pursuant to United Nations Counter-Terrorism Security Council Resolution 1267 (1999) — Afghanistan (section 15); or
- (c) The institution is of the view that a transaction conducted or being conducted or about to be conducted constitutes a transaction of the kind described at section 16 of the TPA (i.e. suspicious¹¹², unusual, complex¹¹³ etc.).

The requisite report must be made to the designated authority¹¹⁴ using either Form 1 (re: a report in relation to a) or b), or Form 2 (re: a report in relation to c)) provided in the Schedule to the Regulations.

Bank of Jamaica (Amendment) Act, 2022

38A. The Bank of Jamaica (Amendment) Act, 2022 (“BOJ (Amendment) Act”) was passed on June 14, 2022. This Amendment Act, amended in relevant part, section 2 of the Bank of Jamaica Act to include the definition of central bank digital currency (CBDC). CBDC is defined as ‘a digital form of currency issued by the Bank under section 12(1) that is legal tender of the country in electronic form.’

This Amendment Act also further amended the definition of cash under section 55 of the POCA to include CBDC.

38B. CBDC is money issued by the Bank in digital form. It is not held in a bank account but is held in a digital wallet that is issued by the Bank and distributed by Banks or authorised Payment Service Providers. It can be exchanged 1-for-1 with bank notes and coins. CBDC is the digital version of the fiat currency of the country and is not cryptocurrency.¹¹⁵

See paragraphs 114A-H below on the KYC and CDD obligations for FIs in relation to CBDC.

Financial Investigations Division Act, 2010

39. The Financial Investigations Division Act (“FIDA”) codified the establishment of the Financial Investigations Division (“FID”) which has been in operation since 2002, and is a Department of the MOFP. The FIDA also provides the statutory basis for the operations and objectives of the FID and outlines these as being to:—

- (a) Investigate all categories of financial crime;
- (b) Collect information and maintain intelligence databases on financial crime;
- (c) Maintain an arm’s length relationship with law enforcement agencies and other authorities of Jamaica and foreign States, and with regional and international associations or organizations, with which it is required to share information;
- (d) Exercise its functions (section 5) with due regard for the rights of citizens. These functions include collecting, requesting, receiving, processing, analysing and interpreting information relating to financial crimes; and transaction reports and any other reports made to or received by the Division; promoting public awareness and understanding of financial crimes and the importance of their elimination from the society; formulating and implementing guidelines and policies and an annual plan¹¹⁶ for the control and prevention of financial crimes; and the compilation and publication of statistics on reports made to the Division, the investigations carried out by the Division, and the prosecution of financial crimes and conviction of persons for financial crimes. The Division may also provide information on typologies and other materials relating to financial crimes to public bodies, and, after consultation with the competent authority, give guidance to financial institutions and designated non-financial institutions regarding their obligations under the FIDA and any other enactment. (Sections 3 & 4).

¹¹¹ Versus “requires reasonable measures to be taken”.

¹¹² The Terrorism Prevention (Amendment) Act, 2011 section 16(3A).

¹¹³ The Terrorism Prevention (Amendment) Act, 2011 section 16(3).

¹¹⁴ The Terrorism Prevention (Amendment) Act, 2013, new section 15(1).

¹¹⁵ [CDBC — FAQs-Booklet.pdf](#)

¹¹⁶ As approved by the Minister of Finance.

40. The FID is the designated authority to receive reports under the POCA (section 91(1)(h); the TP (Amendment) Act (section 15)); and The UNSEC Implementation Act (section 5(1)). The FID statistics and publications including advisories to financial institutions and to designated non-financial institutions can be accessed from its website at www.fid.gov.jm.
41. On June 05, 2014 the FID was accorded membership with the Egmont Group of Financial Intelligence Units.¹¹⁷

Criminal Justice (Suppression of Criminal Organizations) Act, 2014

42. This Act has as its main object the disruption and suppression of criminal organisations and other related matters. To that end, this Act criminalizes forming or establishing, participating in or being part of, a criminal organization, or knowingly facilitating the commission of a serious offence by or on behalf of a criminal organization.

Dangerous Drugs Act, 1948 (last amended 2021)

43. This Act makes it a criminal offence for any person to import, export, cultivate, manufacture, use, sell, transport or otherwise deal in opium, ganja, cocaine, morphine, or any derivatives thereof. In March 2015 this Act was amended to, among other things, modify the penalties applicable for the possession of specified small quantities of ganja and the smoking of ganja in specified circumstances, and for a scheme of licenses, permits and other authorizations for the cultivation or acquisition or use of ganja for medical, therapeutic or scientific purposes. This amendment became effective on 15 April 2015. In this regard the following must be noted:—

- (a) The possession of ganja not exceeding 2 ounces amounts to a contravention of the Act and is a punishable matter¹¹⁸ which will result in—
 - (i) notice that a contravention has occurred and giving the offender thirty days (or such longer period as may be specified in the notice) to pay a fixed penalty of five hundred dollars;
 - (ii) failure without reasonable cause or excuse to pay the penalty within the time period specified, is an offence for which the penalty on conviction in a Petty Sessions Court is to perform unpaid community service for between not less than forty nor more than three hundred and sixty hours; or a fine of two thousand dollars. (Section 7(F) &(G));
- (b) The Cannabis Licensing Authority is established by section 9A for the purpose of enabling the establishment of a lawful regulated industry in hemp and ganja for medical, therapeutic or scientific purposes. This Authority has the power to make regulations (with the approval of the Minister of Justice) for the issue of licenses, permits and authorizations for hemp and ganja for medical, therapeutic or scientific purposes. The Authority is also charged with ensuring that regulations made by the Authority do not contravene Jamaica's international obligations.
- (c) The possession of over 2 ounces of ganja remains a criminal offence, unless that possession is for religious purposes in adherence with the Rastafarian faith; or for medical or therapeutic purposes as prescribed or recommended in writing by a registered medical practitioner or other health practitioner or class of practitioners approved for that purpose by the Minister of Health by order published in the Jamaica Gazette; or for the purposes of scientific research by a duly accredited tertiary institution or otherwise approved by the Scientific Research Council or such other body prescribed by the Minister of Science, Technology, Energy & Mining (section 7C (2)).

The Firearms (Prohibition, Restriction and Regulation) Act, 2022

44. This Act repealed and replaced the Firearms Act, 1967. Akin to its predecessor legislation this Act deals with the regulation and licensing of the sale, purchase, acquisition, ownership, the prohibition and restriction and other dealings with regard to firearms and ammunition.

Law Reform (Fraudulent Transactions) (Special Provisions) Act, 2013

45. This Act has as its main object the prohibition and disruption of offences related to lottery scamming, advance fee fraud, fraudulent transactions and connected matters. The following offences are criminalised, among other things:—
- (a) obtaining property by a false pretence (section 3);
 - (b) inviting persons to Jamaica by a false pretence (section 4);
 - (c) using premises for purposes which constitute an offence under this Act (section 5);
 - (d) using an access device¹¹⁹ or other means to transfer or transport money or monetary instrument either within Jamaica, or between Jamaica and a place outside of Jamaica (section 6);

¹¹⁷ Co-Chairs Statement 22nd Plenary of the Egmont Group of Financial Intelligence Units, 01-6 June 2014 www.egmontgroup.org.

¹¹⁸ See section 7C(2) for the exceptions.

¹¹⁹ “any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, and any other means of access that can be used alone or with another device, to obtain a benefit or other thing of value, or that can be used to initiate a transfer of money;” — section 2 — The Law Reform (Fraudulent Transactions)(Special Provisions) Act, 2013.

- (e) stealing, forging or falsifying an access device; knowingly using an access device that has been revoked or cancelled with an intent to commit an offence; or knowingly possessing or using or trafficking in an access device or a forged or falsified access device that has been obtained, made or altered by an act or omission constituting an offence under this Act, and any other law or by an act or omission constituting an offence in a country other than Jamaica but which act or omission would constitute an offence had it been committed in Jamaica (section 8);
- (f) making, repairing, buying, selling exporting or importing, without lawful justification or excuse any instrument, device, apparatus, material or thing that a person knows has been used or is intended for use for copying data from an access device or forging or falsifying an access device; whilst knowing or having reasonable grounds to believe, that the money or monetary instrument involved in such transfer or transportation constitutes or is substantially related to the proceeds of some form of unlawful activity (section 9);
- (g) knowingly obtaining or possessing, transmitting, distributing etc., identity information including any biological information, name, address, date of birth, written signature, e-mail address, digital signature, user name, credit or debit card number, financial institution account number, Taxpayer Registration Number ('TRN'), Social Security Number or any other unique personal identification number or password (section 10).

Cybercrimes Act, 2015

46. This Act came into effect in December 2015 and repealed and replaced the earlier Act of the same name. It allows for the imposition of criminal sanctions for cybercrimes, and criminalizes, among other things:—
- (a) unauthorised access to computer program or data (section 3);
 - (b) access to any program or data held in a computer with intent to commit or facilitate commission of an offence (section 4);
 - (c) doing any act which it is known is likely to cause an unauthorized modification to the computer whether or not the act is directed at a particular program or data, or directed at a particular program or data held in a particular computer and whether or not the modification is temporary or permanent (section 5);
 - (d) the unauthorised access to any computer to access a service directly or indirectly or the unauthorised interception (directly or indirectly) of a function of any computer. Interception in this case includes listening, viewing or recording a function of the computer or the substance of such function (and excludes interceptions permitted under the Interception of Communications Act) (section 6);
 - (e) the unauthorized, or wilful failure, interruption or obstruction, of the operation of a computer, or the denial of access to, or impairment of, any computer program or data stored in the computer (section 7);
 - (f) fraudulently altering or interfering with data or a computer program with the intent of gaining an advantage for oneself or for another (section 8);
 - (g) using a computer to send to another person any data that is obscene, constitutes a threat, or is menacing in nature; with the intention of causing or being reckless as to whether the sending of the data causes, annoyance, inconvenience, distress, or anxiety, to that person or any other person (section 9);
 - (h) possessing, receiving, manufacturing, selling, importing, distributing, disclosing or otherwise making available, a computer, access code or password or any other device adapted primarily for the purpose of committing an offence at sections 3-9 (section 10).

47. The law states that where any of the foregoing offences involves a 'protected computer', an offender is liable on conviction before the Circuit Court to a fine or imprisonment for a term not exceeding 25 years, or both such fine or imprisonment, which is a higher penalty than included in the specific sections. A 'protected computer' is one which the offender knows or ought reasonably to know, is a computer which is involved with or used in connection with security, defence or international relations for Jamaica; the existence of a confidential source of information relating to the enforcement of the criminal law of Jamaica; the provision of services directly communications infrastructure, banking and financial services, public utilities, public transportation etc. (section 11)
48. Inciting, attempting, aiding or abetting the commission of any offence under sections 3-10 is also an offence and the person shall be liable to the same penalty as the substantive offence under this Act. (section 12).

Other Offences Relating to Fraud, Dishonesty, and Corruption

49. There are several statutes relating to these offences. Some examples are certain offences under the Companies Act, the Income Tax Act, the Customs Act, the Stamp Duty Act, the Charities Act, the Larceny Act, the Corruption Prevention Act, the Copyright Act and other enactments relating to the conferment of or protection and administration of intellectual property rights, and under the JBSA and the BOJA, the Credit Reporting Act, the Securities Act, the Insurance Act, and the Perjury Act. There are also offences that are found in the common law and not codified in statute, for example, Misconduct in a Public Office or Misprision of Felony.

Companies Act

- 49A. The Companies Act was last amended in 2023. The major amendments are related to the beneficial ownership regime, amendments to the nominee shareholder framework via the prohibitions on same and the introduction of a fixed penalty regime.

Some of the important amendments that were made are:

- (i) Section 2 amongst other definitions introduced and defined the following terms which are relevant to FIs in the conduct of their business. They are: *adequate, annual beneficial ownership, beneficial owner, beneficial ownership return, chain of ownership, companies to which Part X applies (that is companies incorporated outside the island carrying on business within the island), designated authority, designated non-financial institution, financial institution, ultimate effective control, ultimate ownership and up-to date.*

Beneficial owner is defined as (a) the individual who exercises whether directly or indirectly ultimate effective control and ultimate ownership of a company; (b) if there is no individual exercising both ultimate effective control and ultimate ownership of a company, the individual who exercises, whether directly or indirectly, either ultimate effective control or ultimate ownership; (c) the individual who exercises control or ownership in any of the ways stated in paragraph (a) or (b) over a company, body of persons, trust or other legal arrangement, who owns 25% or more of a company, or (d) in the absence of an individual referred to in paragraphs (a) or (b), an individual who is an officer of the company who exercises ultimate effective control of the management of the company.
- (ii) The prohibition on any company incorporated under this act of having a nominee shareholder. (Section 23A).
- (iii) The requirement to now provide beneficial ownership information where a return of allotment is filed with the Registrar of Companies.

This also applies where a company is incorporated outside of Jamaica but conducting business in Jamaica. In that instance the company should also produce a certificate of incorporation certified in accordance with section 377 AD(2). (Section 52 (1A and 1B))
- (iv) The requirement for a company to keep a register of its members to now include information as outlined on the beneficial owner of the company. (Section 109(1)(a) and 1A)
- (v) Where a company has notice of any trust whether express, implied, resulting or constructive affecting the membership of the company, the particulars of the beneficial owner shall be entered as required under section 109. (Section 116).
- (vi) The abolition of the nominee director and nominee shareholders for companies incorporated outside of Jamaica carrying on business within Jamaica. (Sections 172 1A and 363B)
- (vii) Introduction of the overseas branch register/register of directors. (Section 363A(a) and (b))
- (viii) Duty to make beneficial ownership return. (Section 377 A-H)
- (ix) Restrictions on share transfers and exercise of powers to borrow unless the information relating to membership and Beneficial ownership is accurate, up-to-date and in compliance with the Companies Act. (Section 377I)
- (x) Establishment of a register/registry for beneficial ownership information of companies. (Section 377J¹²⁰)
- (xi) Company’s duty to keep records of its actions in relation to beneficial ownership information to include a record of the measures used to verify the accuracy of the information. (Section 377R)
- (xii) Other obligations to obtain and verify beneficial ownership information. (Sections 377S and T), notify the Registrar of change in beneficial ownership. (377W)
- (xiii) The introduction of the Fixed Penalty Regime. (Section 386A)

The Prevention of the Proliferation of Weapons of Mass Destruction

- 50. Recommendation 7 (on targeted financial sanctions related to the prevention of the proliferation of weapons of mass destruction) of the revised FATF Forty Recommendations, 2012 requires countries to implement targeted financial sanctions relating to the prevention of weapons of mass destruction proliferation which are contained in the relevant UN Security Council Resolutions that have thus far been issued and remain in force in relation to the Democratic People’s Republic of Korea (DPRK) (Resolution 1718 (2006)) and successor resolutions thereto and as of September 27, 2025 has been reapplied to Iran.¹²¹
 - (a) targeted financial sanctions (*which should be implemented without delay*) include— freezing and prohibiting dealings in funds or other assets of designated persons and entities; and activity based financial prohibitions such as preventing the provision of financial services, financial resources or financial assistance related to the supply, sale, transfer, manufacture, maintenance, or use of items, materials, equipment, goods and technology prohibited by the UN Resolutions¹²².

¹²⁰ Jamaica Beneficial Ownership Registry.

¹²¹ See footnote 29 above re the application to Iran. Please note as well the scope of funds, financial assets and economic resources have been expanded for DPRK to include assets such as vessels and including those funds, other financial resources or economic resources outside of DPRK which are owned or controlled directly or indirectly by entities of the Government or by persons or entities acting on their behalf or at their direction or by entities owned or controlled by them and the State determines are associated with their nuclear or ballistic programmes or other activities prohibited by the relevant UNSCRs.

¹²² Refer also to FATF Guidance on Counter Proliferation Financing: the Implementation of Financial Provisions of UNSEC Resolutions to Counter the Proliferation of Weapons of Mass Destruction, last updated February 2018 (paragraph 11 page 6, paragraph 22 page 9; and Annex C).

- (b) compliance with these mandates to apply targeted financial sanctions requires the ability to be in a position to identify any related suspicious activity and to propose additional persons and entities to the UN Committees for designation. Accordingly, UN Member States have an obligation to ensure the necessary supporting framework is in place to allow for the:—
 - (i) designation mechanisms to allow for the nomination of persons to the UN Committees for designation;
 - (ii) implementation of the required measures and controls that will allow for the following measures to be applied—
 - 1. Identification of transactions, services or other relationships that would be prohibited by the UNSEC Resolutions;
 - 2. Appropriate reporting of the prohibited transactions, services or other relationships that have been identified; and
 - 3. Effective application of the required targeted financial sanctions in the manner required by the UN SEC Resolutions.
 - (iii) appropriate cooperation across borders and within borders (i.e. between countries and among national authorities);
 - (iv) protection of the rights of innocent third parties (e.g. de-listing mechanisms and unfreezing of assets); and
 - (v) orderly application of sanctions — that is, the application of sanctions through mechanisms that adequately address corresponding risks (if any) to financial and payment systems posed by the application of sanctions and which address the protection of the rights of innocent counter-parties acting in good faith. This could include for example, mechanisms designed to—
 - 1. prevent asset flight;
 - 2. facilitate authorization of certain payments by designated banks;
 - 3. permit payments due under prior contracts entered into prior to a person or entity being listed or designated provided such contracts do not involve services, items or assistance prohibited by the Resolutions and provided payments are not being made directly or indirectly to a designated person or entity;¹²³.

United Nations Security Council Resolution Implementation Act

- 51. The United Nations Security Council Resolution Implementation Act (UNSCRIA) was passed in November 2013 and amended in November 2019. It is designed to achieve Jamaica’s compliance with Recommendation 7 (on targeted financial sanctions related to the prevention of the proliferation of weapons of mass destruction) of the revised FATF Forty Recommendations, 2012.
- 52. This Act is an enabling legislation which forms the basis for Jamaica to respond to directives or resolutions issued by the UNSEC by promulgation of the requisite Regulations under this Act. Accordingly, the Act defines certain terminology (section 2)—
 - (a) “asset” (property of any kind, tangible or intangible, moveable or immovable, however acquired whether wholly or jointly owned directly or indirectly by a person or entity that is proscribed under section 3(2)(a) or a person or entity acting on behalf of such a proscribed person or entity);
 - (b) “designated non-financial institution” (i.e. a person designated under the POCA as well as persons listed at section 15 of the TPA);
 - (c) “financial institution” (same as FIDA similar to POCA and TPA¹²⁴)¹²⁵;
 - (d) “relevant authority” (that is, regulator of financial institutions or financial services — such as the BOJ and the FSC), regulator of designated non-financial institutions (such as the General Legal Council, the Real Estate Board, the Betting Gaming and Lotteries Commission and the Casino Commission), border control authorities (such as Jamaica Customs Agency and Passport, Immigration and Customs Agency (PICA), defence authorities (such as the Jamaica Defence Force (JDF) and the Coast Guard and the entity with responsibility for foreign relations (i.e. Ministry of Foreign Affairs and Foreign Trade (MFAFT)), the Jamaica Constabulary Force; any other entity to whom a UN sanction enforcement law requires information or a document to be given;

¹²³ Refer also to FATF Guidance on the Implementation of UNSEC Resolutions to Counter the Proliferation of Weapons of Mass Destruction, updated February 2018 (Annex A).

¹²⁴ Please note the amendment to the MCA in 2021 to the definition of financial institutions which also extends to a microcredit institution licensed under the MCA. Please note the amendment in 2019 to refine the inclusion of insurance business.

¹²⁵ FIDA is the only other statute which refers to cooperative societies which undertake credit union business neither the POCA nor the TPA reflect this qualification in the reference to cooperative societies in the respective definitions of ‘financial institution’.

53. The Act provides for the following:—

- (a) the Minister may make Regulations pursuant to any designations by the UN within 30 days of such designation (New Section 3(1) incorporated under the 2019 Amendment Act);
- (b) the implementation of TFS by way of Court Orders, that is on application by the DPP to a Judge of the Supreme Court for an order declaring a person or entity to be a proscribed person or entity as the case may require. (See section 3A as included via the 2019 Amendment Act and specifically section 3A (2));
- (c) imposes a duty on financial institutions and designated non-financial institutions, *on a continuing basis*, to determine whether or not they are in possession of property or control for a person prescribed by regulations made under section 3(2)(a) or and Order under section 3A and to report whether they are, *or are not*, in possession of property for a person who is so prescribed (section 5). These reports are to be made to the designated authority, which is defined in the Act, to be the CTD of the FID under the FIDA, (section 5(1)). Reporting in this regard must be done in compliance with any directions that may be given by the designated authority, (section 5(4)); and the fact that a report has been made must not be disclosed to any other person, (section 5(6)). These reports are due once every four calendar months. Reports are also due upon request of the designated authority (section 5(3));
- (d) consequent on the 2019 amendments, financial institutions are also required to report any transaction, attempted transaction, assets owned or controlled by or on behalf of such proscribed person or entity by regulations made under section 3(2)(a) and by an order made under section 3 A and in possession or control of the entity; any breach of any provision of UNSCRIA by a proscribed person or entity, any assets owned and controlled by or on behalf of or in possession or control of a proscribed entity and any other action that has been taken in relation to a proscribed person or entity. These reports are mandated to be disclosed to the BOJ as regulator of FIs. (Section 5 (3A and B).
- (e) provides for requests for delisting for persons or entities proscribed under this Act. (Section 5 A as amended in 2019);
- (f) Prohibits dealing whether directly or indirectly in any assets owned or controlled by or on behalf of or at the direction of a proscribed person or entity to include funds derived or generated from such property, entering into or facilitating, directly or indirectly any transaction in respect of these assets, providing financial or other related services in respect of such assets or making any property or any financial or other related service available directly or indirectly for the benefit of, or converting or taking steps to convert or disguise any such property owned or controlled by or on behalf of the proscribed person or entity. (Section 8A, 2019 amendment)¹²⁶;
- (g) provides for statutory protections for persons with reporting obligations under this Act, from civil or criminal liability for breaches of confidentiality; (sections 5(5) re: reporting to the designated authority and 18 re: disclosures to the relevant authority);
- (h) provides for the designation of any provision of a law in Jamaica as a UN sanction enforcement law. This designation is done under section 9 and can only be done to the extent that it gives effect to a decision made by the UNSEC under Chapter VII of the UN Charter and which Jamaica would be obliged to carry out under Article 25 of the UN Charter;
- (i) provides for monitoring compliance with any UN sanction enforcement law by empowering the regulated authority by written notice to request from any person the information or documents specified in the notice. Non-compliance with this request constitutes an offence (sections 14 and 15) however a person is not required to give any information or document in response to a request, if to do so would violate legal professional privilege (section 14(7));
- (j) provides for the development of regulations to give effect to the Act (such as programmes and policies to be implemented by entities to ensure compliance with the Act; forms of reports or returns to be made under the Act, prescription of penalties) (section 21) and to give effect to the UNSEC Resolutions (section 3);
- (k) Mandates notification of designations by the relevant authority, of all designations and delistings of proscribed persons and entities; and to issue guidelines to FIS on measures to prevent PF. (Section 14A as introduced in the 2019 amendment);
- (l) when a directive or resolution is issued from the UNSEC mandating members to take certain actions and/or refrain from activities pursuant to such directive or mandate, Jamaica would then issue the requisite Regulation under this Act giving effect to such a decision and outlining the specific parameters of compliance (section 3). The 2013 Regulations (now revoked by the 2021 Regulations) in this regard was issued simultaneously with the passage of this Act in relation to the jurisdiction of the Democratic People's Republic of Korea.

¹²⁶ Where a person is found to have acted reasonably in taking or omitting to take the measures to comply with section 8A(1) he shall not be liable civilly from having taken or omitted to take the measures if he took all reasonable steps to satisfy himself that the relevant assets were owned or controlled by, or on behalf of the proscribed person or entity. Section 8A(2).

The United Nations Security Council Resolutions Implementation (Democratic Peoples Republic of Korea Sanctions Regime) Regulations, 2021

54. The United Nations Security Council Resolutions Implementation (Democratic People’s Republic of Korea Sanctions Regime) Regulations, 2021¹²⁷ (UNSCRI (DPRK Sanctions Regime) Regulations) were issued pursuant to section 3 of the UNSCRIA and by virtue of Regulation 43 of these new 2021 regulations gazetted on March 16, 2026, revokes and replaces the United Nations Security Council Resolutions Implementation (Asset Freeze — Democratic People’s Republic of Korea) Regulations, 2013. These 2021 Regulations more comprehensively outline Jamaica’s mandates in relation to the directives of the UNSEC regarding the Democratic People’s Republic of Korea (DPRK) in Resolutions 1718(2006) and successor resolutions 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2345 (2017), 2356 (2017), 2371 (2017), 2375 (2017) and 2397 (2017). These resolutions represent UN required sanctions comprising financial prohibitions to prevent the provision of financial services, financial resources or financial assistance to the DPRK, (paragraph 50 above).
55. These Regulations in relevant part criminalize the following activities:—
- (a) provision of a sanctioned service other than in relation to an authorised supply (regulation 14 (1));
 - (b) procuring a sanctioned service from the DPRK, a person in the DPRK or a national of the DPRK (regulation 14(2)(a), (b) and (c)¹²⁸);
 - (c) knowingly engaging in any sanctioned commercial activity (regulation 16)¹²⁹;
 - (d) knowingly using or dealing with freezable assets without authorisation, that is, (a) assets owned or controlled by an entity designated in Annex I or Annex II to UNSEC Resolutions 2087, 2094, 2270, 2321, 2356, 2371, 2375 or 2397, or, (b) derived or generated from any asset owned mentioned at (a), or (c) a vessel designated by the Committee under paragraph 12(d) of Resolution 231 or any cargo contained in that vessel (regulations 17(1))¹³⁰ and 18(1);
- A designated entity is defined under Regulation 2 as a person or entity (a) designated under regulation 4, (b) designated by the Security Council or the Committee for the purposes of paragraphs 8(d) of Resolution 1718; or (c) to whom the measures mentioned in paragraph 8(d) of Resolution 1718 apply under a decision of the Security Council or Committee.
- (e) allowing freezable assets to be used or dealt with (regulation 18(1)(b));
 - (f) facilitating any use of or dealing with, freezable assets (regulation 18(1)(c));
 - (g) knowingly, directly or indirectly making a freezable asset available to a designated entity without Authorisation or as permitted by an Authorisation (regulation and 18(3));
 - (h) holding a bank account and failing to comply with a notice issued to that person in under regulation 19(1). (regulation 20)).
56. The Regulations state that they have effect as a UN sanction enforcement law for the purposes of section 9 of UNSCRIA and accordingly the offence provisions contained there in sections 10 - 12 shall apply to the contravention of named regulations inclusive of those listed in paragraph 55 above. (See regulation 3(2)). The Regulations have extra-territorial effect and criminal liability arises for a contravention of the Regulations in the following circumstances:
- (i) conduct occurring wholly or partly in Jamaica, or wholly or partly on board a Jamaican aircraft or ship;
 - (ii) conduct occurring outside of Jamaica, where a result of the conduct occurs — wholly or partly in Jamaica or on board a Jamaican aircraft or ship; or
 - (iii) conduct occurring outside of Jamaica, where the person is a national of Jamaica at the time of the offence or is a body corporate incorporated under the laws of Jamaica at the time of the offence (see regulation 3(4)(a)(i) and (ii); or
 - (iv) aiding, abetting, procuring, counselling conspiring in, or attempting the commission of any of the mentioned offences where the conduct constituting the offence occurs outside of Jamaica and/or is intended by the person to occur, wholly or partly in Jamaica or on board a Jamaican aircraft or ship. (See regulation 3(4)(b))

The Regulations further stipulate that no action shall lie against any person or entity for breach of contract or failure to perform a transaction where the contract or transaction was prevented by the Act or these Regulations or because of any relevant Security Council resolutions existing from time to time.

The Regulations further outline the process for the obtaining of Authorisations engaging in sanctioned commercial activity, for dealing with freezable assets and the provision of sanctioned services. (See regulations 34 -36 respectively).

¹²⁷ Schedule to the UNSCRIA, 2013.

¹²⁸ See Regulation 13 for the definition of sanctioned services.

¹²⁹ See Regulation 15 for the definition of sanctioned commercial activity.

¹³⁰ Generally that is as a person in respect of which countries must freeze immediately funds, or other financial assets and economic resources which are — in their territories, owned or controlled directly or indirectly by such designated entity, an entity acting on behalf of, or at the direction of an entity that has been designated, or an entity owned or controlled by such designated entity.

UN Security Council Resolutions Implementation (Reporting Entities)
Regulations, 2019

56A. Section 21 of the UNSCRIA allows for Regulations to be made for giving effect to the provision of this Act. Regulations under the UNSCRIA are subject to Affirmative Resolution. The United Nations Security Council Resolutions (Reporting Entities) Regulations were promulgated in November 2019. Under these Regulations, reporting entities include the financial institutions to which these Guidance Notes apply. These Regulations outline the operational procedures that must be maintained by financial institutions particularly when monitoring compliance with UNSEC resolutions and reporting on matters covered under the Act to the designated authority. These Regulations require that the obligations of reporting entities are without prejudice to their reporting requirements under the TPA (Reporting Entities) Regulations and allow for reliance on identification and verification procedures under the TPA and POC (MLP) Regulations in confirming and verifying the identity of customers. (See Regulations 4 and 5) These Regulations also prescribe the requisite Forms for reporting to the designated authority on whether or not they are in possession or control of any relevant assets pursuant to sections 3 and 5 of the Act.

Areas of Enforcement under UNSCRIA Implementation Act, 2013 further amended in 2019,
UNSCRI (DPRK Sanctions Regime) Regulations, 2021 and UNSCRI
(Reporting Entities) Regulations, 2019

Areas of Enforcement	Section of Act/Regs.	Responsible Authority	Additional Comments
Offences under the Act Failing to make a determination on a continuing basis whether there is possession or control of assets owned or controlled by or on behalf of a designated entity. (Sec. 5(2))	Sec. 5(7)	CTD of the FID/DPP	
Duty of entities to report (Sec 5(3))	Sec. 5	CTD of the FID	It is a defence that a person charged has a reasonable excuse for not making the report. (Section 5(8)). ‘Reasonable excuse’ is not defined in the legislation.
Failing to report whether or not there is possession or control of assets owned or controlled by or on behalf of a designated entity. (Sec. 5(3)(b))	Sec. 5(7)	CTD of the FID/DPP	
Failing to comply with a direction of the designated authority in making a report under section 5(3). (Sec. 5(4))	Sec. 5(7)	CTD of the FID/DPP	
Tipping off in relation to a report made under section 5(3). (Sec. 5(6))	Sec. 5(6)	CTD of the FID (to receive the report) DPP (to prosecute where an offence is committed)	
Injunction to prevent breach of an Implementing Regulation	Sec. 7	Attorney General	
Contravention of a UN sanction enforcement law.	Secs. 10 & 11	Relevant Authority (defined in para. 52) /DPP	An offence is not committed by body corporate if it proves that it took reasonable precautions, and exercised due diligence to avoid the contravention concerned. (S. 11(3))

Areas of Enforcement	Section of Act/Regs.	Responsible Authority	Additional Comments
			Compliance is monitored by the Relevant Authority under S.13 of the Act.
Monitoring compliance	Sec. 13	Relevant Authority	See paragraph 52 above for definition of ‘relevant authority’.
Attempting, conspiring, inciting, aiding, abetting, counselling or procuring the commission of any offence under secs. 10 or 11.	Secs. 10(3) A & 11(4)	Relevant Authority	Compliance is monitored by the Relevant Authority under S. 13 of the Act.
<i>Offences under the UNSCRI (DPRJK Sanctions RegimeRegulations)</i>			
Provision of /Procuring of a sanctioned service knowingly engaging in any sanctioned commercial activity	Regs. 14, 16 & 6	CTD of the FID Relevant Authority	Reports are done to the CTD of the FID under s.5 of the Act. Compliance is monitored by the Relevant Authority under s. 13 of the Act.
Knowingly using or dealing with freezable assets, allowing free-zable assets to be used or dealt with; facilitating any use of or dealing with freezable assets; knowingly directly or indirectly making a freezable asset available to a designated entity without Autorisation or as permitted by an Authorization	Reg. 18	Minister of MFAFT by	Applications would be done in relation to prohibitions contained in specific im-plementing Regulations issued under the Act. (See Regs. 34-36)
<i>Offences under the UNSCRI Reporting Entities Regulations</i>			
Reporting form	Sec. 5 of the Act & Reg. 6.	CTD of FID	
Noncompliance with Directions from Designated Authority	Reg. 8	CTD of FID	
Noncompliance with directions of the Competent Authority	Reg. 9	BOJ/FSC	This duty to comply with directions issued does not extend to information or advice that is subject to LPP. (Reg 9(3))

SECTION III — REGULATORY REQUIREMENTS

International Regulatory Requirements

57. The United Nations Convention against Transnational Organized Crime and the Protocols thereto, 2004 (Palermo Convention) established the following main obligations for member states of the United Nations:—
- (a) criminalization of participation in an organized criminal group;
 - (b) criminalization of the laundering of the proceeds of crime;
 - (c) measures to combat money laundering;
 - (d) criminalization of corruption;
 - (e) measures to address the liability of legal persons;
 - (f) legal framework that adequately addresses, among other things:—
 - (i) the prosecution and sanctioning of offences;
 - (ii) confiscation and seizure;
 - (iii) international cooperation for purposes of confiscation;
 - (iv) extradition; and
 - (v) mutual legal assistance.

Jamaica became a signatory to the U.N. Convention against Transnational Organized Crime and the Protocols thereto on September 26, 2001. On September 29, 2003, Jamaica ratified this Convention.

58. The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (Vienna Convention) established the following main obligations for member states of the United Nations:—
- (a) criminalization of the cultivation, production, sale, manufacture, transport or distribution of any narcotic drugs or psychotropic substances and the organization management or financing of any of these activities;
 - (b) criminalization of the conversion or transfer of property knowing that the property was derived from any of the abovementioned activities for the purpose of concealing or disguising the illicit origin of the property;
 - (c) criminalization of the concealment or disguise of the true nature, source, location, disposition, movement or ownership of property knowing that such property is derived from an offence or offences described at (a) or (b) above;
 - (d) criminalization of activities ancillary to the commission of the offences at (a) - (c) above;
 - (e) suppression of illicit traffic by sea in accordance with the international law of the sea;
 - (f) adequate measures to suppress the illicit traffic in narcotic drugs, psychotropic substances and other substances in free trade zones and in free ports
 - (g) adequate measures to suppress use of mail for the illicit traffic;
 - (h) legal framework that adequately addresses, among other things:—
 - (i) sanctions that adequately take into account the grave nature of the offences;
 - (ii) confiscation of the proceeds and instrumentalities of crime;
 - (iii) international cooperation for purposes of confiscation;
 - (iv) extradition;
 - (v) mutual legal assistance; and
 - (vi) other forms of cooperation.

Jamaica became a signatory to the U.N. Convention against Illicit Traffic in narcotic Drugs and Psychotropic Substances, 1988 on October 6, 1989. On December 29, 1995, Jamaica ratified this Convention.

59. The United Nations (U.N.) International Convention for the Suppression of the Financing of Terrorism 1999 established three main obligations for member states of the United Nations:—
- (a) States must establish the offence of the financing of terrorist acts in their national legislation;
 - (b) States must engage in wide-ranging cooperation with other states and provide them with legal assistance in the matters covered by the Convention; and
 - (c) States must enact certain requirements concerning the role of financial institutions in the detection and reporting of evidence of the financing of terrorist acts.

Jamaica became a signatory to the U.N. International Convention for the Suppression of the Financing of Terrorism 1999 on November 10, 2000. On September 16, 2005, Jamaica ratified this Convention.

60. U.N. Resolution 1373 (2001) on threats to international peace and security caused by terrorist acts, also mandates all member states of the United Nations to take action against individuals, groups, organizations and their assets.
61. As a consequence of the United Nation's characterization of acts of terrorism as threats to international peace and security, the United Nations is entitled to take, if necessary, the collective measures ("sanctions") under Chapter VII of the United Nations Charter.¹³¹ To this end the MFATF receives from time to time, an updated listing of individuals and entities which the UN has added to its consolidated list pertaining to Al-Qaida pursuant to United Nations Counter-Terrorism Security Council Resolution 1267 (1999) — Afghanistan. This listing is forwarded to the DPP for the purpose of being addressed pursuant to the listed entity regime. Licensees may, notwithstanding the foregoing, wish to apprise themselves directly from the United Nations web site and in that case may take note that the complete list and updates may be regularly accessed through the United Nations website. The discussion above, at paragraphs 50-56, is also relevant for this section on the International Regulatory Requirements.
62. The Jamaican authorities are also guided by—
 - (a) the (2012) revised Forty Recommendations of the FATF on the Detection and Prevention of Money Laundering, Terrorist Financing and Proliferation Financing.
 - (b) in October 2001, the Basel Committee on Banking Supervision issued Customer Due Diligence best practice standards ("CDD") as the minimum standards to be adopted by banking institutions in all countries. This document has been superseded by the Committee's publication of Sound Management of Risks Related to Money Laundering and Financing of Terrorism, issued in January 2014 and revised last in July 2020 and which can be accessed at the BIS website www.bis.org.

Other relevant publications published by Basel include—

 - (i) Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross Border Wire Transfers, May 2009; and
 - (ii) General Guide to Account Opening and Customer identification, February 2003 as last revised in Annex 4 of Sound Management and Risks mentioned above in 2016.
63. In conjunction with these Guidance Notes, financial institutions must be guided by the FATF standards, principles and recommendations in establishing policies, programs and procedures to prevent and detect money laundering and in combating the financing of terrorist activities as well as the prevention of the proliferation of weapons of mass destruction. The FATF Recommendations set out the internationally and regionally accepted principles relating to the appropriate measures to combat money-laundering, terrorist financing and the proliferation of weapons of mass destruction. The revised FATF Forty Recommendations can be accessed from both the FATF and CFATF¹³² websites at www.fatf-gafi.org and www.cfatf.org. Further guidance can also be obtained from the Best Practices issued by the FATE, which though not binding, outline very useful approaches to employ in addressing the international standards. Examples of some of the guidance issued by FATF and found on its website are listed below—
 - (a) Politically Exposed Persons, June 2013;
 - (b) Combating the Terrorist Financing Abuse of Non-Profit Organisations, June 2013, updated November 2023;
 - (c) Guidance for a Risk-based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services, June 2013;
 - (d) Financial Inclusion and Anti-money Laundering and Terrorist Financing Measures, November 2017, updated June 2025;
 - (e) The Implementation of Financial Provisions of UNSEC to Counter the Proliferation of Weapons of Mass Destruction, June 2013 updated February 2018;
 - (f) Guidance on Proliferation Financing Risk Assessment and Mitigation, June 2021;
 - (g) Targeted Financial Sanctions Related to Terrorism and Terrorist Financing, June 2013;
 - (h) National Money Laundering Terrorist Financing Risk Assessment, February 2013¹³³;
 - (i) Managing the AML/CFT Financing Policy Implications of Voluntary Tax Compliance Programmes, October 2012;
 - (j) Combatting the Abuse of Alternative Remittance Systems, June 2003;
 - (k) Risk-based Approach for Money Value Transfer Services, February 2016; and
 - (l) Correspondent Banking Services, October 2016;
 - (m) Beneficial Ownership and Transparency of Legal Arrangements, March 2024.

¹³¹ Suppressing the Financing of Terrorism — A Handbook for Legislative Drafting Chapter on U.N. Security Council Resolutions on Terrorism Financing — Page 15 — (Prepared by the IMF).

¹³² CFATF is a FATF Styled Regional Body (FSRJ3) comprising twenty-seven states of the Caribbean Basin and as of 2024 the United States of America is the 28th member, which have agreed to implement common countermeasures to address the problem of criminal money laundering. It was established as the result of meetings convened in Aruba in May 1990 and Jamaica in November 1992.

¹³³ See also: [Lessons Learned from the First Generation of Money Laundering and Terrorist Financing Risk Assessments](#) — World Bank Group 2023.

*Advisories and Public Statements issued in relation to certain Jurisdictions
(Specified Territories)*

64. Public statements are issued by the FATF in relation to jurisdictions which have been identified as *Jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or which have not committed to an action plan developed with the FATF to address the deficiencies*. These public statements either call on members to consider the risks arising from the deficiencies associated with these jurisdictions that are reflected as having strategic deficiencies or call on member states to apply counter measures to jurisdictions which have not settled an action plan and or who are deemed as not making sufficient effort or progress in addressing their AML/CFT deficiencies.
- These public statements are updated periodically and can be accessed from the FATF’s website.
65. Similar public statements are also issued by the CFATF for its members. These public statements are also updated periodically and can be accessed from the CFATF’s website.
- 65A. The United Nations (UN) imposes financial sanctions and requires member states to implement them through Resolutions passed by the UN Security Council. This information can be accessed from the UNSEC’s website.

Advisory by the Financial Stability Board

66. According to the Financial Stability Board (‘FSB’)¹³⁴, the publication of an advisory in relation to a jurisdiction comprises a negative measure that the FSB has agreed should be applied in relation to a jurisdiction that is considered to be a risk to the global financial system or which is non-compliant with international standards. An assessment of a jurisdiction’s levels of compliance with regulatory and supervisory standards relevant to international cooperation and information exchange is based on assessments of underlying ROSCs¹³⁵ (prepared by the IMF and World Bank) as well as signatory status to the multilateral MOU overseen by the International Organisation of Securities Commission.

*Statutes Which May Impact Financial Institutions Doing Business in the
United States of America (‘US’)*

67. Although not falling within the ambit of international best practice, financial institutions with correspondent banking relationships in the US must be aware of the relevant general Anti-Money Laundering Prohibitions to include any Executive Orders and must also be aware of the USA Patriot Act, as well as the Foreign Narcotics Designation Kingpin Act and Regulations. **Please note however that while these measures do not directly impose obligations under Jamaica’s domestic law**, these laws, prohibitions and/or orders directly impact the offer of correspondent banking services by US financial institutions and their holding of assets overseas.
- 67A. The U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) exercises regulatory functions under the statutory framework for AML. These provisions include authority, as delegated to the FinCEN Director, to impose “special measures” on domestic financial institutions and agencies to protect the U.S. financial system from foreign jurisdictions, financial institutions, classes of transactions, or types of accounts “of primary money laundering concern” (31 U.S.C. & 53 18A). The fifth “special measure” prohibits U.S. financial institutions and agencies from opening or maintaining correspondent or payable-through accounts associated with a foreign target of primary money laundering concern—a move that has been imposed in several instances to prevent misuse of the U.S. financial system, at least in part, for illicit drug-related financial activity¹³⁶.

USA Patriot Act

68. The “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (‘USA PATRIOT’) Act of 2001” — was passed by the US Congress in direct response to the September 11 terrorist attacks and became effective on 26 October 2001. This legislation has, among other things, expanded the money laundering laws of the US and has placed more stringent procedural requirements on financial institutions. Of specific importance to Jamaican financial institutions is the additional authority that has been vested in the US Secretary of the Treasury to regulate the activities of US financial institutions and in particular their relations with foreign individuals and entities. All banks and other financial institutions operating in Jamaica that have established correspondent accounts or any other business relationship with banks in the USA must therefore be aware of the provisions of this Act, including those highlighted below:—
- (a) provisions which permit the US Authorities to forfeit funds held by foreign banks in correspondent accounts held with banks situated in the US. (S. 319)¹³⁷;

¹³⁴ FSB members — Australia, Argentina, Brazil, Canada, China, France, Germany, Hong Kong SAR, India, Indonesia, Italy, Japan, Korea, Mexico, Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain, Switzerland, Turkey, United Kingdom, United States, IMF, The World Bank, Bank for International Settlements, European Central Bank, Organisation for Economic Cooperation and Development, ECB Banking Supervision, European Commission, Basel Committee on Banking Supervision, International Association of Insurance Supervisors, International Organisation of Securities Commissions, International Accounting Standards Boards, Committee on the Global Financial System, Committee on Payments and Market Infrastructures.

¹³⁵ Report on Observance of Standards and Codes.

¹³⁶ Taken from Paper — US Sanctions — Targeting International Illicit Drug Production and Trafficking — Congressional Research Service — INFOCUS — updated August 19, 2024.

¹³⁷ Reference taken from “Current Developments in Monetary and Financial Law — Cap 19 — pages 349-352.

- (b) provisions that will allow the US authorities to seize correspondent accounts held in US financial institutions for foreign banks which are in turn holding forfeitable assets (s. 317 and s. 319)¹³⁸;
- (c) provisions prohibiting US financial institutions from establishing, maintaining and administering or managing correspondent accounts with foreign banks that have no physical presence in any jurisdiction (i.e. shell banks), with certain limited exceptions; (s. 313)¹³⁹;
- (d) provisions requiring US financial institutions to take “reasonable steps” to ensure that accounts for foreign financial institutions are not used to indirectly provide banking services to shell banks; (s. 313)¹⁴⁰;
- (e) provisions which grant the Treasury and the US Attorney General power to issue a subpoena or summons to any foreign financial institutions with a correspondent account in the US and to request records relating to the account. A financial institution that has a correspondent account for a foreign financial institution must maintain certain delineated records in the US relating to that foreign financial institution (s. 319 (b))¹⁴¹; and
- (f) provisions which grant the Treasury and the US Attorney General power to direct a financial institution to terminate its relationship with a foreign correspondent financial institution that has failed to comply with a subpoena or summons. The directive must be by written notice and non-complying financial institutions are subject to civil penalties of up to US\$10,000 per day (s. 319 (b))¹⁴².

Foreign Narcotics Kingpin Designation Act¹⁴³

69. Also known as the “Kingpin Act” its purpose is to deny significant foreign narcotics traffickers, their related businesses, and their operatives’ access to the U.S. financial system ,and to prohibit all trade and transactions between the traffickers and U.S. companies and individuals. The Kingpin Act authorizes the President to take these actions when he determines that a foreign person plays a significant role in international narcotics trafficking.

Congress modelled the Kingpin Act on the effective sanctions program that the Department of the Treasury’s Office of Foreign Assets Control¹⁴⁴ (‘OFAC’) administers against the Colombian drug cartels pursuant to Executive Order 12978 issued in October 1995 (“Executive Order 12978”) under authority of the International Emergency Economic Powers Act (“IEEPA”).

Under the Kingpin Act, the President may identify foreign entities as well as foreign individuals as Significant Foreign Narcotics Traffickers, or “kingpins”: A foreign person is defined in the Act as “any citizen or national of a foreign state or any entity not organized under the laws of the United States, but does not include a foreign state.” Likewise, the President is not required to designate Colombian persons exclusively under Executive Order 12978, and may impose sanctions on a Colombian individual or entity under the Kingpin Act, which is intended to be global in scope.

Individuals who violate the Kingpin Act are subject to criminal penalties of up to 10 years in prison and/or fines pursuant to Title 18 of the U.S. Code. Entities that violate the Act face criminal penalties in the form of fines up to \$10 million; officers, directors, or agents of an entity who knowingly participate in any violation of the Kingpin Act are subject to criminal penalties of up to 30 years imprisonment and/or a \$5 million fine. The Kingpin Act also provides for civil penalties of up to \$1.075 million against individuals or entities that violate its provisions.’

US Executive Orders¹⁴⁵

Iran Freedom and Counter Proliferation Act (IFCA), 2012

70. On June 3, 2013, the President of the USA issued Executive Order 13645¹⁴⁶ (“Authorizing the Implementation of Certain Sanctions Set Forth in the Iran Freedom and Counter-Proliferation Act of 2012 and Additional Sanctions With Respect to Iran”) (“E.O. 13645”). Section 2 of E.O. 13645 blocks, with certain exceptions, all property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person, including any foreign branch, of persons determined by the Secretary of the Treasury, in consultation with the Secretary of State, to satisfy any of the criteria set forth in subsection (a)(i) or (a)(ii) of section 2.¹⁴⁷

¹³⁸ Reference taken from “Current Developments in Monetary and Financial Law - Cap 19 - pages 349-352.

¹³⁹ Ibid

¹⁴⁰ Ibid

¹⁴¹ Ibid

¹⁴² Reference taken from “Current Developments in Monetary and Financial Law — Cap 19 — pages 349-352.

¹⁴³ This update on the Foreign Narcotics Kingpin Designation Act is taken from White House Press Release, Office of the Press Secretary April 15, 2009 — Fact Sheet: Overview of the Foreign Narcotics Kingpin Designation Act.

¹⁴⁴ OFAC administers and enforces economic and trade sanctions based on US foreign policy and US national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific (US) legislation, to impose controls on transactions and freeze foreign assets under US jurisdiction” (Source - <http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx>).

¹⁴⁵ Central Bank advisories on these Executive Orders were issued to financial institutions in July and August 2013.

¹⁴⁶ This Order took effect on July 1, 2013.

¹⁴⁷ Federal Register, The Daily Journal of the United States Government, <https://www.federalregister.gov/articles/2014/09/05/2014-21169/actions-taken-pursuant-to-executive-order-13645> as at 28/8/15.

International Emergency Economic Powers Act (IEEPA), 2007

71. US Executive Order 13581 of July 24, 2011 was issued by the President of the USA to create the designation of persons pursuant to the International Emergency Economic Powers Act (IEEPA) (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*) (NEA), and section 301 of title 3, United States Code, AND in respect of which additional designations were made on June 5, 2013.
- The Order authorizes the blocking of all property and interests that are in the USA, that subsequently come within the USA or that are or subsequently within the possession or control of any US person including any overseas branch of the persons listed in the Annex to the captioned order, and the persons determined by the Secretary of the Treasury to be a person to whom the Order applies (see targeted persons below) and further, that such property and interests may not be transferred, paid, exported, withdrawn or otherwise dealt in.
72. The Order accordingly targets—
- (a) Any foreign person that constitutes a significant transnational criminal organization (TCO);
 - (b) Any person who has materially assisted, sponsored, or provided financial, material or technological support for, or goods or services to or in support of, any person whose property and interests in property are blocked pursuant to this Executive Order; and
 - (c) Any person who is owned or controlled by, or who has acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this Executive Order.
73. For the purposes of this Order, the term “foreign person” means any citizen or national of a foreign state, or any entity organized under the laws of a foreign state or existing in a foreign state, including any such individual or entity who is also a US person; and the term “significant transnational criminal organization” means a group of persons, that includes one or more foreign persons which engages in an ongoing pattern of serious criminal activity involving the jurisdictions of at least two foreign states; and that threatens the national security, foreign policy or economy of the US.

US Economic Sanctions Programmes

74. OFAC administers a number of different sanctions programmes. The sanctions can be either comprehensive or selective, **using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals¹⁴⁸**.
- As of September 2025, OFAC has in place sanction programs involving at least 20 nations, including Cuba, Crimea, Iran, Iraq, Lebanon, South Sudan, and Zimbabwe.
- (a) *Specially Designated Nationals (SDN) and Blocked Persons*
- OFAC has identified and officially “designated” numerous foreign agents and front organizations, as well as terrorists, terrorist organizations, and narcotics traffickers, on its SDN list, which contains over 5,000 variations on names of individuals, governmental entities, companies, and merchant vessels located around the world.
- All U.S. persons (including individuals and organizations) are responsible for ensuring that they do not undertake a business dealing with an individual or entity on the SDN list. U.S. persons are:
- (i) All U.S. citizens and permanent residents;
 - (ii) All persons located in the United States;
 - (iii) Overseas branches of U.S. companies; and
 - (iv) In the case of the Cuba and North Korea programs, non-U.S. subsidiaries of U.S. companies.
- A complete list of individuals and entities designated can be found at: OFAC Specially Designated Nationals List — Sanctions List Service
- (b) *Penalties for Noncompliance*
- The only way to ensure compliance with OFAC-administered sanctions is to develop a process for regularly checking customers/clients against the SDN list described above. OFAC violations have serious consequences. Persons not complying with OFAC-administered sanctions are liable for significant penalties, even if their action was inadvertent or uninformed.¹⁴⁹ Penalties include:
- (i) Civil penalties¹⁵⁰: \$250,000 or twice the amount of each underlying transaction up to \$ 1,075,000 per violation;

¹⁴⁸ Sanctions Programs and Country Information / Office of Foreign Assets Control as at 12/09/25.

¹⁴⁹ Notable actions of OFAC involving Banks: — USD16.562 million Settlement Agreement with BOA for apparent violations of the Foreign Narcotics Kingpin Sanctions Regulations, 31 C.F.R. Section 598; the Narcotics Trafficking Sanctions Regulations, 31 C.F.R. Section 536 (24/07/2014); and the Reporting, Procedures and Penalties Regulations, 31 C.F.R. Section 501; USD 152 million agreement with Clearstream Banking, S.A. (Luxembourg) regarding an apparent violation of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. Section 560 (23/01/2014).

¹⁵⁰ Civil Penalties and Enforcement Information | Office of Foreign Assets Control gives a list of civil penalties and enforcement actions to date.

- (ii) Criminal penalties: \$50,000 to \$10,000,000 fine; 10-30 years in prison; and
- (iii) Publication of penalty: OFAC publishes the names of companies that have been penalized.

Domestic Regulatory Requirements

75. The domestic legal requirements outlined above at Section II of these Guidance Notes highlight legislation and other guidance developed for the purpose of preventing and detecting money laundering,¹⁵¹ terrorist financing¹⁵² activities; and the proliferation of weapons of mass destruction activities which must be adhered to, established and implemented by financial institutions.

Bank of Jamaica’s Specified Territories Supervisory Authority Notice, 2022¹⁵³

- 75A. Pursuant to section 94 of the POCA, on the 2nd of May, 2023, the Bank in its capacity as Supervisor issued *the Bank of Jamaica’s Specified Territories Supervisory Authority Notice, 2022*. This Notice applies to all entities regulated by the Bank. (See Appendix VII)
- 75B. By virtue of this notice financial institutions are required to apply enhanced due diligence measures¹⁵⁴; ensure that the background and purpose of relevant transactions are examined and the findings documented and available to the competent authority upon request, for natural and legal persons of countries specified by FATF.
- 75C. Financial institutions are also required to apply countermeasures for any business or transaction with a customer domiciled in a specified territory by FATF or as otherwise identified by the Supervisory Authority whether spontaneously as a risk mitigation measure or in response to international obligations.
- 75D. Financial institutions in complying with these Notices should ensure that they exercise care not to disrupt the flow of donations to and by non-profit organisations in territories included in these Notices.
- 75E. Financial institutions are reminded that in applying ML/TF/PF risk-based measures particular care must be taken to avoid the unintended consequence of unduly restricting legitimate financial activity by non-profit organizations (NPOs), including the receipt and disbursement of donations. FIs are expected to implement proportionate countermeasures that address identified risks, while ensuring that such actions do not unreasonably impede the lawful operations of NPOs operating within or engaging with jurisdictions subject to these Notices¹⁵⁵.

The Data Protection Act

75F. The Data Protection Act, 2020 (“the DPA”) which first came into effect on December 1, 2021¹⁵⁶, applies to financial institutions in their collection, storage, handling of, sharing and overall processing of personal data¹⁵⁷. Financial institutions are required to act in compliance with all relevant laws and guidelines to include the legal obligations related to personal data processing as outlined in the DPA. In responding to supervisory requests for information that would extend to personal as opposed to organisational data, a financial institution should be mindful of the legal exemptions applicable to a Supervisor’s request for personal data information as contained in Part V.

Part V titled — *exemptions to data protection standards or to disclosure to data subject requirements*, exempts personal data requests which amongst other things cover statutory functions (section 34), regulatory activity (section 35) and research purposes (section 37).

National Identification System (NIDS¹⁵⁸)

- 75G Under the POC (ML) Regulations, 2007 last amended in 2019, and the TP (Reporting Entities) Regulations, 2010 (last amended 2019), FIs are required to identify their customers and to verify these identities, undertake regular reviews of customer information, including retrospective reviews of all existing customers’ records. The NIDS implemented by the Government of Jamaica is a system intended to establish reliable national identification and identification authentication mechanisms for all Jamaican citizens and residents who opt to be registered in the National Identification Database (NID). The enrolment of the individuals will be done using information from existing Government issued identification as well as biometrics and other information pertaining to these individuals that will be included in the database and which information will then permit the generation of a national identification number (NIN) and national identification card (NIC). Enrolment of an individual also involves storing identity related information collected from enrolled individuals and verifying the authenticity of identifications generated by the NID framework for persons seeking to transact business with enrolled individuals, as well as to generate and issue NINs and NICs. The overall goal is to strengthen identity verification for citizens and residents who opt to be enrolled in this database and authentication of such identification in our jurisdiction.
- 75H. In April 2024 the National Identification and Registration Act fully came into force. Section 17 of this Act states that an enrolled individual who is issued a national identification card (NIC) may use the card as a means of proving that

¹⁵¹ See POCA (MLP) Regulations, 2007 (r. 5)

¹⁵² See TPA section 18

¹⁵³ Can be found at: BANK-OF-JAMAICA-SPECIFIED-TERRITORIES-SUPERVISORY-AUTHORITY-NOTICE.pdf

¹⁵⁴ As defined in Regulation 7A(5) of the POC (MLP) Regulations.

¹⁵⁵ Discussed further in Part V below.

¹⁵⁶ Per appointed day Notice of November 30, 2021 sections 2, 4, 56, 57, 60, 66, 74, 77 and the First Schedule came into effect on December 1, 2021. Since then other sections of the DPA and its Regulations have come into force.

¹⁵⁷ Section 2 defines both the words process and personal data. Personal data is defined as information (however stored) relating to a living individual or an individual who has been deceased for less than 30 years who can be identified from that information alone or from that information and other information in the possession of, or likely to come into the possession of, the data controller and includes any expression of opinion about that individual and any indication of the intentions of the data controller or any other person in respect of that individual.

¹⁵⁸ Reference is made to BOJ’s Letter to all commercial banks, merchant banks and building societies titled “Bank of Jamaica’s expectations for onboarding, ongoing know your customer and ongoing customer due diligence requirements leveraging the national identification system’ dated October 7, 2022.

person’s identity and where it is furnished to an individual requiring proof of the person’s identity it shall be accepted as sufficient proof of same and the person shall not be required to provide any additional proof of identity. As such, FIs may leverage the services offered by the National Identification and Registration Authority (NIRA) to verify an individual’s identification. Specifically, for customers or prospective customers of FIs enrolled in the NID and issued a NIC the references in Part V to identification measures required for KYC will not be mandatory for:

- (i) face to face onboarding of customers with NICs; or
- (ii) non-face-to-face onboarding of customers with NICs once verification with the NIRA has been satisfactorily established digitally¹⁵⁹.

Summary

76. In summary, financial institutions are expected to demonstrate full awareness of:—
- (a) the nature of the money-laundering and terrorist financing threats, and the nature of threats of the proliferation of weapons of mass destruction;
 - (b) the local laws relating to combating money-laundering, terrorist financing and the proliferation of weapons of mass destruction, and the potential liability of institutions and employees for failure to comply with these obligations; these Guidance Notes as well as related international standards and related best practices;
 - (c) the obligations to ensure the implementation of the requisite systems and processes for customer and ultimate beneficial ownership identification and verification, enhanced due diligence procedures, including special procedures for non-face to face transactions, electronic funds transfers transactions; high risk customers, ‘Politically Exposed Persons’ (PEPs), and transactions with overseas counterparts;
 - (d) the requisite systems for the recording and reporting of unusual and suspicious transactions and transactions that exceed the statutory thresholds; including the role of the nominated officer;
 - (e) the requisite programmes for ensuring employee integrity and awareness through effective screening and due diligence prior to hiring and continued relevant training post hiring, and continued screening of employees post hiring (viz. job performance; adherence to internal policies and procedures including codes of conduct and AML/CFT requirements as well as the general integrity of employees); and
 - (f) the obligations to ensure the implementation of the requisite systems and processes to ensure compliance with the specified territories’ notices.

SECTION IV — RISKED-BASED FRAMEWORK

77. Under the revised FATF Forty (40) Recommendations, 2012¹⁶⁰, countries are required to identify, understand and assess, the money laundering, terrorist financing and proliferation financing risks posed to the country. Countries must ensure that their national AML/CFT/CPF policies are informed by the risks identified through the national risk assessment. This national risk assessment will therefore inform the overall national AML/CFT/CPF strategy and framework for a country and the implementation of appropriate risk-based measures for the relevant sectors within the country. The revised recommendations also indicate that the resulting national risk-based approach employed by a country shall not exempt financial institutions, Designated Non-Financial Businesses and Professions (‘DNFBPs’), persons, institutions and entities from the requirement to apply enhanced measures when higher risk scenarios have been identified by these persons.

All financial institutions are required to implement an appropriate ML/TF/PF risk assessment framework. As stated in the foreword, these Guidance Notes set out the minimum expectations regarding the ML/TF/PF risk assessment process and is expected to lead to improvements in financial crime risk management through the identification, assessment and monitoring of the risks faced by financial institutions.

78. A financial institution shall identify, assess and take effective action to mitigate its money laundering and terrorist financing risks in relation to)—
- (a) customers, beneficial owners and other counterparties; parties (i.e. persons other than customers with whom FIs conduct business);
 - (b) countries or geographic areas;
 - (c) products;
 - (d) services;
 - (e) Complexity, type, volume and size of transactions;
 - (f) delivery channels, including outsourced arrangements; and
 - (g) operating environment (business (size, activities and complexities); sector; national frameworks and national and global issues).

¹⁵⁹ Where the conditions above are not satisfied, paragraph x will still apply.

¹⁶⁰ FATF Recommendation 1 and Interpretive Note to Recommendation 1.

- (h)—
- i. the nature of the money-laundering and terrorist financing threats, and the nature of threats of the proliferation of weapons of mass destruction;
 - ii. the local laws relating to combating money-laundering, terrorist financing and the proliferation of weapons of mass destruction, and the potential liability of institutions and employees for failure to comply with these obligations; these Guidance Notes as well as related international standards and related best practices;
 - iii. the obligations to ensure the implementation of the requisite systems for customer and ultimate beneficial ownership identification and verification, including special procedures for non-face to face transactions, electronic funds transfers transactions; high risk customers, ‘Politically Exposed Persons’ (PEPs), and transactions with overseas counterparts;
 - iv. the requisite systems for the recording and reporting of unusual and suspicious transactions and transactions that exceed the statutory thresholds; including the role of the nominated officer; and
 - v. the requisite programmes for ensuring employee integrity and awareness through effective screening and due diligence prior to hiring and continued relevant training post hiring, and continued screening of employees post hiring (viz. job performance; adherence to internal policies and procedures including codes of conduct and AML/CFT/CPF requirements as well as the general integrity of employees).

Failure to identify the risks itemized in this paragraph will constitute a breach of the BOJ’s AML/CFT Supervisory Rules.

78A. The risk assessment methodology, the process for identifying and evaluating factors, scoring criteria and weights, should be clearly documented in the financial institution’s policies and procedures. The documented methodology should allow third parties (Internal Audit, External Audit, Competent Authority), to test the design and operational effectiveness of the risk assessment.

Failure to comply with this requirement will constitute a breach of the BOJ’s AML/CFT Supervisory Rules.

79. The AML/CFT/CPF risk assessment shall be:—
- (a) maintained through ongoing and periodic reviews to understand changes in ML/TF/PF risk factors. The risk assessment must be documented (i.e. “be in writing”) and must be submitted within 30 days following Board approval to the Competent Authority every three years or more frequently as the Competent Authority may require for specific entities;
 - (b) undertaken so that there is a clear identification, determination and understanding of the risks involved;
 - (c) based on practical, comprehensive and up-to-date understanding of threats;
 - (d) inclusive of commensurate measures that are clearly defined and applied; and
 - (e) as earlier indicated, approved by the Board or other body (by whatever name called) of the regulated business (which include FIs) responsible for the governance and oversight of the regulated business, and made available to officers and employees or staff where commensurate with respective functions, to allow for the identified measures to be applied and monitoring to be undertaken.
80. Assessments shall be informed by a country’s latest national risk assessment and other assessments available from the national authorities and agencies in relation to any sector; as well as peer review assessments (such as mutual evaluation reports) and financial sector assessments (FSAP reports). However, the absence of a national risk assessment does not absolve a financial institution from undertaking its own assessment of the risks posed to its operations as reflected at paragraphs 78, 78A and 79.
- Failure to comply with any one or more of the requirements in paragraphs 79 and 80 will constitute a breach of the BOJ’s AML/CFT Supervisory Rules.
81. In undertaking its enterprise risk assessment, and where higher risks are identified, countermeasures should be applied where applicable, i.e. where a higher risk scenario is identified, a financial institution, shall apply enhanced measures to address such higher risks. A failure to apply enhanced measures is an offence under the AML/CFT legislation¹⁶¹. Assessment procedures which are not robust enough to reasonably allow for a high risk of ML/TF or PF to be identified will constitute a breach of the BOJ’s AML/CFT Supervisory Rules.
82. A financial institution shall note that regardless of the level of risks involved, there is no exemption from recordkeeping requirements.

¹⁶¹ See 2019 Amendment to POCA s94A (3).

83. The BOJ's examination processes will continue to include an assessment of the adequacy of a financial institution's AML/CFT/CPF policies and systems, the institution's compliance with these policies and systems as well as the applicable legislation and these Guidance Notes. The AML/CFT/CPF oversight of financial institutions under the BSA by the BOJ is undertaken through a specialized unit of the Supervisory Division which is tasked specifically with the BOJ's AML/CFT/CPF oversight functions¹⁶². The objective of this approach is to:—
- (a) assist with better understanding each financial institution's ML/TF/PF risks;
 - (b) allow for a more targeted assessment of the adequacy and appropriateness of an institution's own risk assessments and AML/CFT/CPF policies and procedures; and
 - (c) facilitate the collection of data that will facilitate the BOJ's broader participation in the country's risk-based assessment.
84. Financial institutions must be aware that as competent authority under the AML/CFT/CPF legislation, the BOJ can have independent interaction with the designated authority or an authority of equivalent jurisdiction (whether local or foreign), regarding an institution's compliance with its obligations under the applicable legislation. A financial institution's breach of its obligations under the applicable legislation can, in addition to the imposition of sanctions, also be reported to the designated authority. (See paragraph 15 above on competent authority).
85. For financial groups under the BSA, it is anticipated that the mandates at paragraphs 78, 78A and 79, will be addressed through the group risk management initiatives that are contemplated by the consolidated supervisory provisions under the BSA¹⁶³. A failure therefore to comply with these mandates may be considered a failure to manage group risks and may result in the BOJ taking regulatory action, under the BSA in addition to the sanctions that will be applicable under the AML/CFT/CPF Supervisory Rules.
86. Where financial institutions under the BSA are required to provide information pursuant to parent company or holding company obligations to consolidate AML/CFT/CPF compliance initiatives, this can be done pursuant to paragraph (n) of the Ninth Schedule to that Act.

Branches and Subsidiaries

87. Financial institutions are required to advise their branches/subsidiaries (resident in Jamaica or overseas)¹⁶⁴ of the provisions of the Jamaican AML/CFT/CPF laws together with the provisions of any applicable Guidance Notes insofar as the dealings of such subsidiaries or branches are affected. Branches are not considered to be legally distinct from their head office and therefore are subject to Jamaican laws.
88. Each financial institution is therefore required to assess the AML/CFT/CPF regime existing in any jurisdiction in which its branches and/or subsidiaries operate to ensure that its respective branches and subsidiaries apply the requirements of the Jamaican law. An exception is where the overseas operation is required to comply with the AML/CFT/CPF laws in that jurisdiction and those requirements meet or exceed Jamaican law. Where the AML/CFT/CPF requirements in that jurisdiction fall short of the Jamaican requirements¹⁶⁵ the financial institution shall ensure that appropriate additional measures to manage the ML/TF/FP risks are developed, documented, implemented and communicated to the BOJ.
89. Overseas based subsidiaries and foreign branches of local financial institutions *must* inform their local parent companies and local head offices if they are not in a position to observe AML/CFT/CPF measures of the local parent company or head office where compliance therewith will contravene the laws of the overseas jurisdiction/(s) in which these subsidiaries and branches reside. In such circumstances the local head office/parent company *must* accordingly advise BOJ¹⁶⁶ of the inability, the reasons, and the measures to minimise the money laundering/terrorist financing/proliferation financing risks that are developed, documented and implemented. BOJ will then make a determination on the adequacy of the measures applied and any other or further required course of action which may also include closure of the relevant overseas subsidiary or branch.
90. A financial institution regulated by the BOJ shall ensure that its local subsidiaries engaged in financial services implement, and conform to obligations under the POCA under the TPA, under the UNSCRIA and regulations issued thereunder as well as these Guidance Notes. A failure to ensure compliance with these requirements enunciated in paragraphs 89 and 90 will constitute a breach of the BOJ's AML/CFT/CPF Supervisory Rules. For financial institutions under the BSA this may also be considered to be a failure of the statutory obligation to manage group risks pursuant to the consolidated supervisory provisions under the BSA and could result in the BOJ taking other regulatory action.
91. In complying with the mandates at paragraphs 78, 78A and 79 a financial institution shall in relation to its subsidiaries and branches, ensure—
- (a) the KYC details for customers are well documented and stored (i.e. identification and other customer information as defined under the POC (MLP) Regulations, 2007 as amended), submitted and recorded;

¹⁶² The decision to use this approach was taken in March 2015, an industry advisory was issued in April 2015.

¹⁶³ See Section XIV of the BSA.

¹⁶⁴ See Regulation 18, POC (MLP) Regulations, 2007 further amended in 2019 and Regulation 18 of the TP (Reporting Entities) Regulations, 2010 further amended in 2019.

¹⁶⁵ See Regulation 18 of the POC (MLP) Regulations and FATF Recommendation 18.

¹⁶⁶ See Regulation 18(2) of the POC (MLP) Regulations, 2007 as amended in 2019; and Regulation 18(2) of the TP (Reporting Entities) Regulations, 2010 as amended in 2019.

source of wealth, where appropriate, based on the risk profile, is obtained as a part of the financial history of the customer, as well as transaction details (including nature of the transaction, transaction amount; currency used; method of payment (cheque/cash/credit card/debit card/wire transfer/digital currency) and source of funds used to make the payment) are recorded;

- (b) AML/CFT/CPF internal regulatory controls (i.e. employee training; designation of a nominated officer; auditing of internal controls etc.) are documented (where applicable) and implemented;
- (c) required disclosures (i.e. STRs) are made and any other reporting obligations are met;
- (d) in relation to branch and subsidiary operations in Jamaica, measures that track cash transactions are to be implemented to prevent anonymity in relation to financing of transactions and source of funds. Additionally, financial institutions who are “permitted persons” as defined under POCA will need to invoke appropriate measures to ensure that where cash transactions over one million Jamaican dollars (or the equivalent amount in any other currency) are facilitated, this does not itself facilitate a breach of the cash transaction limit provisions under POCA;
- (e) AML/CFT/CPF risk-based measures are employed within the parameters of the AML/CFT/CPF laws.

A failure to comply with any one or more of these requirements under this paragraph will constitute a breach of the BOJ’s AML/CFT/CPF Supervisory Rules.

91A. The risk assessment undertaken by FIs should also consider, in relation to its operations and persons with whom or through whom business is conducted—

- (a) the nature of the money-laundering and terrorist financing threats, and the nature of threats of the proliferation of weapons of mass destruction;
- (b) the local laws relating to combating money-laundering, terrorist financing and the proliferation of weapons of mass destruction, and the potential liability of institutions and employees for failure to comply with these obligations; these Guidance Notes as well as related international standards and related best practices;
- (c) the obligations to ensure the implementation of the requisite systems for customer and ultimate beneficial ownership identification and verification, including special procedures for non-face to face transactions, electronic funds transfers transactions; high risk customers, ‘Politically Exposed Persons’ (PEPs), and transactions with overseas counterparts;
- (d) the requisite systems for the recording and reporting of unusual and suspicious transactions and transactions that exceed the statutory thresholds; including the role of the nominated employee (officer); and
- (e) the requisite programmes for ensuring employee integrity and awareness through effective screening and due diligence prior to hiring and continued relevant training post hiring, and continued screening of employees post hiring (viz. job performance; adherence to internal policies and procedures including codes of conduct and AML/CFT requirements as well as the general integrity of employees).

Non-Financial Subsidiaries

92. Financial institutions under the BSA are subject to mandates on the type of subsidiaries that can be held and must therefore always be in a position to prove to the BOJ that the operations and activities of their subsidiaries (especially where these are non-financial) are relevant and complementary to the licensee¹⁶⁷ and do not pose a financial drain or a money laundering, terrorist financing or proliferation financing risk to the licensee.

The kind of AML/CFT/CPF processes implemented in relation to these types of subsidiaries must, for practicality, amount to measures designed to address the ML/TF/PF risks posed by these subsidiaries to their parent financial institutions and other members of the financial group.

93. Financial institutions that have local subsidiaries which are themselves subject to AML/CFT/CPF and other guidance from authorities other than the BOJ (whether regulatory or otherwise) shall assess the AML/CFT/CPF guidance against which their subsidiaries operate and shall ensure that those subsidiaries apply the higher required standard.¹⁶⁸

Gatekeepers/Designated Non-Financial Businesses and Professions (DNFBPs) Affiliates and other parties

94. According to FATF, persons falling within the definition of ‘Designated Non-Financial Businesses and Professions (DNFBPs) includes *inter alia* lawyers¹⁶⁹, notaries, other independent professionals and accountants; dealers in precious metals and stones (jewellers); trust and corporate service providers; casinos; and real estate agents) (See FATF Recommendation 22 and the Interpretative Notes thereto). The FATF Recommendations also state that (in the situations outlined in the recommendations) such persons shall be subject to the following:—

- (a) implementation of AML/CFT/CPF regulatory controls (policies and procedures including training of employees and audits of AML/CFT/CPF controls (FATF Recommendation 18);

¹⁶⁷ Section 73(2) BSA.

¹⁶⁸ Regulation 18 of the POCA (MLP) Regulations, 2007 as amended in 2019; and Regulation 18 of the TP (Reporting Entities) Regulations, 2010 as amended in 2019; See also FATF Recommendation 22.

¹⁶⁹ In February 2023, the UK Privy Council in *The AG v JAMBAR; the GLC v JAMBAR* [2023] UKPC 6, ruled that the imposition of a duty on Attorneys-at-Law to report to the relevant authority, suspicious activities relating to clients, is not unconstitutional.

- (b) the customer due diligence and record-keeping requirements set out in recommendations 10 (customer due diligence), 11 (record keeping), 12 (politically exposed persons), 15 (new technologies) and 17 (reliance on third parties);
- (c) suspicious transaction reporting (STR) requirements (FATF Recommendation 20) and as such entitled to protection from any liability from such disclosures made, and, prohibited from disclosing the fact of the STR or related information being reported to the designated authority (FATF Recommendation 21); and
- (d) requirements for other measures such as internal controls and foreign branches and subsidiaries obligations (R18); and obligations regarding higher risk countries (R19).

Financial institutions must therefore take the matters set out in this paragraph and paragraph 95 into consideration when establishing, or in the course of reviewing an existing relationship with a DNFBP.

95. The POCA is applicable to businesses in the regulated sector. A business is in the regulated sector if it is a financial institution or an entity that has corporate responsibility for the development and implementation of group wide anti-money laundering or terrorism prevention, policies and procedures for the group of companies of which the entity forms apart; or if it is a designated non-financial institution (‘DNFI’)¹⁷⁰.

A DNFI means “...a person who is—

- (i) not primarily engaged in carrying on a financial business; and
- (ii) designated as a non-financial institution for the purposes of this Act by the Minister by order subject to affirmative resolution.”

A DNFI is therefore subject to the statutory AML provisions that are applicable to financial institutions.

96. In November 2013, the following persons were designated by the Minister of National Security as DNFI’s — real estate dealers, casinos, gaming machine operators, lawyers, notaries, other independent legal professionals and accountants, in relation to the activities specified in the designation orders¹⁷¹.

In November 2017, real estate dealers, casinos, gaming machine operators, were designated as reporting entities under the Terrorism Prevention Act. The designation took effect in May 2018. Subsequently in February 2019, Attorneys were similarly designated under the TPA.

In December 2021, Trust and Corporate Service Providers were designated by the Minister of National Security as a DNFI under the POCA.

(Refer to Appendix III for copies of the requisite Designation Orders).

- (a) The designated competent authorities¹⁷² for these persons are—
 - The Real Estate Board (re: Real Estate Dealers);
 - The Betting Gaming and Lotteries Commission (re: Gaming Operators);
 - The Casino Commission (re: Casinos);
 - The General Legal Council (re: Attorneys);
 - The Public Accountancy Board (re: Accountants); and
 - The Financial Services Commission (re: Trust and Corporate Service Providers)

(Refer to paragraph 15 above on Competent Authority.)

97. It must also be noted, where the DNFI makes a disclosure pursuant to its statutory obligations under the POCA, that disclosure liability must not be interpreted as a breach of information restraints to which that DNFI may have been subject. Accordingly, section 100 states that—

- (a) once the information or matter comes to a person in the course of that person’s trade, profession, business or employment; and
- (b) that information or matter raises the belief or knowledge that another person has engaged in money laundering; and
- (c) the disclosure of the information or matter is made to an authorized officer (i.e. a constable; a customs officer; or an officer of the Asset Recovery Agency) or a nominated officer.

such disclosures shall not amount to a breach of any restriction on the disclosure of information by whatever means imposed.

¹⁷⁰ Refer POCA, 2007 Fourth Schedule as amended and section 94 of the POCA amended in 2013.
¹⁷¹ The Proceeds of Crime (Designated Non-Financial Institution) (Real Estate Dealers) Order, 2013; (effective April 2014).
The Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order, 2013; (effective April 2014).
The Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order, 2013; (effective June 2014).
The Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order, 2013; (effective April 2014).
The Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013; (effective April 2014).
¹⁷² Designation took effect November 29, 2013.

SECTION V — “KNOW YOUR CUSTOMER” (KYC), “KNOW THE TRANSACTION COUNTERPARTY” AND CUSTOMER DUE DILIGENCE (CDD)

Interpretation

98. For the purpose of this section of the Guidance Notes, the terms used in this section will have the meaning set out in this paragraph.

“affiliate/affiliated”	has the meaning assigned in section 2 of the Companies Act;
“charity/charities”	means charitable organization as defined in section 2 of the Charities Act, 2013. For the purpose of these Guidance Notes the term ‘charity’ includes a non-profit organization (NPO);
“connected Party”	has the meaning assigned in the Banking Services Act;
“current”	in relation to information means information which is valid in substance, and accurate in respect of all [material] details and particulars;
“customer name”	means, (a) in the case of a natural person, the official name recorded at birth or recorded in the records of the Deputy Keeper of the Records and verified by sight of the official identification document as described in paragraph 121 below¹⁷³; (b) in the case of a legal person, the name in which the business is incorporated or established, and verified by sight of the certificate of incorporation or certificate of Registration of Business Name (whichever is applicable);
“known employer”	includes:— (a) in the case of a business, one that is registered on the Jamaica Stock Exchange; a microcredit service provider, a person who is required to be registered with a government body or agency or statutory body in order to operate and is so registered; (b) a financial institution as defined in these Guidance Notes; (c) a financial institution which is registered with or licensed by the Financial Services Commission; or (d) an employer within the public sector. Public sector for the purposes of these Guidance Notes means the Central Government or a public body¹⁷⁴ as defined in the Financial Administration and Audit Act;
“on-profit organization”	see ‘charity’ above;
“outdated information”	refers to information other than current information and accordingly includes:— (a) expired identification, (i.e. identification where the validity of the identification has ended or has expired); (b) in relation to the name of a customer, a change of name of the customer, subsequent to the date when the customer commenced the business relationship with the financial institution or since the date the last transaction was conducted with the financial institution (whether or not the transaction was conducted at the same branch location); (c) in relation to a customer’s residential address (in the case of a natural person) or registered address (in the case of a legal person), the physical address at which the customer no longer physically resides or is no longer physically situated; and (d) in relation to financial and other information regarding the personal, business or official affairs of the customer, (i) (for financial information) the date at which the information represented has expired for at least 18 months; or (ii) information in respect of which an intervening event has occurred after the information is provided to the financial institution and which event makes the information provided, unreliable or unhelpful for the institution to undertake customer due diligence and risk profile analyses or to maintain the status quo as ‘knowing its customer’;

¹⁷³ See also paragraphs 75G & H above on NIDS.

¹⁷⁴ “public body” means a statutory body or authority or any government company; (section 2 — the Financial Administration and Audit Act).

“ongoing measure”	means, in relation to a customer or in relation to a business counterpart, a measure that must be applied by a financial institution for the duration of the business relationship with the customer or counterpart;
“personal or private information”	means, in relation to:— (a) a natural person, customer information as defined in regulation 7(5) of the POC (MLP) Regulations as amended in 2019, and includes personal data as defined under section 2 of <i>The Data Protection Act, 2020</i>, and (b) a legal person, the information set out in regulation 13(1)(c) of the POC (MLP) Regulations and at regulation 13(1)(c) of the TP (Reporting Entities) Regulations;
“records”	includes records pertaining to identification, transactions, business correspondence, accounts files, instructions, determinations and bases for allowing or not proceeding with a transaction; account reviews and findings, transaction reviews and findings, requests for updated CDD information and related updates provided, accessed or ascertained);
“repeat customer”	means, a person who transacts business of US\$250 and over or the equivalent amount in any other currency more than once with the financial institution or any of its branches; and applies to transactions conducted within a three-month period with subsidiaries of financial institutions or other parties to the financial institution or affiliates where the circumstances or the risk profile of the transacting customer warrants this to be done;
“senior manager”	for the purposes of this section of the Guidance Notes, in relation to— (i) a body corporate, means an executive director, a managing director, a chief executive officer, a chief financial officer, the nominated officer, a manager, a senior officer and the company secretary or such other person by whatever name called, who undertakes duties or has responsibilities akin to these positions; (ii) any other legal arrangement, includes an individual whose function, by whatever title used, involves functioning as an executive director, a managing director, a chief executive officer, a chief financial officer, a nominated officer, a manager or a company secretary or such other function by whatever name called which is akin or equivalent to these functions;
“significant transaction”	means a transaction undertaken by a financial institution in respect of a customer, which varies in the nature of business usually undertaken or substantially in value and/or in amount of business conducted or number of transactions normally undertaken by that customer or in relation to the account/(s) involved. For instance, (a) an account ordinarily involving low value JMD transactions suddenly being used for mid-to-high value transactions in JMD or foreign currency; (b) a relationship that is normally related to banking activities for a corporate customer is used to finance or cover personal expenses or conduct personal banking activities; (c) or deposit and withdrawal activities consistent with a standard personal savings account becomes more consistent with those indicative of flows generated from and/or expenses associated with commercial activity.
“source of funds”	Source of funds refers to the origin of the particular funds or instrument that is relied on or used for a transaction and can therefore also be derived from a customer’s wealth. Examples of source of funds are: (i) Bank account; (ii) Proceeds from the sale of an asset, for example, car, property etc.; (iii) Proceeds from investment pay-outs; (iv) Proceeds from pension releases.
“source of wealth”	Source of wealth refers to the origin of the assets the customer has and which may be the source of the funds used for a transaction. <i>Source of wealth is therefore that information set that allows for a determination of net worth. Examples of source of wealth are:</i> (i) Self-employment;

- (ii) employment with the public or private sector;
- (iii) inheritance;
- (iv) royalties;
- (v) investment portfolio;
- (vi) winnings from games of chance;
- (vii) successful pay-out from a lawsuit;

“ultimate beneficial owner” has the meaning assigned in Regulation 2 of the POC (ML) Regulations, as amended in 2019.

General Requirements for Know Your Customer (“KYC”) & Customer Due Diligence (“CDD”)¹⁷⁵

99. ‘Knowing your customer’ is the status of being reasonably satisfied the customer is who he says he is by identifying the customer. Verification of a customer’s identity is therefore the process which allows an FI to be reasonably satisfied of the identity of the customer.
100. The requirement to conduct customer due diligence includes identifying the customer and verifying that customer’s identity (i.e. KYC), as well as satisfactorily establishing details pertaining to the customers’ occupation, economic activity (including an understanding of the purpose and intended nature of the business relationship), personal and financial information sufficient to allow for a risk profile of the customer, transaction or relationship (as applicable) to be generated¹⁷⁶; personal financial track record, business track record, contact information and details, capacity in which the business is being transacted, details of representation or relationship if business is being transacted on behalf of another, rationale and authorities established to act for persons benefiting from the transaction or relationship with the financial institution, regulatory status (i.e. compliance record with statutory and operational obligations), personal compliance with laws (i.e. character and integrity).

In the case of customers which are legal persons or established by some other form of legal arrangement, identification of the customer includes identification of the beneficial owner/(s) and verifying that identification¹⁷⁷ as well as identification of the senior managers/senior officers or other person exercising control¹⁷⁸. The customer due diligence that is conducted must be designed to allow a financial institution to understand who its customers are by requiring the gathering of information on what the customer does and why that customer requires the services requested of the financial institution¹⁷⁹. Where the customer is a legal person or established by legal arrangement the due diligence undertaken shall include understanding both the ownership and control structure of that customer as well as the information articulated above at paragraph 104¹⁸⁰.

Reference is made to the table below which illustrates at a glance the main obligations and distinctions between KYC and CDD:

KYC	Satisfactory identification of the customer
	(a) Applies to all customers and transacting counterparties
	(b) One-off requirement i.e. must be met—
	i. At the start of the relationship
	ii. At on-boarding of customers
	iii. Must be updated every 7 years
	(c) Rules based obligation i.e. see b(i) and (ii) above
CDD	ID information + due diligence (see para 103 below)
	Applies to all customers and transacting counterparties
	Goes beyond identification of individual, legal person and legal arrangement, intermediate and ultimate beneficial owner.

¹⁷⁵ See POCA (MLP) Regulations, 2007 as amended in 2019 (r. 7, 11, 12, 13); TP (Reporting Entities) Regulations, 2010 (r. 7, 11, 12, 13) amended in 2019; and FATF Recommendations R.10.

¹⁷⁶ Information required to generate the required risk profile should include source of funds and source of wealth as deemed applicable in the circumstance. See further discussions below.

¹⁷⁷ FATF Recommendation 10 (CDD measures to be taken), Regulations 7, 7A, 11 and 13 of the POC (MLP) Regulations as amended in 2019

¹⁷⁸ Reference Regulation 13 of the POC (MLP) Regulations as amended in 2019.

¹⁷⁹ FATF Risk-based Approach Guidance for the Banking Sector, October 2014- Section III B — Risk Mitigation.

¹⁸⁰ FATF Recommendation 10 (CDD measures to be taken).

Obligation is ongoing as information must remain current, adequate and accurate

Risk based obligation (as needed, based on risk and/change in risk profile)

Policies and Procedures FOR KYC AND CDD

101. Central to an effective AML/CFT/CPF programme is the formulation and implementation of comprehensive, rigorous and thorough KYC and customer due diligence (CDD) policies and procedures.

KYC and CDD policies and procedures must contain a clear statement of management’s overall expectations and establish specific lines of responsibilities not only at the point of the institution’s first contact with the customer, but throughout the business relationship, including continuous identification, assessments and verification of the customer when initiating, reviewing and approving a product or delivery channel (debit card, online banking, point of sale terminal, etc.) for that customer. Policies and procedures must be properly documented, form a part of training content, and clearly communicated and readily available to staff.

KYC and CDD policies and procedures shall not only be geared toward the timely prevention and detection of money laundering, terrorism financing and proliferation financing activities but must also form a fundamental part of the financial institution’s overall risk management and internal control systems. This is essential, as inadequate KYC and CDD standards can result in undue risk exposures, particularly as they relate to ML/TF/PF, reputational, operational and legal risks.

102. Policies and procedures must therefore be developed on the basis of the financial institution’s ML/TF/PF risk assessments) and must therefore be reflective of¹⁸¹:—
- (a) the financial institution’s understanding of the ML/TF/PF risks present in its customer base, delivery channels, products and services offered and under development before these are launched, as well as the jurisdictions within which the FI and its customers do business. An understanding of the ML/TF risks is also required in relation to activities undertaken by the financial institution including promotional sponsorships, philanthropic/benevolent initiatives and sovereign based arrangements (contracts with sovereign);
 - (b) the financial institution’s understanding of risks present in its general operations, which could impact or increase its exposure to a ML, TF or PF related offence taking place, for example, risks associated with product usage; transaction patterns, group of accounts or a particular category of customers; inadequate internal control mechanisms, weak hiring policies, absence of appropriate and periodic AML/CFT/CPF training for the board, management and staff; weak communication policies, absence of clear reporting lines and responsibilities within the financial institution; weak disciplinary mechanisms (in terms of sanctions and/or appropriate remedial measures/mechanisms); lack of access to timely information, poor records management practices and weak records management and retention policies; absence of robust escalation of matters to the Board’s attention; ineffective compliance functions;
 - (c) threats and vulnerabilities that have been identified which have a probability of occurring and the impact such occurrences could have on the financial institution’s operations and reputation;
 - (d) customer and transaction acceptance requirements which shall be informed by an assessment of the types of customers that are likely to pose a risk of ML or TF or lower risk of ML or TF. Accordingly, while basic due diligence is applicable to all customers and transacting counterparties, policies and procedures must clearly reflect the due diligence that will be applicable for relationships or transactions that are subject to assessments of risks determined to be low, medium, or high;
 - (e) circumstances in which transactions can be started or business relationships established prior to verification of the CDD or KYC information;¹⁸²
 - (f) circumstances under which transactions or relationships can, should or must be terminated or discontinued, circumstances under which relationships will not be established and transactions will not be conducted or facilitated;
 - (g) bases on which risk profiles for customers, products, delivery channels or services offered can be revised and the procedure for such revision. In this regard financial institutions must develop graduated “know your customer” and CDD policies and procedures for high-risk customers that go beyond the basic information-gathering requirements for clients rated as average or low risk clients. This must include a detailed description of the types of customers that are likely to pose a higher than average risk to a financial institution based on assessment of certain factors including, customers’ background, country of origin, important public or high-profile position/(s) held, linked accounts, business activities or other risk indicators; and

¹⁸¹ Reference: Basel Committee on Banking Supervision Sound Management of Risks Related to Money Laundering and Financing of Terrorism — January 2014 rev July 2020.

¹⁸² Regulation 13(2) of the POC (MLP) Regulations, 2007; Regulation 13(2) of the TP (Reporting Entities) Regulations, 2010.

- (h) measures designed to allow for the identification of high-risk customers and transactions that breach the proliferation of weapons of mass destruction obligations as outlined in the UNSCRIA and regulations thereunder.

103. Accordingly, the minimum, KYC and CDD policies and procedures must address:—

- (a) the establishment of a robust customer identification programme which includes the following:
 - i. the identification of the customer and in the case of customers who are legal persons or legal arrangements, the identification of the interim and ultimate beneficial owners or beneficiaries and senior officers thereof as discussed above;
 - ii. verification of the customer’s identification information and, in keeping with the risk-based approach, obtain and verify all relevant information necessary to establish a comprehensive risk profile. This includes verifying the customer’s identity, ascertaining the nature and purpose of the customer’s business activities, and understanding the intended purpose and nature of the business relationship. Institutions must also determine whether the customer is acting on their own behalf or on behalf of another party. Where the customer requires the financial service for commercial or official purposes, sufficient details of the associated business or organization must be obtained. These measures collectively enable the institution to assess whether transactions align with the expected risk profile and to effectively identify unusual, suspicious, or inconsistent activity.
- (b) the recording and regular review of customer information (identification and other information) as well as transaction information or records to ensure that the information kept by the financial institution is current and comprehensive, as well as the retention of such information for a minimum of seven (7) years after the transaction has been completed, or the business relationship has been terminated, whichever occurs later. Under the POC (MLP) Regulations, financial institutions are required to ensure that customer information is kept under review with a view to ensuring its accuracy and is updated at least once every seven (7) years or, at more frequent intervals as warranted by the risk profile of the relationship. If therefore during the course of the business relationship an institution’s records reflect that the customer’s information is outdated, the institution shall update that information at the earliest opportunity as the CDD process is an ongoing measure¹⁸³. The requirement to keep information current and comprehensive and under review essentially, has a built-in requirement for retroactive due diligence (RDD) to ensure these obligations are met and continue to be met on an ongoing basis by the financial institution. In this regard it must be noted that in relation to RDD and matters pre-dating March 29, 2007, the 2013 amendments to the POC (MLP) Regulations state that a financial institution is not required to obtain information or evidence in respect of any transaction conducted prior to March 29, 2007, (regulation 19), RDD however remains a requirement for all accounts opened subsequent to March 29, 2007;
- (c) the regular reviews of customer (identification, transaction and other) information include undertaking a retrospective review of all pre-existing accounts for customers to ensure that up-to date or current full customer identification and other details are on the file for accounts established after March 29, 2007¹⁸⁴;
- (d) the ongoing application of CDD which takes account of the level of risk posed to the financial institution by transacting business with the particular customer; (i.e. individuals opening standard savings accounts obviously funded primarily by salary; pension payments etc. vis-a-vis corporate accounts opened via pooled arrangements involving multiple parties or accounts for customers.);
- (e) measures clearly reflecting the procedures required for accounts for high-risk customers to include the fact that accounts for high-risk customers must not be opened unless senior management approval is obtained¹⁸⁵;
- (f) mechanisms designed to ensure that there are adequate management information systems to provide timely and comprehensive management reports to facilitate effective monitoring of high-risk client accounts by senior management;
- (g) measures to deal with special areas of operations or operational complexities (e.g. financial institutions which have established operations (via branches and subsidiaries) in more than one jurisdiction; or financial institutions within a financial group which offers a wide range of financial products and services; or financial institutions with a very diverse customer base).

¹⁸³ Regulation 71(c) of the POC (MLP) Regulations. Where customer information is not updated in contravention of this section, the business relationship shall not proceed any further and the FJ shall make all the required disclosures pursuant to section 94 of POCA (i.e. disclosures as to transactions which could constitute or be related to ML). Regulation 71(d) as amended in 2019.

¹⁸⁴ Note that Regulation 19 of the POC (MLP) Regulations reflects that financial institutions are not required to obtain information or evidence in respect of any transaction conducted prior to the relevant date (which is March 29, 2007).

¹⁸⁵ Whilst the term Senior Manager in these Guidance Notes includes a Nominated Officer, a Nominated Officer is ineligible as a Senior Manager who can extend such approvals as such a function is to be sufficiently independent of the business line of the institution to allow for an objective assessment, monitoring, and enforcement of the institution’s compliance with its AML/CFT/CPF obligations (legislative; as well as policies and procedures). (See also Part VI of these Guidance Notes).

104. A failure to carry out CDD in relation to a business relationship, when commencing a relationship or onboarding a customer is an offence under the POC and TP legislation. **Additionally, failing to comply with any one or more of the requirements in paragraph 103 will constitute a breach of the BOJ’s AML/CFT/CPF Supervisory Rules.**
105. Policies and procedures must be approved by the Board of Directors (or other body by whatever name called) of the financial institution. Noncompliance with this requirement will constitute a breach of the BOJ’s AML/CFT/CPF Supervisory Rules.
106. For licensees under the BSA, MCA, BOJA, and for credit unions, it is expected that CDD procedures will also be applied on a consolidated and global basis where applicable. This requires *inter alia*, the capacity to aggregate and monitor significant balances and transactions for the under-mentioned customers:
- (a) Customers with multiple accounts/transactions at the financial institution — either within a particular branch or among several branches situated locally and within a foreign jurisdiction; and
 - (b) Customers with multiple accounts/transactions at several entities within the financial group. (This is required whether the accounts are held on balance sheet or off-balance sheet as assets under management,¹⁸⁶ or on a fiduciary basis).
107. Vulnerability is not limited to transactions with customers. Any transaction undertaken by the financial institution can expose that institution to ML/TF/PF, reputational, operational, legal and/or concentration risk. As far as is reasonably practical and possible, financial institutions shall apply the KYC and CDD policies and procedures to **all financial transactions undertaken, whether customer related or not**. For these purposes, non-customer related transactions include:—
- (a) transactions conducted by the financial institution on its own behalf or on behalf of another financial institution; and
 - (b) in-house operational matters (back office activities, proprietary securities acquisitions or dispositions; correspondent (local and overseas) relationships; housekeeping matters; administrative matters and so forth).

BANKS, MERCHANT BANKS, BUILDING SOCIETIES, CREDIT UNIONS, MICROCREDIT INSTITUTIONS,
CAMBIOS AND REMITTANCE COMPANIES

General Requirements for Know Your Customer (“KYC”) & Customer Due Diligence (“CDD”)¹⁸⁷

108. Financial institutions are required to establish the identity of an applicant for business (i.e. a customer, for the purpose of these Guidance Notes) as soon as is practicable, but no later than 14 days after contact is first made. This obligation exists whether it is a one-off transaction or an ongoing business relationship. Where the financial institution is unable to verify the customer’s identity within the 14 days, the following obligations come into effect:
- (a) Risk management measures are to be applied to the conditions under which the transaction or business relationship is proceeding while the verification process of the customer’s identity is being carried out. (Regulation 7(1) POC(MLP) Regulations).
 - (b) Where the financial institution has reasonable grounds to suspect that a business relationship or one-off transaction constitutes or could be related to ML and is of the belief that carrying out the full required CDD measures might alert the person that such a suspicion has been formed, then the regulated business should act as follows:
 - (i) Discontinue the CDD procedures, however document on the file the reasons for suspension of CDD procedures;
 - (ii) Make the required disclosure (STR) under section 94 or 95 of the POCA or section 16(3) of the TPA;
 - (iii) Ensure that in discontinuing the CDD procedures, enough information is collected to adequately identify the applicant for business so that a valid STR may be submitted to the FID. (Regulation 7(4A) POC(MLP) Regulations)
 - (c) Where a financial institution is not satisfied with the outcome of its CDD inquiries, but there are no reasonable grounds to suspect that the business relationship or one-off transaction constitutes or could be related to ML, then:
 - (i) The business relationship or one-off transaction shall not proceed any further, unless conducted with the permission of, and in accordance with guidelines issued by, the BOJ; and

¹⁸⁶ Reference herein to assets under management is only to the extent that deposit taking institutions have their own assets under proprietary management. Otherwise, asset management on behalf of customers is not an activity that can legally be undertaken by deposit-taking institutions. See also BSA section 54.

¹⁸⁷ See POCA (MLP) Regulations, 2007 as amended in 2019 (r. 7,11, 12, 13); See TP (Reporting Entities) Regulations, 2010 (r. 7, 11, 12, 13) as amended in 2019; and FATF Recommendations R.10 181.

- (ii) The financial institution shall make an assessment as to whether any disclosure is required under section 94 or 95 of the POCA; that is, a suspicious transaction report (“STR”); (Regulation 7(4B) POC(MLP) Regulations).

Where an applicant for business refuses to produce any requested information, the relationship or transaction must not proceed. Where an existing customer unreasonably refuses to provide the information requested by the financial institution pursuant to CDD or KYC requirements, or if any other verification problems arise which cannot be resolved, the business relationship with that customer shall be legally terminated (unless otherwise advised by law enforcement authorities)¹⁸⁸.

109. In seeking to—

- (a) discontinue the procedures for establishing a business relationship or for the transaction started or attempted; or
- (b) terminate the business relationship, financial institutions must be mindful of the prohibition against tipping off or unauthorised disclosures outlined under sections 97 and 104 of the POCA and section 17 of the TPA and section 5(6) of the UNSCRIA, and must therefore be careful not to “tip off” applicants for business, customers, or any other person where a suspicion has been formed by the financial institution that an offence is being attempted or has been or is being committed¹⁸⁹.

110. A financial institution shall ensure that it has the ability to legally terminate arrangements, transactions or the business relationship where it forms the view that criminal activity is taking place and that continuing the arrangement, transaction or relationship could lead to legal, operational, reputational or other risks to the institution due to the suspected criminal activity.

A financial institution must therefore ensure that its mandates with customers and indeed contractual arrangements entered into in the course of the regulated business permit the legal termination of the arrangement, transaction, or business relationship in the event it forms the view that criminal activity is taking place and to continue with the arrangement, transaction or relationship would expose the institution to legal or reputational risks due to the suspected criminal activity.

Prior to the termination of a business relationship, where there is suspicion that the funds in an account may constitute criminal property, a financial institution should file the requisite STR and *must* seek appropriate written consent from the Designated Authority before returning such funds to the customer.

- 111. Financial institutions shall undertake periodic risk-based reviews¹⁹⁰ (including retrospective reviews) of all existing customers’ records (identification & other particulars) to ensure that they remain up-to-date, relevant, consistent with the financial institution’s risk profile of that customer, and remain subject to appropriate know your customer and customer due diligence processes. The review of customer identification information shall be done at least seven (7) years from the date of the commencement of the relationship and at minimum seven years increments thereafter, or, at more frequent intervals as warranted by the risk profile of the relationship, to ensure the accuracy of the information held by the institution (refer also to paragraphs 103(c) and (d) above); however CDD is an ongoing obligation and should be updated as warranted by the risk profile of the relationship or of the customer or circumstances.
- 112. The financial institution shall communicate to the customer, his/her/its obligation to notify the financial institution of any change in the customer’s identification information or changes in other particulars whether personal or private information or otherwise which would render the information with the financial institution to be outdated or no longer accurate.
- 113. Reviews¹⁹¹ shall also be necessary under the following circumstances:—

- (a) Upon the execution (or attempted execution) of a significant transaction¹⁹²;
- (b) Upon material changes to customer documentation standards;
- (c) When there is material change in the manner in which the account is operated;
- (d) When, during the course of the business relationship, doubt arises regarding the true identity of the customer or the beneficial owner of the account;
- (e) When there is any change in the ownership or control of a corporate customer, or of a customer established through a legal arrangement;

¹⁸⁸ See footnote 35 above NCB v Olint Corp Ltd - Privy Council Appeal No. 61 of 2008 [2009] UKPC 16. Per Lord Hoffman at paragraph 1.

¹⁸⁹ *Shah v HSBC Private Bank (UK) Ltd. (No. 2) [2012] EWHC J283(QB)*, the ruling confirms that to ensure distance from the zone of ‘tipping-off’, a money laundering reporting officer should stay clear of any dialogue, with the customer, about the fact that a report was made under POCA to the requisite statutory body. This appears to be the current legal position as it remains to be challenged in the Court of Appeal.

¹⁹⁰ POCA (MLP) Regulations, 2007 as amended in 2019 — r. 7(1)(c) & (d) and r. 19; TP (Reporting Entities) Regulations, 2010 (r. 5 as amended in 2019 and 21).

¹⁹¹ POCA (MLP) Regulations, 2007 as amended — r 7(1)(c), r. 7(2)(b) and 7(3); and TP (Reporting Entities) Regulations, 2010 — Regulations 5 as amended in 2019 and 6(2)(b)J.

¹⁹² For the avoidance of doubt, a “significant transaction” is not limited to a specific monetary threshold but is determined by its potential to present heightened ML/TF risk, its inconsistency with the customer’s known financial behaviour, or its association with other risk indicators such as geographic, sectoral, or transactional red flags, as outlined in POCA and the TPA, and guided by the FI’s internal risk assessment framework.

- (f) Where the financial institution becomes aware at any time that it lacks sufficient information about an existing customer/or about the existing business relationship with a customer;

(g) Where any transaction involves/exceeds the prescribed amount and represents a significant transaction or a material change in the manner in which the account is operated¹⁹³;

(h) Where transactions earned out in a single operation or in several operations appear to be linked;

(i) Where a transaction is carried out by means of wire transfers;

(j) Where there is any doubt about the veracity or adequacy of previously obtained evidence of identity;

(k) Where the financial institution is required to make a report under section 94 (STR) or 95 (STR by the nominated officer) of the POCA, or under section 16(3) or (3A) of the TPA (STR by the nominated officer — TP (Reporting Entities) Regulations, regulation 15)¹⁹⁴.
114. If during the course of the updating exercise or any time after the business relationship has commenced the financial institution discovers that the information on file is not accurate, or is no longer applicable and the correct or updated information is not available or is, in the view of the financial institution, unreasonably withheld, then the financial institution must take steps to terminate the relationship¹⁹⁵ and consider referring the matter to the designated authority. The financial institution shall conduct the necessary analysis and review of the account to inform its consideration of whether the matter must be referred to the designated authority¹⁹⁶ and records of the conduct and results of this exercise shall be in writing and available on request, to the competent authority, and the designated authority and provided within the time indicated in the request¹⁹⁷, and shall also be available to the auditors (internal and external) where applicable, of that institution.

Specific Guidance — KYC and CDD for Central Bank Digital Currency (CBDC)

- 114A. As Jamaica advances the adoption of its Central Banlc Digital Currency (CBDC), JAM-DBX, financial institutions (FIs), particularly deposit-taking institutions (DTIs), must align their Know Your Customer (KYC) and Customer Due Diligence (CDD) frameworks to incorporate CBDC-related activities, including the use of digital wallets by clients. This integration must be proportionate, risk-based, and consistent with Jamaica’s legislative framework under the POCA and its Regulations, the TPA and its Regulations and UNSCRIA and its Regulations, and the Bank of Jamaica’s AML/CFT/CPF supervisory expectations outlined through guidance.
- 114B. FIs must treat client-owned CBDC wallets similarly to conventional account relationships, ensuring KYC and CDD is applied based on the nature of the wallet tier, transaction limits, and associated risk exposure. For example:

• Low-value, basic wallets with strict transaction and balance limits may qualify for simplified CDD, consistent with FATF Recommendation 10 and Jamaica’s National Risk Assessment (NRA) outcomes for low-risk, financial inclusion products.

• Higher-value, unrestricted wallets or those linked to complex or international transactions must be subject to full CDD, including identity verification, beneficial ownership checks, and, where applicable, source of funds/wealth assessments.
- 114C. Where a customer holds both traditional banking products and a CBDC wallet with the same institution, FIs must ensure a consolidated risk profile. All wallet transactions should be monitored in conjunction with the customer’s broader account activity to identify unusual patterns, layering attempts, or misuse for ML/TF/PF purposes.

Systems should be designed to prevent fragmentation of customer information, maintaining consistency on customer risk assessments and ongoing due diligence.
- 114D. FIs must integrate CBDC wallet activity into existing transaction monitoring systems, applying thresholds, triggers, and typology-based detection in line with STR reporting obligations under the POCA and TPA.

Wallet transactions that demonstrate structuring, use of proxies, or cross-border elements inconsistent with customer profiles should prompt enhanced scrutiny and, where appropriate, regulatory reporting.
- 114E. Given JAM-DEX’s design for potential cross-institution use, FIs must establish interoperability agreements and data-sharing protocols, ensuring that KYC/CDD standards remain consistent even when wallets interface with external entities.

Supervisory oversight will emphasize that wallet-to-wallet transfers within the CBDC ecosystem do not create regulatory blind spots with FIs responsible for ensuring traceability, record-keeping, and customer identity validation.
- 114F. Where FIs offer services to customers using third-party-issued CBDC wallets, they must implement appropriate reliance frameworks, ensuring those providers meet equivalent AML/CFT/CPF standards as set by the BOJ.

¹⁹³ POCA speaks to the following prescribed amounts — a TTR limit for cash transactions (see Regulation 3 of the POC (MLP) Regulations and cash transaction limits (see POCA section I01A). No amounts are prescribed under the TPA or Regulations thereunder.

¹⁹⁴ Financial institutions should be guided by their respective statutory AML/CFT/CPF obligations and where the circumstances call for this, the transaction should either not be conducted or consideration be given to terminating the relationship.

¹⁹⁵ POC (MLP) Regulations, 2007 as amended in 2019 Regulation 7(1)(b) & TP (Reporting Entities) Regulations, 2010. Regulation 5(a)(iii).

¹⁹⁶ POC (MLP) Regulations, 2007 as amended in 2019 Regulation 7(1)(b).

¹⁹⁷ Regulation 14(4) of the POC Regulations amended 2019 (MB. Regulation 14 of the TP (Reporting Entities) Regulations speaks to the record keeping obligation of reporting entities).

This reflects FATF guidance on third-party reliance (Recommendation 17) and is critical to preserving the integrity of the financial system.

- 114G. Supervisory expectations emphasize that integration of CBDCs into KYC/CDD frameworks should not impose disproportionate barriers, particularly for underserved or financially excluded populations. Consistent with FATF’s Financial Inclusion Guidance, simplified CDD for basic-use wallets is encouraged, provided that cumulative risks remain low and proper limits are enforced¹⁹⁸.
- 114H. FIs must update internal policies, staff training programs, and technological systems to reflect CBDC — specific KYC/CDD processes. Records of wallet ownership, transaction history, and CDD measures must be maintained in accordance with BOJ record-keeping requirements and made available for regulatory inspection.

Unclaimed Moneys¹⁹⁹

115. If the circumstances described above occur in the case of accounts that would qualify as unclaimed monies then, subject to any contrary directives from the designated authority pursuant to the appropriate consent requirements, on closure of the account, the funds contained therein shall be subject to the usual course of action governing unclaimed moneys²⁰⁰.

Other Accounts

116. If the circumstances described above occur in the case of accounts that would not qualify as unclaimed monies, then, subject to any contrary directives from the designated authority pursuant to the appropriate consent requirements, on closure of these accounts the funds contained therein shall be returned to the named account holders.

Updating KYC and CDD Records

117. The law requires that customer information be updated at a frequency of at least once every seven (7) years²⁰¹ from the date of the commencement of the relationship and at minimum seven-year increments thereafter, or, at more frequent intervals to ensure the accuracy of the information held by the institution or as warranted by the risk profile of the relationship.

Where gaps are discovered in the customer information database²⁰² financial institutions must ensure that these gaps are addressed at the earliest opportunity and not at the end of a seven-year period from the last update. Updates in this regard include matters involving—

- (a) addressing omissions in the database of customer information particulars that are required under the law or AML/CFT/CPF regulatory framework (particularly where this occurs in relation to customers that are identified or classified as ‘high risk’);
- (b) addressing incomplete information. (If for instance the customer provided an alias or trading name other than the customer name as defined in these Guidance Notes, then the information on the institution’s database shall be treated as incomplete and the customer name must be obtained and verified);
- (c) adjusting records to reflect changes to the customer information particulars such as, name change by marriage or deed poll; changes in the current permanent address; changes in employment/business trade and/or profession; financial institutions shall ensure that the records reflect the appropriate updates in this regard (i.e. current information)²⁰³; and
- (d) correcting errors or addressing inaccuracies.

The KYC and CDD processes should ideally be implemented in a manner designed to minimize the disruption of business. Accordingly, the requirements need not be ‘sprung’ on existing customers. Such persons may for instance be provided advance notification of the information required and given a reasonable timeframe within which to provide the information. For example, in the case of existing customers wishing to do new business with the bank, this would be an appropriate time to seek to ensure KYC and CDD updates and shortfalls are addressed.

References

118. Pursuant to letter dated November 3, 2023 the Bank in relevant part indicated that “effective immediately, the requirement for references, as outlined in Section 118 of the Guidance Notes on the Prevention of Money Laundering and Countering the Financing of Terrorism, Proliferation and Managing Related Risks (“Guidance Notes”), will no longer be mandatory.” This remains the position of the Bank.

¹⁹⁸ See Section below on Financial Inclusion.

¹⁹⁹ Section 126 BSA. The concept of unclaimed balances is not applicable to credit unions and building societies.

²⁰⁰ For licensees under the BSA see section 126.

²⁰¹ POC (MLP) Regulations as amended in 2019, Regulation 7(1)(c) & (d) & 19.

²⁰² The law indicates there is no obligation for such reviews to be done in relation to matters which pre-date the prescribed date of 29th day of March, 2007 (Regulation 19(3) — POC (MLP) Regulations amended 2013).

²⁰³ Please be reminded that in the case of IDs, the information contained therein may be useful for identifying the customer as who he/she says he/she is but is not mandatory for CDD.

Expired Identifications

118A. The Bank of Jamaica expects institutions to treat expired identification documents as **supplementary information** only, never sufficient on their own to establish or re-establish a customer’s identity. Institutions are expected to address the presence of expired IDs as part of their retrospective due diligence reviews (outlined above at paragraph 117), ensuring that customer records are accurate, current, and risk-appropriate.

1. *Requirement for Valid Identification at Onboarding*

At the point of establishing a new business relationship or conducting an initial one-off transaction, financial institutions must obtain at least one valid (unexpired) government-issued photo identification (e.g., passport, driver’s licence, voter’s identification card, or NIDS credential), or an equivalently reliable and authoritative form of digital identification. Where such valid identification cannot be produced, the transaction or relationship shall not proceed and the FI should act in accordance with Regulation 7 of the POC (MLP) Regulations.

2. *Treatment of Expired Identification Documents in Ongoing Relationships*

Where an existing customer seeks to transact using an expired identification document, financial institutions may only proceed where all of the following conditions are satisfied:

- The expired ID is paired with at least one corroborating independent source of identification (e.g., TRN, birth certificate, or authoritative registry check);
- The institution verifies the authenticity and security features of the expired ID; and
- The individual presenting is matched face-to-face or digitally against the photograph on the expired ID.

Time Limitation on Reliance:

Reliance on expired IDs under these conditions shall be permitted for a period of no greater than three (3) months from the date of expiry. During this period, financial institutions must:

- o Encourage and facilitate customers in obtaining valid, up-to-date IDs;
- o Apply risk-based safeguards (enhanced monitoring, thresholds, or temporary limits); and
- o Ensure that business relationships do not continue indefinitely on the basis of expired IDs, regardless of the customer’s risk classification.

At the end of the 3-month period, the institution must obtain a valid, unexpired ID (or an authoritative digital equivalent). If the customer fails to provide such ID, the relationship shall not proceed further.

3. *Risk-Based Application*

Low and Medium-Risk Relationships: Expired IDs may be relied upon only with corroboration from an independent source. Institutions must document the rationale, the corroborative source used, and any risk-mitigation measures applied.

High-Risk Relationships: At least one valid (unexpired) government-issued or authoritative digital ID is mandatory. Expired IDs cannot be accepted as the primary identification in such cases.

4. *Risk Mitigation Measures*

Where expired IDs are accepted in permitted low or medium-risk cases, institutions must:

- Apply enhanced monitoring and, where appropriate, transaction thresholds;
- Document and justify reliance on expired ID, including the corroborative evidence used; and
- Require the customer to provide an updated valid ID within a reasonable timeframe.

Natural Persons

119. Financial institutions must be aware that the best identification documents for natural persons are those that are the most difficult to obtain illicitly. Positive identification must be obtained from documents issued by reputable sources²⁰⁴, which include anyone of the following:

- (a) identification under the National Identification System (NIDS) (i.e., number, card) (reference para 75F above);
- (b) valid driver’s licence (bearing a photograph), issued by the authorities in the country in which the person is resident”;
- (c) current valid passport;

²⁰⁴ See Basel Committee on Banking Supervision — Sound management of risks related to money laundering and financing of terrorism, January 2014 rev. July 2020 paragraph 37.

- (d) current valid voter’s identification card;
 - (e) signed (known) employer identity card or valid worker’s identification from a known employer, bearing a photograph and signature of the employee in question and bearing the authorized signature on behalf of the employer;
 - (f) any other government issued ID bearing the photo and signature of the person.
- 120. In cases where the identification described at paragraph 119 above genuinely cannot be produced, the financial institution will need to analyse the situation to determine whether it should exercise its discretion to facilitate the transaction on the basis of alternative forms of identification.
- 121. The acceptable forms of alternative identification include, in the case of:—
 - (a) an applicant for business, a birth certificate (or equivalent document constituting a jurisdiction’s official record of birth) accompanied by a Voluntary Declaration of Identification (or equivalent document with equivalent attestation requirements) from a person who is personally familiar with the subject of the Declaration and who has a familial relationship with the subject (i.e. parent, guardian or older sibling etc.) and a photograph, both of which (i.e. the Declaration and the photograph) must be signed by any one of the following—
 - (i) Justice of the Peace (JP);
 - (ii) Notary Public; or
 - (iii) Attorney-at-Law,to whom the customer is personally known for a period of not less than twelve months, and who is reasonably capable of confirming the identity of the customer;
 - (b) a customer or applicant for business who has not attained the age of majority²⁰⁵, and who is enrolled in a secondary or tertiary institution, a valid school ID may be accepted **PROVIDED:**
 - (i) The ID has the following features:
 - 1. A photograph of the student;
 - 2. Signature of ID holder (student);
 - 3. ID Number;
 - 4. Expiry date of ID;
 - 5. Name of the relevant academic institution (high/secondary school or tertiary institution);
 - 6. Signature of principal/bursar/vice-principal of the relevant academic institution.(The foregoing is applicable only to individuals under the age of 18 years as persons over 18 years of age will have attained the age of majority and will have achieved the age limit to qualify for obtaining other forms of identification i.e. Drivers Licence; Voters ID. etc.); and
 - (ii) The transaction pertains to the opening of an account through or with at least one adult constituting either the parent or legal Guardian of the applicant for business; or the transaction pertains to an account that is held jointly with at least one adult constituting either the parent or legal Guardian of the customer.
- 122. Where a financial institution is approached for business by a person seeking to use an acceptable form of alternative identification, the financial institution;
 - (a) must be satisfied that:— the person’s inability to produce at least one form of standard identification (as listed in paragraph 119 above) is genuine; and
 - (b) must ensure that appropriate safeguards are in place consistent with the assessed risk profile of the customer such as, transaction threshold limits applied to the business transacted.
- 123. It is not anticipated that a significant portion of the customer base of a financial institution will fall within this category. Consequently, a financial institution that seeks to rely on this exception above as the normal acceptable form of identification outside of the parameters indicated at paragraph 119 will be deemed to be acting contrary to its KYC obligations and will expose itself to regulatory action.
- 124. Paragraphs 120-122 outline minimum requirements a financial institution shall address when approached by applicants for business who seek to transact business using alternative forms of identification. However, a financial institution’s KYC and CDD processes and procedures must also speak to this matter and shall clearly indicate the transaction safeguards and other measures that will be applied to minimise the risk of conducting business with a person using an alternative form of identification.

²⁰⁵ See The Law Reform (Age of Majority) Act, (1979, sections 3 and 6.

125. Details for natural persons that must be in place for basic customer information **and** in the event the financial institution is served with a customer information order, include the following²⁰⁶:—
- (a) Information below in paragraph 126;
 - (b) Account / transaction number;
 - (c) Date on which the individual began to hold the account;
 - (d) Date on which the individual ceased to hold the account;
 - (e) Transaction date and description of transaction type;
 - (f) Account number of any other accounts to which the individual is a signatory and details (comprising the personal or private information) of the other persons holding those accounts;
 - (g) Source of funds that will be used in the transaction or used to access the service offered by the financial institution;
 - (h) Source of wealth;
 - (i) Occupation or economic activity/ties) responsible for the source of income;
 - (j) Business and personal contact details;
 - (k) Capacity in which the business is being transacted, (including details of the representative relationship (if applicable)); and
 - (l) Any other particulars necessary to complete its customer information requirements.

Customer Identification for Natural Persons (Whether Resident in the Jurisdiction or not)

126. The following information²⁰⁷ must be obtained from all prospective customers:
- (a) Full true name and names used;
 - (b) Verified current address and postal address (if different from the permanent address²⁰⁸);
 - (c) Date and place of birth and mother’s maiden name (in the case of an individual);
 - (d) For a joint holder of the account, full name, date of birth, place of birth and mother’s maiden name (in the case of an individual);
 - (e) Nationality;
 - (f) Taxpayer Registration Number (TRN)²⁰⁹;
 - (g) Contact numbers (work; home; mobile);
 - (h) Institutions must also require the submission of a photograph of the customer for their records. In the case of customers who are visitors to the island and not transacting business in the course of, or pursuant to a work permit situation, this requirement can be fulfilled by provision of an official identification which ordinarily carries a photograph such as drivers licence or passport.

NB. The foregoing is required in relation to all holders of the account and beneficiaries (interim and/or ultimate).

127. Under the POC (MLP) Regulations, customer information includes the TRN or other reference number (in the circumstances this may include NIS or other official number issued by a Government department or unique reference numbers generated by the financial institution). However, before proceeding with a transaction, the financial institution always has to be cognizant of what its legal position will be if it should be served with a customer information order pursuant to section 120 of the POCA.
128. Persons who would not reasonably be expected to have TRNs would include citizens of other countries who are:
- (a) visiting the island (e.g. Tourists; persons attending seminars or training workshops and courses; persons who are in the island pursuant to work permit arrangements or study arrangements (e.g. students enrolled with programmes and/or educational institutions that are accredited with the Ministry of Education);

²⁰⁶ POCA section 120(2) & (3). POCA (MLP) Regulations, r.7(5) where customer information is defined and same includes the TRN or other relevant reference number and the identity of the settler and beneficiary in arrangements involving settlements or trusts as per regulation 13(1)(c).

²⁰⁷ POCA (MLP) Regulations, 2007 as amended in 2019 r. 7(5) for the definition of “customer information”.

²⁰⁸ Note also 2008 Supreme Court (unreported) decision in the dual citizenship case of Richard Azan v. Michael Stern in which Mrs. Justice Marva McIntosh ruled that an address listed on the nomination paper as Main Street, Frankfield was incomplete. The Judge however went on to rule that the address to which a document comprising the substance of the matter was sent is sufficient once the address is the same place where the defendant could be found or communicated with. Leave was granted to appeal the decision, not to set aside the service and to strike out a Fixed Date Claim Form, notice of presentation of election petition and security filed by Richard Azan. The Appeal was dismissed.

²⁰⁹ Under the POC (MLP) Regulations, regulation 7, customer information “includes the applicant for business’s full name, current address, taxpayer registration number or other reference number, date and place of birth (in the case of a natural person) and mother’s maiden name (in the case of an individual), where applicable, the information referred to, at regulation 13(1)(c), TP (Reporting Entities) Regulations, (i.e. identity of beneficial owner). Under section 120 of the POCA, customer information also refers to the customer’s TRN which forms a part of the information an institution must present/produce in compliance with a customer information order.

- (b) persons passing through Jamaica to other destinations (i.e. in transit).
- 129. The onus will be on the financial institution to satisfy itself that the natural person with whom business is conducted is not a citizen of Jamaica and as such, is a person in respect of which a TRN would not be required. Relying on a driver's licence from the jurisdiction of residence has its limitations to the extent that it is possible for a person to have more than one driver's licence issued by different jurisdictions. As such, a person who is a citizen of Jamaica and who should be subject to the TRN requirement could bypass the requirement by tendering a driver's licence from another jurisdiction.

Self-Employed Persons & Sole Proprietors

- 130. Financial Institutions must ensure that they obtain the following information and documents or their equivalent in respect of new accounts or conduct appropriate reviews of such information and documentation when conducting significant transactions for self-employed persons and sole proprietors:—
 - (a) Identification and other details outlined above at paragraphs 119 and 126 above;
 - (b) Business Registration Certificate (where applicable);
 - (c) Account opening authority containing specimen signature/(s) (the authority must be clear as to whether the arrangement will include a nominee or alternate operator of the account. Where a nominee or alternate is indicated, the information at (a) above must also be obtained in respect of the nominee or alternate);
 - (d) A financial statement of the business (depending on the size²¹⁰ of the operations or magnitude of economic activity, these should be either audited statements, or financial accounts which have been prepared by a person who is duly registered as a Public Accountant in accordance with the Public Accountancy Act);
 - (e) Documentation listed at (f), (i), (j) and (k) at paragraph 131 below;

Membership in a recognized representative body or association is not mandated but is desirable as such memberships usually assist with regularisation and transparency of the business activities of their respective members.

Bodies Corporate²¹¹

- 131. Financial Institutions must be vigilant when dealing with corporate vehicles as they may be used as a method of maintaining anonymity. In all cases the financial institutions must fully understand the structure of the prospective corporate client, the structure in which the corporate client is held, the source of that customer's wealth, and the source of funds involved in the transaction and the beneficial owners, signatories and controllers²¹². This shall be the case whether the corporate client is locally incorporated or a foreign company. As of March 31, 2023, and referenced in paragraph 49A above on the Amendment to the Companies Act, companies incorporated in Jamaica or incorporated elsewhere but carrying on business in Jamaica, are required to identify, record and verify the identification and other information on their beneficial owners to include any change in beneficial ownership. (Sections 109 1(a) and 1A, 377A-377S, 377T)

Non-compliance with these obligations has serious consequences that include being struck off the register of companies at Companies Office to the issuance of criminal sanctions and/or administrative sanction in the form of fixed penalties. (See for example, sections 377H, 377I, 377W and 386A)²¹³

Financial institutions shall also ensure that they obtain the following documents or their equivalents in respect of new accounts, or undertake appropriate reviews of such information and documentation of the intensity and frequency consistent with the customer's risk profile or when conducting significant transactions for existing bodies corporate customers:

- (a) Certificate of Incorporation or certificate of registration;
- (b) Articles of Incorporation;²¹⁴
- (c) Directors' Resolution authorising company's management to engage in transactions;
- (d) Financial Institutions mandate, signed application form, or an account opening authority containing specimen signatures;

²¹⁰ The Development Bank of Jamaica website reflects a table of asset size and number of persons hired and categorization of micro, medium and small businesses; the Small Business Association of Jamaica's (SBAJ's) website reflects that the SBAJ's membership comprises businesses with 1- 50 persons with annual turnover not exceeding USD5Million and which is not a part of a conglomerate.

²¹¹ POC(MLP) Regulations, as amended in 2019 (r. 11, 12 & 13)

²¹² See POC (MLP) Regulations, 2007 as amended in 2019 (r. 11, 12 & 13); Basel Committee on Banking Supervision -Sound management of risks related to money laundering and financing of terrorism, January 2014 rev July 2020.

²¹³ Companies, others warned to disclose true owners be struck off the register | Business | Jamaica Gleaner

²¹⁴ Under the Companies Act, 2004 (operational 2005) the requirement for Memorandum of Association has been discontinued, however, Memorandum and Articles of Association would still be relevant for the purpose of these Guidance Notes until this documentation has been updated pursuant to the new Companies Act.

- (e) A financial statement of the business -Audited²¹⁵, or in the case of
 - (i) a company incorporated and in operation for under eighteen months, in-house financial statements;
 - (ii) a company which meets the criteria outlined at section 159 of the Companies Act, (company accounts which are in accordance with paragraph 5 of Section II of the 7th Schedule to the Companies Act and which have been prepared by a person who is duly registered as a Public Accountant in accordance with the Public Accountancy Act).

- (f) A description of the customer’s principal line of business and major suppliers or major customers/main target market (where applicable) (and other services or activities that materially contribute to the entity’s income); and whether the entity is designated as or associated or affiliated with any charitable establishments (locally or overseas);
- (g) A list of names, addresses and nationalities of principal owners, directors, signatories, beneficiaries and senior officers; evidence of the identity of the natural persons who are the beneficial owners, that is to say, the individuals that ultimately own or control the company or body corporate (i.e. holding 10% or more of the voting rights²¹⁶) must also be provided or be demonstrably readily accessible directly by the financial institution at will or immediately, on request;

Verification of the information provided on the directors, who are the persons responsible for the mind and management of the body corporate with whom the relationship will be established or transaction conducted, should also be independently verified from National company registries (including the COJ BO Registry), and other places where the information may have to be provided. Disclosures on the particulars of owners, and directors. Please be reminded that pursuant to section 23A of the Companies Act as amended in 2023 and discussed at paragraph 49A above, no company incorporated under this Act is permitted to have a nominee shareholder.

Where the directors and beneficial owners are themselves body corporates or trustees or settlers, the obligation to identify the ultimate beneficial owner is not satisfied until the identity of the natural beneficial owner or the senior manager with responsibility for the legal person or arrangement, is ascertained²¹⁷;

Disclosures on the particulars of owners, signatories and directors must include disclosures in relation to shadow directors.

- (h) Group/Corporate structure, where applicable;
- (i) A copy of the licence/approval to operate where the principal line of business is one that falls under a regulatory/supervisory body or is a regulated activity (i.e. a licence; or other authorisation must be obtained in order for the business activity to be legitimately undertaken);
- (j) Tax Compliance Certificate (TCC)²¹⁸ or other equivalent official confirmation from the relevant tax authorities of compliance with income tax obligations;
- (k) Proof of Compliance with the Beneficial Ownership requirements under the Companies Act of Jamaica;
- (l) The source of wealth of the corporate customers; and
- (m) The source of funds being placed with the financial institution.

Membership in a recognized representative body or association is not mandated but is desirable as such memberships usually assist with regularisation and transparency of the business activities of their respective members.

132. Customer information details for body corporates that must be in place for basic customer information requirements and in the event that the financial institution is served with a customer information order, includes the same information above at paragraph 125 on natural customers. Where the corporate customer is a part of a group of companies, the financial institution must ensure that it is aware of, and understands any group structures in which the corporate customer resides, and has undertaken the requisite due diligence to apprise itself of any relationships or activities (commercial and otherwise) within the group that could present a legal or reputational risk to the financial institution.²¹⁹

²¹⁵ The need for audited financial statements is applicable to locally established entities (i.e. subsidiaries or stand- alone legal persons i.e. akin in legal capacity to a body corporate).

²¹⁶ POC (MLP) Regulations as amended in 2019, regulation 13(1)(c)(iii)(A); TP (Reporting Entities) Regulations, regulation 13(1)(c)(iii)(A).

²¹⁷ POC(MLP) Regulations as amended in 2019 regulation 13(l)(c)(i)A and regulation 13(l)(c)(ii)(B); TP (Reporting Entities) Regulations as amended in 2019 regulation 13(1)(c)(i)A.

²¹⁸ TCCs (or equivalent confirmation of tax compliance) valid for one year can be obtained provided the taxpayer’s information in the database of the Tax Administration Jamaica can support the issuing of a TCC/or other such confirmation for that period. The application process involves submission of the application form + requisite clearance letters as outlined on the TAJ’s website. Electronic/online applications can also be facilitated. Applications can indicate whether or not the TCC/or other such confirmation is for several purposes (i.e. single purpose (eg. accessing banking facilities) or multipurpose (accessing banking facilities; imputation of goods etc.). Once the purpose of the TCC changes, the likelihood of achieving eligibility for a TCC that is valid for one year decreases because there would be no supporting information in the TAJ’s database in relation to the new purpose for the TCC, unless the requisite information is provided to allow for the relevant database to be updated accordingly.

²¹⁹ The DTIs must ensure that their account opening form includes an agreement to obtain written consent for access to the beneficial owner information from the beneficial owner. See section 352 (1A) of the Companies Act as amended in 2023.

Mandatory Use of the Companies Office of Jamaica’s Beneficial Ownership Registry

132A. Reference is made to letter sent by the Bank dated June 24, 2025 to all commercial banks, merchant banks and building societies, in relation to the operationalisation of the COJ’s Beneficial Ownership (BO) Registry. Pursuant to section 377J the Registrar of Companies is mandated to establish and maintain an accurate, adequate and up-to-date register of beneficial owners in respect of each company entered in the register of companies. Licensees are permitted access to the Registry in the carrying out of their KYC, EDD and CDD functions.

This registry serves as a key component of the national framework for promoting transparency and accountability in corporate structures and is aligned with international best practices, including the Financial Action Task Force (FATF) Recommendations 24 and Immediate Outcome 5.

Consequent on this letter all FIs have been mandated by the Supervisor to fully utilise the BO Registry in the conduct of customer due diligence (CDD), enhanced due diligence (EDD), and ongoing know your customer (KYC) processes when engaging with legal persons (such as companies, limited liability partnerships etc.).

Partnerships²²⁰

133. Financial institutions shall fully understand:

- (1) the obligations, responsibilities and entitlements arising under the partnership;
- (2) the source of wealth accumulated by the Partnership;
- (3) the source of funds involved in the transaction; and
- (4) the controllers and beneficiaries under the partnership (where this differs from the persons indicated as the Partners).

The above must be the case whether the partnership is locally established or established outside of Jamaica. Financial Institutions must also ensure that they obtain the following information and documents or their equivalents in respect of new accounts or undertake appropriate reviews of such information and documentation when conducting significant transactions involving partnerships or similar arrangements (by whatever name called):—

- (a) Partnership Deed (or other Instrument in writing which is duly signed by the Partners and which confirms the fact of the establishment of the Partnership);
- (b) Business registration certificate (where applicable) or equivalent instrument as the case may be;
- (c) The information regarding the authority to undertake or agree to engage in transactions which legally bind the partnership, signing authority for the account mandate and specimen signatures;
- (d) A financial statement of the business which must either be:—
 - (i) Audited, in the case of partnerships in operation for over 18 months and whose operations, if it were a company, would be in excess of the operating levels of a company described at section 159 of the Companies Act; or
 - (ii) In the case of partnerships in operation for over 18 months and whose operations, if it were a company, would either meet or fall below the operating levels of a company described at section 159 of the Companies Act, business accounts prepared in accordance with paragraph 5 of Section II of the 7th Schedule to the Companies Act, and which have been prepared by a person who is duly registered as a Public Accountant in accordance with the Public Accountancy Act;
- (e) A description of the principal line of business;
- (f) CDD for all partners, management officers and beneficiaries under the partnership (where these differ from the partners); nationalities and evidence of the identity of the partners, must also be provided or be readily accessible directly by the financial institution at will, or immediately, on request;
- (g) Details of entities, (incorporated or unincorporated) with which any one or more of the partners is affiliated. For the purpose of this requirement, details include name, business or registered address of the affiliated entity and the nature of the relationship with the affiliated entity;
- (h) Tax Compliance Certificate or other equivalent official confirmation from the relevant tax authorities of compliance with income tax obligations;
- (i) Confirmation of the source of funds being placed with the financial institution and source of wealth of the partnership as well as the partners, management officers, and beneficiaries under the partnership (where these differ from the partners).

²²⁰ New legislations (Partnership (General) Act, 2017, Partnership (Limited) Act, 2017, etc.) which will impact the definition and operation of partnerships are now in effect, both gazetted on February 8, 2017. These new legislations allow for partnerships to have separate legal standing and therefore would have separate liability from its partners.

*Principals and Beneficial Owners under, Trusts, Settlements and Other Legal Arrangements*²²¹

134. Financial Institutions must ensure that they obtain the following information and documents or their equivalents in respect of new accounts or conduct appropriate reviews of such information and documentation when conducting significant transactions involving trusts, settlements and other legal arrangements:—
- (a) Trust Deed or Instrument under which the trust, settlement or other legal arrangement, is derived²²² and evidence of the registration of the deed or other instrument. Appointments as Trustees that occur pursuant to section 10 of the Trusts Act are subject to the additional requirements that trusts relating to land shall be registered with the Registrar of Titles, and otherwise, registration must occur with the Island Record Office²²³;
 - (b) Identification and other details outlined above at paragraphs 119 and 126 are equally applicable in relation to all principals of trusts, settlements and other legal arrangements and beneficial owners and ultimate beneficial owners thereof who are natural persons. Where such principals and beneficial owners are themselves body corporates or trustees or settlors, then the obligation to identify the ultimate beneficial owner is not satisfied until the identity of the natural beneficial owner is ascertained²²⁴. Verification of identification information provided on such principals and beneficial owners must be independently verified from, for example, national registries (which record information on trusts and/or other legal arrangements, where these exist). Otherwise ownership and director identification details must, at a minimum, be accessible from the senior manager with responsibility for the trust or other legal arrangement²²⁵;
 - (c) List of names, addresses and nationalities of principal trustees or directors or other persons who are members of the board (or other body by whatever name called) of the trust, settlement or other legal arrangement that is responsible for the governance and oversight of the trust, settlement or other legal arrangement; beneficiaries, ultimate beneficiaries and management officers. Where such principals and beneficiaries/ beneficial owners of the board members (or other body by whatever name called) are themselves body corporates or trustees or settlors, evidence of the identity of the natural persons, that is to say, the individuals that ultimately own or control those members must also be provided or be readily accessible directly by the financial institution at will or immediately, on request²²⁶. In relation to the directors of trusts, settlements or other legal arrangements, as these persons would be responsible for the management of such trusts, settlements or other arrangements with whom the relationship will be established or the transaction conducted, the verification of the information provided on the members of the board or other body (by whatever name called) shall also be independently verified from National registries, and other places where the information may have to be provided²²⁷. The foregoing disclosures must also include disclosures in relation to nominee shareholders and nominee directors.

Charities/Non-Profit Organisations

135. Financial institutions play a critical role in facilitating legitimate access to financial services for Non-Profit Organizations (NPOs) and charities, while also serving as gatekeepers to safeguard the financial system from abuse. Supervisory expectations, consistent with FATF Recommendation 8 and Immediate Outcome 10, require financial institutions to adopt a balanced, risk-based approach when onboarding and maintaining relationships with NPOs and charities. Institutions should not apply blanket restrictions or disproportionately onerous requirements that undermine financial inclusion or hinder the essential humanitarian, social, or developmental work carried out by NPOs. Instead, they must assess each NPO or charity based on its specific risk profile, considering factors such as the nature of its activities, geographic areas of operation, funding sources, and transparency of governance structures.
- At the same time, financial institutions must remain vigilant to the potential for misuse of NPO and charitable structures for money laundering, terrorist financing, or proliferation financing. Supervisory guidance emphasizes the importance of applying enhanced due diligence where elevated risks are identified, such as where an NPO operates in conflict zones or high-risk jurisdictions, engages in complex financial flows, or displays opaque governance practices. However, for NPOs operating within low-risk parameters — such as those providing domestic community services with transparent funding sources — simplified due diligence may be appropriate. Financial institutions are expected to demonstrate that their onboarding practices strike the right balance between facilitating legitimate NPO access to financial services and ensuring robust, proportionate risk mitigation, aligned with Jamaica’s AML/CFT/CPF framework and international best practices.”
- 135A. Special care must be taken by financial institutions in dealing with unincorporated bodies (such as foundations; trusts etc.)²²⁸. The legal relationship shall only be established with the principal officers or principal representatives of the body, and information on these persons, the purpose of the account and intended nature of the business relationship must be obtained.

²²¹ POCA (MLP) Regulations, 2007 (r. 11, 12 & 13) as amended.

²²² Trusts Act; Trustees, Attorneys and Executors (Accounts and General) Act — These statutes govern the activities of Trustees.

²²³ Trustee Act, section 10(6)

²²⁴ POCA (MLP) Regulations amended 2019 regulation 13(1)(c)(i)A; TP (Reporting Entities) Regulations, regulation 13(1)(c)(i)A as amended 2019.

²²⁵ POC (MLP) Regulations, regulation 13(1)(c)(ii)(B) as amended 2019.

²²⁶ In relation to verification of the identity of Owners see above paragraph 130(g).

²²⁷ POC (MLP) Regulations as amended, regulation 13(1)(c)(iii); OECD — Supervision and Enforcement in Corporate Governance, 2013.

²²⁸ FATF’s 2003/4 AML and CFT typologies exercise covering, *inter alia*, non-profit organizations. (See also FATF Best Practices — Combating the Abuse of Non-Profit Organisations, June 2013 & FATF Best Practices — Transparency and Beneficial Ownership, October 2014).

136. Financial Institutions must therefore ensure that they obtain the following information and documents or their equivalents in respect of new accounts or significant transactions involving charities, or non-profit organizations (NPO):—
- (a) In the case of a charity which is established as a body corporate by incorporation as a company or otherwise, the articles of incorporation²²⁹ and certificate of incorporation or charter, statute or other like instrument by which it is established;
 - (b) The constitution (as defined under the Charities Act) of the charity or NPO;
 - (c) Evidence of registration in accordance with the Charities Act, 2013;
 - (d) In relation to charities or NPOs which have been established as bodies corporate, whether as companies or otherwise, the information set out at paragraph 125 (c), (d) and (e) of these Guidance Notes;
 - (e) List of names, addresses and nationalities of principal owners or of the beneficial owners (if different from the principal owners) (i.e. to say the individuals who ultimately own or control the charity or NPO), directors, trustees, settlors or other persons who are governing board members as defined in the Charities Act, and management officers;
 - (f) A financial statement of the charity or NPO which shall be prepared as outlined in the Charities Act or Regulations thereunder and which must be:—
 - (i) Audited, in the case of charities in operation for over 18 months and whose operations, if it were a company, would be in excess of the operating levels of a company described at section 159 of the Companies Act; or
 - (ii) In the case of charities in operation for over 18 months and whose operations, if it were a company, would either meet or fall below the operating levels of a company described at section 159 of the Companies Act, business accounts prepared in accordance with paragraph 5 of Section II of the 7th Schedule to the Companies Act, and which have been prepared by a person who is duly registered as a Public Accountant in accordance with the Public Accountancy Act;
 - (g) A list of the charity’s significant donors and recipients of financial and other assistance (including name, address, nationality; main business activity or occupation and where the donor is a body corporate, trust, settlement or other legal arrangement, the names of the natural persons who are the directors and beneficiaries thereof). Financial institutions will need to ascertain whether the information provided by the charity, is sufficient to allow for a determination to be made by the financial institution regarding the risks of doing business with that charity including the risk of a terrorist financing activity being facilitated through dealings with that charity and the extent of business that is facilitated with or involving that charity;
 - (h) Evidence of the due diligence done to confirm the bona fides of the source of funds received from the donor and source of wealth of the donor.

Customers Resident Overseas

137. In addition to the foregoing considerations, additional factors must be included in the due diligence and broader KYC processes and measures that are applied.
138. Financial institutions are required to ensure that, among other things, a financial institution’s AML/CFT/CPF measures include paying special attention to all business relationships and transactions with any customer resident or domiciled in a territory specified in a list of territories published by notice in the Gazette on the recommendation of the competent authority and the designated authority.²³⁰ For the purposes of these Guidance Notes, the jurisdictions that would ordinarily be targeted for this special attention include jurisdictions flagged by:—
- (a) FATF;
 - (b) One or more of the other 8 FATF Styled Regional Bodies (“FSRJB”);
 - (c) UNSEC;
 - (d) A country with which Jamaica is Party to a treaty that requires a Party to such treaty to take certain actions in relation to nationals of either Party in accordance with the circumstances outlined in such treaty, and
 - (e) Any other territory not specified above identified by the Supervisory Authority whether spontaneously as a risk mitigation measure for the protection of the financial system or in response to other international obligations.

²²⁹ Refer to paragraph 130, on Bodies Corporate, for a definition.

²³⁰ POCA (Amendment) Act, 2019 section 94A, POC (ML) Regulations, 2019, Regulation 8. Also see the BOJ’s Supervisory Authority Notice published May 2, 2023 and available on the BOJ’s website at www.boj.org.jm.

(Refer to Section III above at paragraph 64 and 75A -D above on “*Advisories and Publications issued in relation to certain Jurisdictions*” and “*Domestic Regulatory requirements.*”)

139. Financial institutions must exercise a high level of caution when establishing business relationships with foreign companies that have nominee shareholders or bearer shares. If the ultimate beneficiary(ies) or beneficial shareholder(s) cannot be reliably established or there are no reliable measures in place to monitor any changes in the ownership structure or to capture details of the holder of bearer shares, then the relationship shall **not** be commenced, or where a business relationship has already been established, this relationship must be legally terminated.
140. Institutions must also exercise particular care when dealing with overseas counter-parties or financial institutions acting for overseas clients, where to the local financial institution’s knowledge, the overseas counter-party or representative financial institution is not subject to AML/CFT/CPF laws and regulatory arrangements at least as stringent as those applicable to Jamaica. In this regard the guidance on Introduced Business and Professional Intermediaries etc. is particularly relevant. Additionally, financial institutions must apply EDD and carefully scrutinize any transaction proposed to be carried out with any client, counter-party or financial institution situated in a jurisdiction with weak or non-existent AML/CFT/CPF programmes or with a known history of involvement in drug production, drug trafficking, corruption, money laundering or terrorist financing or renowned for industry sensitive activities such as the production and transportation of arms; or whose citizens or which is itself the subject of targeted financial sanctions as indicated in these Guidance Notes. Financial institutions must also seek to keep abreast of steps being taken by such jurisdictions to effectively deal with such matters.

Natural Persons Resident Overseas

141. The identification and KYC requirements for natural persons resident in Jamaica also apply to natural persons resident outside of Jamaica. Financial Institutions are required to obtain the same identification documentation or their equivalent for prospective customers resident outside of Jamaica. Financial Institutions must also ascertain why a non-resident client has chosen to open an account in the local jurisdiction²³¹.

Overseas Based Bodies Corporate

142. The requirements for the KYC and customer due diligence for domestic corporate customers are also applicable to overseas corporate bodies with which a financial institution does business. Comparable documents to those listed in paragraph 131 must be obtained, when opening accounts for companies or any bodies corporate incorporated outside of Jamaica.
143. The financial institution would be expected to ensure that the foregoing is considered in the context of a jurisdiction which is not subject to any one or more of the following actions:—
- (a) identification by the FATF; CFATF or any FRSB as a jurisdiction with strategic deficiencies or weaknesses in its AML/CFT/ CPF framework;
 - (b) identification by the United Nations as a jurisdiction subject to targeted financial sanctions pursuant to UN Resolutions on Terrorism and Terrorist Financing — i.e. UN Resolutions 1267 (1999), 1373 (2001), and related resolutions; and targeted financial sanctions pursuant to UN Resolutions on the proliferation of weapons of mass destruction²³²; or
- identification as a ‘specified territory’ by a supervisory authority pursuant to section 94A of POCA by notice published in the *Gazette*.
144. Particular attention must be paid to the place of origin of identity and other documents provided in such circumstances, and the background against which they are produced, bearing in mind that standards of control vary between countries. A financial institution may have to request certified copies of documents notarised by a foreign official such as a notary public, or county clerk in addition to making appropriate enquiries with overseas authorities, statutory organizations, overseas credit reference agencies, or similar bodies.

Transaction Counter-parties

145. A counterparty to any transaction with a financial institution shall be subject to the same due diligence undertaken in relation to customers as far as this is applicable in the circumstances.

Verification of CDD, KYC & Transaction Details

146. Financial institutions are strictly required to apply the verification protocols outlined herein as a baseline and not as an exhaustive checklist, ensuring that additional measures, caution, and professional scepticism are exercised throughout the customer due diligence process. The independent verification of identity, proof of address, beneficial ownership, employment status, and other KYC/CDD details must be conducted in accordance with these protocols, while recognising that evolving risks, inconsistencies, or incomplete information may necessitate further scrutiny beyond the stated procedures. Institutions are reminded that reliance on isolated checks — such as verifying details solely with an account holder, affiliated entity, or through a single source — does not satisfy the broader obligation to obtain independent, reliable, and corroborative verification. Moreover, where reliance on external databases,

²³¹ POC (MLP) Regulations and the TP (Reporting Entities) Regulations include in the description of ‘high risk’ customers, ‘a person who is not ordinarily resident in Jamaica.

²³² UN Resolutions 1718(2006), 1737(2006), 1747(2007), 1803(2008), 1874(2009) and 1929(2010).

customer consents, or practical limitations (such as geographic proximity for spot checks) apply, FIs must still ensure that risk-based, proportionate, and where necessary, enhanced due diligence is exercised to close any verification gaps. Supervisory expectations require flexibility in applying additional verification layers when the customer’s risk profile, transactional behaviour, or other red flags indicate the need for heightened controls, consistent with Jamaica’s AML/CFT/CPF regulatory framework and international best practice.

In support of the above, the name, permanent address and employment/business details of a customer must be verified by an independent source, (i.e. by a source other than those provided by the customer), as per the following examples:

- (a) *Identity*
Independent confirmation of national identifications with the relevant Government Authorities, e.g. (confirming driver’s licences with the records of the Collectorate; confirming Voters ID with the relevant electoral office of Jamaica; confirming passports with the Passport, Immigration and Citizen Agency and confirming employee identification cards with the indicated employers, cross-checking NIC and NIN across the national identification database).
- (b) *Proof of address*
 - (i) Requesting sight of a current utility bill for the customer’s place of residence (for example, electricity, telephone, and water) or cable receipt in the name of the customer²³³; to include a letter from a landlord etc²³⁴); requesting sight of correspondence from an independent source such as a central or local government department or statutory body. Documents addressed to, for e.g. P.O. Box numbers may be relied on where there is no street number or other coded identification to identify the physical location of the address or where the P.O. Box number comprises a routine part of the standard mailing address and it is confirmed that the customer receives mail using that mailing address;
 - (ii) Checking a local telephone directory and calling the number for verification purposes;
 - (iii) Checking the Voters’ List ²³⁵;
 - (iv) Spot check visits to the home address or work place (where practical i.e. where the home or work place of the customer is in relatively close proximity to any locations where the financial institution is represented or has a physical presence);
- (c) Beneficial Owner²³⁶.
- (d) Confirming customer’s details and status of employment independently with the employer; confirming customer’s salary scale by obtaining general information from the employer of the salary scale and benefits applicable to the level indicated by the customer;
- (e) Cross-checking KYC and CDD details with other financial institutions or businesses that the customer indicates financial business is transacted with (for instance the issuing bank in the case of cheque transactions; the insurance company from which the funds are indicated as being obtained, the Cambio from which the foreign currency was received, or the remittance company through whom the funds were sent). In so doing, financial institutions will need to be guided by the respective Agreements with the customer which must ideally reflect that the customer’s consent has been obtained to do this type of check.
(See also paragraph 148 below)
- (f) Cross-checking KYC and CDD details for one account holder with the other holder of the account and vice-versa (however if this check is done it shall not comprise the only effort at establishing independent verification of information is that which is provided by an account holder).
- (g) Cross-checking KYC and CDD details provided with other affiliated companies within the corporate group with whom the customer has also done business. (In so doing financial institutions will need to be guided by the respective Agreements with the customer which shall ideally reflect that the customer’s consent has been obtained do this type of check.)

(NB. Reference to the customer also includes reference to the Applicant for business)

²³³ POC (MLP) Regulations, regulation 7(5) definition of ‘satisfactory evidence’.

²³⁴ The following utility bills are accepted Cable, Electricity, Water, and Internet* (*Only on-premise internet bills are accepted.) * Physical and electronic copies (E-bills) of utility bills are accepted. However, E-bills must be scrutinised carefully for authenticity. In the case of a private residence, a utility bill must accompany a Letter of Authorization/Confirmation of the residential address. The owner of the home must confirm the use of the address and state the relationship to the individual. A copy of a form of national identification of the owner of the residence must also accompany the letter. Handwritten letters of authorization/confirmation are acceptable for the required purpose. (To be completed ONLY if the Utility Bill is not in the Applicant’s Name. In the case of a rental, a copy of the Lease/Rental Unit Agreement for the rental premises identified bearing the name of the applicant must be presented. If the utility bill or Lease/Rental Unit is not in the applicant’s name, a letter from the owner confirming the applicant’s residence and a copy of a form of national identification of the owner (National ID, Passport or Driver’s Permit) must be submitted.

²³⁵ Checking with the Post Office which has listings according to constituency or purchasing the information from the Electoral Office of Jamaica.

²³⁶ The Companies Act was amended in 2023 for access to BO information held in a registry.

Verification of Identification Details Post Commencement of Business Relationship

147. POCA (MLP) Regulations, 2007 (and as amended 2019) (r. 7) speaks to situations in which satisfactory evidence of a customer’s identification can be obtained as soon as is reasonably practicable and not more than fourteen days after contact is first made between that person and an applicant for business. Before proceeding in this manner, a financial institution must be in a position to provide documentary evidence of the risk management evaluation it undertook to satisfy itself that it could proceed with the transaction. This includes evidence of considerations which at a minimum shall include—
- (a) The nature of the proposed business relationship;
 - (b) The nature of the transaction/(s) contemplated;
 - (c) The geographical location of the parties;
 - (d) Practicality of proceeding viz. entering into commitments; or facilitating transactions before confirmation of the identification is obtained, (included in this consideration is whether proceeding is essential to not interrupting the normal conduct of business);
 - (e) Assessment of the risks to the institution if it proceeds without confirmation of the customer’s identification.

Confirmation of KYC/ or CDD with the assistance of other financial institutions

148. In some cases, a financial institution may require the customer to issue instructions to another financial institution with whom he/she/it has dealings and which institution is able to provide appropriate KYC verification for the customer in question. A financial institution may therefore need to approach another on a non-competitive basis, specifically for the purpose of verifying certain KYC/ CDD details. Where this is the case, it is expected that members of the industry will formulate industry agreements and/or protocols on these matters, within the specific constraints of the law. Where KYC/ or CDD verification is pursued through this option and the information is still not forthcoming from the institution from whom the assistance is requested, then unless the information is obtained,
- (a) the transaction shall not proceed; or
 - (b) where commenced in circumstances where it was deemed reasonable to proceed ahead of the verification, must not be completed; or
 - (c) where the relationship is already formed (e.g. an account is opened ahead of verification) then no other service or facility or transaction must be provided or conducted with, on behalf of, or in relation to this customer;

unless and until the appropriate KYC/ or CDD verification information has been received whether from the institution from which the information was requested or from an alternative but equally reliable independent source. The financial institution must ensure that it is legally in a position to terminate the account/transaction or sever the business relationship where the verification of KYC/ or CDD details cannot be obtained.

In order to facilitate compliance with the law it is critical that institutions respond in a timely manner to each other’s requests for assistance with the verification of KYC/ or CDD information. Financial institutions should also be reminded that the legal obligation to accurately identify and verify the identity of an applicant for business remains with an FI throughout.

Transaction Verification

149. Transaction verification involves ensuring that the transaction indicated and conducted is the one intended by the customer/counterparty. Verification processes therefore contemplated by these Guidance Notes include—
- (a) Ensuring that agents acting on behalf of customers/counterparties have tendered evidence of the requisite authority and that the instructions pertaining to the transaction at hand are verified. E.g. Conducting a \$500,000 transaction when the intention or authority was for a \$50,000.00 transaction.
 - (b) That transactions indicated are in essence the transactions conducted and are genuine in terms of correct documentation, proper invoicing, source of asset ownership, source of funds etc.
 - (c) Consistency of transaction being conducted with transaction patterns for the industry/sector business or the account history.
 - (d) Commercial reality or method by which the transaction is conducted must be consistent with approved or accepted industry practice or must clearly serve and reflect economic and/or lawful purpose. e.g. transactions, in which the payment is not directly reflected between the entity and the counterparty, shall be flagged.
150. Verification procedures would therefore include—
- (a) Ensuring that the customer or counterparty to the transaction is not a listed entity under the TPA; or a person who is personally subject to criminal designation e.g. drug kingpin; or confirming whether or not a person is operating from a jurisdiction that is the subject of a public statement or designation from an internationally recognized AML/CFT/CPF authority reflecting it has weak or non-existent AML/CFT/CPF laws and measures.

- (b) Establishing the source of funds or source/origin of the property that is the subject of the transaction.
 - (c) Checks (where applicable) with the relevant Trade/Service regulator to ensure the customer or counterparty is not subject to regulatory sanctions that would make it illegal or unlawful for the transaction at hand to be undertaken.
 - (d) Measures employed to satisfy the financial institution that any applicable industry requirements or laws are not being breached or the breach thereof is not facilitated by the transaction being conducted or to be conducted with the financial institution.
 - (e) Measures employed to satisfy the financial institution that agents acting on behalf of customers or counterparties have tendered evidence of the requisite authority and that the instructions pertaining to the transaction at hand are verified.
151. Under the POC (MLP) Regulations, a record of each transaction conducted must be kept in a manner that will facilitate the reconstruction of such transactions²³⁷. Additionally, a financial institution is required to keep account files in relation to each customer containing all pertinent information to include customer information, types of accounts held and a summary of activities of each account, in respect of each of the customer’s accounts with the institution²³⁸. A financial institution must also ensure that evidence of transaction verification it has undertaken, is documented and retained either with the transaction itself or in a manner which allows for ready or immediate recollection on request or as necessary, and readily available to the designated authority and/or competent authority. This information must also be readily available to the auditors of the financial institution.

FINANCIAL INCLUSION

SIMPLIFIED AND ENHANCED DUE DILIGENCE — IDENTIFICATION AND KYC REQUIREMENTS

152. The application of measures that enable more individuals and businesses, especially low-income, unserved and underserved groups, to access and use regulated financial services increases the reach and the effectiveness of anti-money laundering/countering the financing of terrorism (AML/CFT) regimes and enhances financial sector transparency and integrity²³⁹.

The risk-based approach is a central element to combatting ML/TF and financial inclusion²⁴⁰ is supportive to AML/CFT objectives. Recognising that AML/CFT measures can be implemented in a way that undermines financial inclusion, financial institutions are encouraged in employing the risk-based approach to AML/CFT measures to facilitate financial inclusion and to minimise unnecessary disruption to financial activities. To this end, it is noted that FIs may configure services and products to facilitate financial inclusion. By way of examples, it is anticipated such approaches may include:

- facilitating opening of basic accounts which are established simply to, for e.g. facilitate salary-based payments between an employer and its/his/her employees; or for e.g. establishing accounts to allow for compensation or compassion-based payments from the GOJ;
- broadening the circumstances or conditions under which a customer may utilise the business relationship prior to verification;
- adjusting customer ID procedures to focus initial or sole reliance on identification documents other than government issued ID, for example, a letter addressed to the customer by a governmental body or other reliable public body;
- application of SDD as the default due diligence based on pre-identified factors which permit the transaction or relationship to be identified as low risk; and
- adjusting CDD such that based on the risk, source of funds and source of wealth due diligence would only be applicable where enhanced due diligence is considered warranted in the circumstances and/or not mandated by law.

Building from the above are the following examples of anticipated Risk mitigation measures:

- FIs may limit the number, types and/or amount of transactions that can be performed and pay special attention for any the large or complex transactions being carried out outside the expected norms for that type of relationship;
- FIs should not extend the approach to overseas based customers; and
- There may be greater use made of financial technology (Fintech) to track factors contributing to risk profiles and patterns that could be indicative of behaviour that requires heightened monitoring or application of more routine CDD type measures.

²³⁷ Regulation 14(4)(a) as amended in 2019.

²³⁸ Regulation 14(4)(b) as amended in 2019.

²³⁹ FATF Guidance on AML and TF measures and financial inclusion referred at para 63 above, pg 3.
‘.... unserved and underserved persons in both developing and developed countries should not be automatically classified as resenting lower risk for ML/TF but that appropriate risk assessments often conclude that they present a lower risk.’

²⁴⁰ FATF *ibid* at para 22, has updated the definition of financial inclusion to mean “... in general terms, financial inclusion refers to both access to and active use of an adequate suite of regulated, appropriate, safe, convenient and affordable financial services by individuals (including households) and entities that would benefit from such services. “Appropriate” means that the products and services are tailored to the customer needs and delivered transparently and fairly. The concept of financial inclusion has evolved, from access to regulated financial services to also include appropriate usage and quality of those services and products, financial literacy, financial resilience and financial well-being of end-users.”

Where a financial institution deems that there is a basis on which transactions could or should proceed ahead of firm establishment of the identity of a customer or applicant for business, FIs are reminded of the legal obligation contained in regulation 13(2) of the POC (MLP) Regulations referred to above that there should be clear documentation of the rationale for proceeding on that basis. Proceeding should be subject to a time bound course of action for completing the identification procedures or for completing the verification of identification.

153. The revised FATF Recommendations allow for either simplified or enhanced measures to be applied for specifically defined customers and products which have been assessed as presenting a higher risk or lower risk of money laundering or terrorist financing²⁴¹. This has been codified in POCA and its regulations (*see paragraph 29 above*). Where higher risks for ML, TF or PF are identified by a country, that country must either prescribe that financial institutions and DNFBPs take enhanced measures to manage and mitigate these higher risks or require these persons to ensure that such information is taken into account when undertaking their respective risk assessments²⁴².

Meeting this requirement, among other things, involves:—

- (a) Conducting an assessment as discussed above in Section IV of these Guidance Notes. The assessment methodology (including data source; active periods covered by the assessment; basis for methodology and findings) shall be documented and readily available to the Supervisor, designated authority and/or external auditors;
- (b) Ensuring the assessment is reflective of the country’s assessment of its ML, TF and PF risks;
- (c) Ensuring the assessment is kept up to date (i.e. assessments being undertaken periodically (at least once every three (3) years or more frequently where trends and typologies warrant);
- (d) Having the Supervisor review the ML, TF and PF risk profiles and risk assessments that have been prepared by the financial institution to monitor whether the financial institution’s operations are consistent with the risk assessments and risk profiles that it has generated.

Simplified Due Diligence

154. Financial institutions may apply simplified due diligence (SDD) measures after a thorough risk assessment has identified lower risks with respect to doing business, or establishing or maintaining certain relationships with certain customers or counterparties. FIs may use a combination of these factors to make a determination in applying these simplified measures. However, the financial institution must ensure that the lower risks are commensurate with the overall risk assigned to the relevant sector, customer or activity type, as well as those identified in the NRA or any available sectoral risk assessments²⁴³.

Examples of circumstances in which a financial institution may apply simplified measures include, but are not limited to²⁴⁴:

- (a) Customer factors, such as:
 - (i) Individuals whose sole or primary source of income is employment based and who fall in the category of PA YE under Jamaica’s tax laws or under any other tax law;
 - (ii) Low income earners;
(as determined in relation to an objective metric such as the national minimum wage)
 - (iii) Pensioners (where the pension situation reflects a single source of income and the pensioner also qualifies as a low-income earner);
 - (iv) Financial institutions where the preventive measures implemented comply with the statutory AML/CFT requirements to combat money laundering and terrorist financing and are commensurate, with the risks identified by the financial institution;
 - (v) Public administrations or enterprises [which are in compliance with the Public Bodies Management and Accountability Act and the Financial Audit and Administration Act and which have no material matters outstanding with the Auditor General or Integrity Commission] where the risk assessment justifies this approach.
- (b) Product, service, transaction or delivery channel risk factors, such as:
 - (i) FATF gives one example of “financial products or services that provide appropriately defined and limited services to certain types of customers to increase access to financial inclusion, for example “small bank accounts” for unbanked individuals where there are caps on overall value²⁴⁵;

²⁴¹ FATF Guidance Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion, February 2013 updated June 2025 — Paragraph 68.

²⁴² Revised FATF Recommendations — Paragraph A4 — Interpretive Note to R1.

²⁴³ Reference footnote 110 above. The different approaches prescribed for handling clients in situations assessed as low risk under the POCA and the POC (MLP) Regulations and the TPA and TP (Reporting Entities) Regulations are to be noted. For the avoidance of doubt the TPA requires licensees to seek the approval of the Supervisor before applying SDD measures where the TF risk has been assessed as low. Further guidance will be provided on this matter in separate future communication. In the interim where the risk under the TPA is assessed as low and it is intended to apply SDD this will be addressed by the Supervisor being written to for its non-objection on a case by case basis.

²⁴⁴ FATF Recommendation 10 — Customer Due Diligence — Interpretive Note.

²⁴⁵ See paragraph 69 of the FAT Guidance on Financial Inclusion.

- (c) FIs must apply a risk-based approach to financial inclusion offerings, ensuring proportionate controls while maintaining vigilance for these typologies. Simplified CDD measures must not be applied indiscriminately, and monitoring systems should be calibrated to detect unusual patterns consistent with the outlined risks. Enhanced due diligence, transaction monitoring, and ongoing customer reviews are critical when activity deviates from the expected financial behaviour of inclusion-focused products. This approach aligns with FATF Recommendations 1, 10, and 20, as well as Jamaica’s national AML/CFT/CPF framework.
155. SDD measures for a customer may include the following²⁴⁶:
- (a) Reducing the verification thresholds for prospective customers (i.e., requiring only one form of Government-issued identification and accepting alternative forms of identification other than Government-issued identification);
 - (b) Collecting basic identity verification information such as names, dates of birth, or in the case of business customers, dates and places of incorporation²⁴⁷;
 - (c) Reducing the frequency of customer identification updates;
 - (d) Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold as determined by the financial institution, which in any event should be based on the customer profile;
 - (e) Relying on publicly available documents or a third party that is subject to analogous obligations to conduct verification of identity of applicant/customer/beneficial owner(s).

De Minimis Transactions

156. Exemptions from the requirement for identification procedures are applicable in the case of de minimis transactions. Under regulation 8 of the POC (MLP) Regulations, transactions amounting to or less than US\$250.00 or the equivalent in any other currency are exempted from the identification procedures outlined in Regulation 7 where the nature of same does not give rise to the knowledge or belief or reasonable grounds for such knowledge or belief that the transaction is or is related to ML.²⁴⁸
157. There is no exemption from extending risk assessments to transactions of a de minimis nature. For de minimis transactions identification and transaction verification need not be invoked however all other AML/CFT/CPF precautions and requirements remain applicable. This means that for the purpose of record keeping, financial institutions must ensure that the following measures are taken:
- (a) Transaction records shall reflect salient details and shall include:
 - (i) The customer’s name;
 - (ii) The customer’s permanent address²⁴⁹ and jurisdiction of residence or incorporation/establishment;
 - (iii) Transaction type;
 - (iv) Transaction amount;
 - (v) Transaction currency (and Jamaican dollar equivalent if the transaction is in foreign currency);
 - (vi) Identification type and number; and
 - (vii) TRN (where applicable) or other reference number.
 - (b) Transaction processes must be risk-based. Transactions are required to be monitored/reviewed to detect/prevent Layering/Structuring — i.e. transactions by the same person (connected transactions) or transactions conducted separately but which are intended to take effect as one transaction for the benefit of one person. Connected transactions which take place on the same day which each meet internal limit but which altogether exceed the institution’s internal limit, shall be reviewed to determine whether procedures for identification and transaction verification must be applied notwithstanding the transaction amount, since such transactions could constitute layering or structuring to avoid KYC/CDD requirements.

Transactions for which the De Minimis Approach does not Apply

158. Transactions subject to Required Disclosure (Suspicious Transactions) — The de minimis exemption is not applicable to transactions that require disclosure under sections 94 and 95 of the POCA, POC(MLP) Regulation (r.8(1)) or disclosure under sections 16 or 17 of the TPA (r.8(l)) of the TP (Reporting Entities) Regulations.

²⁴⁶ The POC (MLP) Regulations, amended 2019 regulation 7.

²⁴⁷ Address verification may not be required for SDD.

²⁴⁸ Initially, the inclusion of the concept of a de minimis level in the AML framework, was based on the observations of the financial crimes investigative authorities that the transactions which appeared to present risks of a financial crime being conducted and which featured significantly in the STRs generated, were those which reflected amounts in excess of approximately USD\$250. It must be noted that the AML/CFT laws do not reflect that the de minimis approach absolves financial institutions from conducting their own risk assessments in relation to such transactions.

²⁴⁹ Address verification may not be required for SDD, however the address of the Originator maybe required. See FATF Recommendation 16.

159. Remittance Transactions — The de minimis approach is not applicable to remittance transactions (r. 8(2) of the POC (MLP) Regulations and (r. 8(2) of the TP (Reporting Entities) Regulations).

Transactions to which the De Minimis Approach shall not Apply

160. Critical Transactions — The Bank of Jamaica considers the following to be critical transactions for the purposes of these Guidance Notes—
- (a) Transactions effectively amounting to the opening of accounts and/or closing of accounts;
 - (b) Transactions that are assessed as ‘high risk’ for ML FT or transactions which are subject to circumstances which are described in the AML/CFT laws as falling in the category of ‘high risk’.

Accordingly, it is expected that transactions which in dollar value fall within the de minimis limit but which in nature are “critical transactions” shall be subject to the usual KYC and CDD policies and procedures.

- 160A. Transactions which in dollar value fall within the de minimis limit and which are assessed as ‘high risk’ for PF should NOT be eligible for application of the de minimis approach.

General Comment

- 160B. SDD must not be applied in higher-risk scenarios where there is an increased risk, or suspicion that the customer is engaged in ML/TF/PF, or the customer is representing or acting on behalf of another person that is engaged in ML/TF/PF, or where the customer is from or is in a country or jurisdiction considered to have inadequate AML/CFT/CPF measures.
- Financial institutions are mandated by law to document the full rationale behind decisions to apply SDD to any customer or transaction and make relevant information and documentation available to the Supervisor upon request.

Enhanced Due Diligence

161. Heightened requirements are applicable where either the ML/TF/PF risk of doing business or establishing or maintaining certain relationships with certain customers or counterparties increases.
- Such circumstances of increased risk arise for instance by virtue of jurisdiction in which the customer or the property involved in the transaction is located, the positions held or functions undertaken by the customer or transacting counterparty, or in relation to customers or transacting counterparties in respect of which the financial institution conducting business will either not have, or will have very limited opportunity to transact business directly with that customer or counterparty on a face-to-face basis and as such will have to rely on the judgment and information provided by a third Party.
- Accordingly, under POC (MLP) Regulations and TP (Reporting Entities) Regulations, the persons who are identified as high risk and to whom EDD must be applied on the basis of being high-risk are—
- (a) Politically Exposed Persons (PEPs) (POC (MLP) Regs. reg. 7A(6),
 - (b) A person who is not ordinarily resident in Jamaica;
 - (c) A person acting as a trustee for another in relation to the business relationship or one-off transaction concerned;
 - (d) A company having nominee shareholders²⁵⁰ or shares in bearer form; or
 - (e) Where the applicant for business is not the ultimate beneficial owner of the assets concerned in the business relationship or one-off transaction; or
 - (f) Such other class or category of persons specified by the supervisory authority by notice published in the *gazette*.

Therefore, based on the AML/CFT legislation in relation to these specified categories of persons, applying simplified due diligence measures or exemptions from CDD MUST NOT occur.

162. Risks²⁵¹ also increase if the customer or counterparty resides in, or operates from, a jurisdiction which is the subject of an adverse rating or an international sanction related to identified deficiencies in that jurisdiction’s prudential, regulatory or AML/CFT/CPF framework. Risks also increase if the customer or counterparty resides in, or operates from, a jurisdiction which is subject to a regulatory or supervisory framework that is incompatible with the supervisory or regulatory framework in Jamaica. Incompatibility would be measured by the absence or presence of any one or more of the following circumstances such as:—
- (a) The financial activity not being subject to any regulation or supervision, or is not subject to an equivalent regulatory or supervisory framework;
 - (b) The person undertaking an intermediary, agent or representative role in relation to the transacting counterparty or customer is not subject to AML/CFT/CPF laws and regime; and/or
 - (c) The existence of secrecy laws and other legislative or policy requirements that adversely impact or hinder or prevent effective regulatory collaboration or cooperation from taking place between BOJ and the regulatory/supervisory/competent authorities in that jurisdiction.

²⁵⁰ Please note the amendment to section 23A to the Companies Act in 2023 which states that “No company incorporated under this Act (in Jamaica) shall have a nominee shareholder.”

- 162A. For the purposes of the Reporting Entities Regulations under the UNSCRIA, relationships or transactions that should be identified as high-risk include—
- (a) Those relationships or transactions which the financial institution believes, or suspects pertain to customers or other transacting parties, counterparties or properties located in [or associated with] the DPRK or DPRK nationals;
 - (b) Transacting parties with no sanctions screening processes or with limited or inadequate sanctions screening processes.
- 162B. The list of relationships or transactions reflected in the AML/CFT regulations is not exhaustive and can be expanded by the supervisory authority under the POCA, by Notice published in the *gazette*. As such, **financial institutions are subject to the statutory mandate to establish a risk profile regarding its operations generally and all respective business relationships and one-off transactions**²⁵². The POC (MLP) Regulations define “risk profile” as a formal assessment made by the regulated business concerned as to the level of ML risk posed to the regulated business by the business relationship or transaction concerned. It is recommended a similar approach be applied in relation to the establishment of a risk profile in relation to TF risks.
163. Additional circumstances which, based on the foregoing, appear to increase the ML/TF/PF risks to a financial institution doing business include:—
- (a) Verification of identification post commencement of the business relationship;
 - (b) Introduced business;
 - (c) Accounts opened by Professional Intermediaries;
 - (d) Private banking clients; Transferring clients;
 - (e) Transactions via emerging technology (e.g. transactions involving virtual assets or virtual asset providers; transactions involving virtual assets; transactions with persons established and /or operating only through a digital presence);
 - (f) Correspondent banking; payable through accounts;
 - (g) Countries with inadequate AML/CFT/ CPF frameworks;

Enhanced Due Diligence for High Risk Jurisdictions

- 163A. Financial institutions are required to apply enhanced due diligence measures to all business relationships and transactions that are—
- assessed as high risk;
 - required by law to be treated as high risk²⁵³; or
 - involve assets or persons (natural and/or legal) which are resident or domiciled or incorporated in a specified territory.
- 163B. The enhanced due diligence measures that may be undertaken by financial institutions include:
- (a) Obtaining additional information on the customer (e.g. information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner;
 - (b) Obtaining additional information on the intended nature of the business relationship;
 - (c) Obtaining information on the source of funds or source of wealth of the customer;
 - (d) Re-checking or re-verification of information on the reasons for intended or performed transactions;
 - (e) Obtaining the approval of senior management to commence or continue the business relationship;
 - (f) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination; and
 - (g) any other measures that have a similar effect in mitigating risks.

164. In the case of complex, unusual, large transactions and/or unusual patterns of transactions which do not appear to have any economic benefit, the financial institution may require the first payment to be carried out through an account in the customer’s name with a bank subject to similar CDD standards.

*Introduced Business*²⁵⁴

165. Introduced business refers to cases where on the introduction/referral of a prospective customer, a financial institution relies, whether in whole or part, on the KYC/CDD procedures undertaken by another regulated financial institution. In circumstances where business is being introduced, the ultimate responsibility is on the recipient financial institution

²⁵¹ For clarity, reference here in this paragraph to risks is to inherent risk.

²⁵² The POC(MLP) Regulations amended 2019 — regulation 7A; The TP (Reporting Entities) Regulations amended 2019 — regulation 6A. This would also include a series of one-off transactions that create a pattern presenting indicators of ML/TF/PF/Risks.

²⁵³ The POC(MLP) Regulations amended 2019 — regulation 7 A; The TP (Reporting Entities) Regulations amended 2019 — regulation 6A.

²⁵⁴ POC (MLP) Regulations as last amended 2019, Regulations 7 and 12; TP (Reporting Entities) Regulations as last amended 2019, Regulations 5 and 12; FATF Recommendation 17.

to know the referred customer and his/her/its business and to establish the adequacy of the KYC/CDD details regarding this introduced business.

- 165A. Financial institutions may consider themselves entitled to rely on the identification procedures that the introducers have performed if the circumstances outlined in regulation 11 of the TPA (Amendment) Regulations 2019 and regulations 12(1)²⁵⁵ and 12(1)(A) of the POC (MLP) Regulations, 2019 are in place. At a minimum, financial institutions must, among other things:—
- (a) carefully consider the fitness and propriety of introducers and assess the adequacy of the customer identification and due diligence standards that the introducers maintain, and to which they are held, pursuant to the AML/CFT/CPF laws and framework which govern the introducer;
 - (b) be satisfied that introducers adhere to minimum “Know Your Customer” and “Customer Due Diligence” standards as identified within these Guidance Notes;
 - (c) be able to verify the due diligence procedures undertaken by the introducer at any stage and the reliability of the systems put in place to verify the identity, financial history and CDD details of the customer;
 - (d) be able to procure and review all the relevant identification data and other documentation pertaining to the customer’s identification, financial history, business dealings and other CDD data, either as soon as is reasonably practicable, or within fifteen (15) days, after the introduction;
 - (e) A financial institution’s compliance with this requirement will be assessed by the Supervisor based on the availability of the CDD & KYC information for review by the Supervisory Authority;
166. Whenever possible, the prospective customer must be interviewed; and where it has been determined that the information provided in relation to the customer is not adequate or the mechanism by which the information was obtained is deficient, then the financial institution must conduct its own CDD.
167. The information provided to the financial institutions must also be available to the BOJ as well as to the designated authority under the POCA and any other competent authority as may be warranted in the circumstances²⁵⁶.

Trust Accounts

168. Subject to paragraph 166, where an account is being opened by a trustee, settlor or grantor, pursuant to trust arrangements, the identity of all parties, beneficiaries and each beneficial owner or person who exercises effective control of the trust or other legal arrangement must be ascertained and recorded in keeping with the AML and CFT Regulations²⁵⁷. This would also include identification of the trustees, settlors and grantors, and each beneficial owner or person who exercises effective control of the trust or other legal arrangement account, source of wealth from which the proceeds of the trust or other legal arrangement are derived, as well as the source of funds involved in the transaction, and the purpose and details (i.e. terms) of the trust or other legal arrangement.

*Accounts Opened by Professional Intermediaries*²⁵⁸

169. Professional intermediaries generally include pension funds, unit trusts and other fund managers, as well as lawyers, securities dealers and stockbrokers managing single or pooled accounts held on deposit or in escrow for clients. A financial institution may rely on the professional intermediary’s due diligence process, but only where the professional intermediary is itself subject to and compliant in implementing an AML/CFT/CPF regulatory framework²⁵⁹.
170. Financial institutions should note that, notwithstanding the ability to place reliance on third party introductions, the statutory obligations under the law for identification of the customer and beneficial owners, is placed on the financial institution. Accordingly, the financial institution must ensure its procedures, policies and measures on CDD including those established to facilitate reliance on third party identification processes, are compliant with the AML/CFT laws and framework²⁶⁰ and allow for its undertaking the requisite CDD checks and verifications as may be necessary in the circumstances.
171. Financial institutions must be reasonably satisfied that where an account in the name of a professional intermediary is being held on behalf of one or more clients, that client is/those clients are subject to appropriate CDD including identification and source of funds verification and, the financial institution can either obtain confirmation of identification and other CDD related information for the beneficiaries of the accounts, or be in a position to confirm that such information can be retrieved on demand. The latter position is predicated on the POC (MLP) Regulations which only permit reliance on third parties where the third party is itself subject to an AML/CFT regulatory framework.

²⁵⁵ TP(Reporting Entities) Regulations, Regulation 12(1).

²⁵⁶ POC (MLP) Regulations 2007, regulation 14(1)(2) and (4) last amended in 2019.

²⁵⁷ POC (MLP) Regulations last amended in 2019, (r. 11, 12 & 13); — TP (Reporting Entities) Regulations (r. 11, 12 & 13).

²⁵⁸ POC (MLP) Regulations (r. 11, 12 & 13); TP (Reporting Entities) Regulations (r. 11, 12 & 13);FATF Recommendation 17.

²⁵⁹ The Attorney General (Appellant) v The Jamaican Bar Association (Respondent) (Jamaica) The General Legal Council (Appellant) v The Jamaican Bar Association (Respondent) (Jamaica). The Privy Council has ruled that the provision under POCA which requires attorneys to report suspicious actions by their client is justified and the regime does not breach constitutional rights. Therefore, the statutory obligations under POCA that apply to the regulated sector (namely financial institutions and designated non-financial institutions - R10, II, 12, 15, 18, 20, 21, and 24) apply to attorneys and enforcement of these obligations commenced in 2023.

²⁶⁰ See also Basel Committee on Banking Supervision - Sound management of risks related to money laundering and terrorist financing — January 2014 rev. July 2020 — Annex I — Reliance on third parties — Section II.

Private Banking/Private Wealth Management / Wealth Management / High-net-worth Clients

172. In particular, institutions that offer private banking services, (or similar services by whatever other name called), for high net-worth individuals, must ensure that enhanced due diligence policies and procedures are developed and clearly documented in the overall CDD policies and procedures to govern this area of operations. Senior management with ultimate responsibility for such operations shall ensure that the personal circumstances, income sources and sources of wealth of high-net-worth clients are known and verified as far as possible, and must also be alert to sources of legitimate third-party information. Whilst it is appreciated that efforts must be made to protect the confidentiality of high-net-worth clients and their businesses, these accounts must be available for review by the Supervisory Authority, (i.e. BOJ), the designated authority, and the financial institution’s internal compliance officers and internal and external auditors. The approval of these banking relationships must be obtained from at least one senior level officer, other than the private banking officer/relationship manager.

Transferring Clients

173. Where accounts are transferred from another financial institution, enhanced KYC/CDD standards shall be applied especially if the licensee has any reason to believe that the account holder has been refused banking facilities by the other financial institution or has had his/its relationship or facilities terminated by the other financial institution²⁶¹.

Politically Exposed Persons (PEPS)²⁶²

174. PEPs are individuals who are or have been entrusted with prominent public functions. The 2013 amendments to the POC (MLP) Regulations and TP (Reporting Entities) regulations define the category of persons who, in relation to any State, carry out functions analogous to any of the following, and includes their immediate family and close associates²⁶³—

- (i) heads of state or of government;
- (ii) a member of any House of Parliament;
- (iii) a Minister of Government;
- (iv) a member of the judiciary;
- (v) a military official above the rank of Captain;
- (vi) a member of the police of or above the rank of Assistant Commissioner;
- (vii) a Permanent Secretary, Chief Technical Director or chief officer in charge of the operations of a Ministry, department of Government, executive agency or statutory body;
- (viii) a director or chief executive officer of any company in which the Government owns a controlling interest;
- (ix) an official of any political party;
- (x) persons who hold, or have held, a senior management position in an international organization (i.e. senior management — directors, deputy directors, and members of the board or equivalent functions).

Middle ranking or more junior individuals in the foregoing categories are not expressly included in the designation or classification as PEP. However, as discussed further below, should it be known, revealed or discovered that these persons have the type of influence and/or the level responsibility for public assets and information akin to or exceeding that of the standard PEP, then the FI should consider assessing or re-assessing the risk profile of that individual and consider extending the PEP approach to that individual if the risk analysis suggests this is warranted.

Additional Considerations²⁶⁴

175. Given the risk assessment profile requirements under the AML/CFT/CPF regulations as well as the revised FATF Recommendations, a financial institution would not be precluded from extending the enhanced or heightened measures to persons who are not expressly reflected in the list at regulation 7A(6) of the POC (MLP) Regulations and at regulation 6A(6) of the TP (Reporting Entities) Regulations (such as former PEPs or middle ranking or junior officials acting in the name of, or on behalf of or for a PEP), if from a financial institution’s own risk assessment, the profile of the person warrants such an approach to be taken. It is expected that in such cases, such a profile would be reflective of any one or more of the following—

- (a) whether the individual is an elected representative or not,—
 - (i) the individual carries out functions of a public nature, which permit access (directly or indirectly) to public property (including funds or benefits — whether in cash or kind) and which give the individual the authority to make decisions or issue directives regarding the use of public property; and

²⁶¹ See section above on Introduced Business.

²⁶² See FATF Recommendation 12.

²⁶³ Parents, siblings, spouse, children and in-laws as well as close associates i.e. individuals who are business partners, or associated in any other form, in a common commercial enterprise are also included in requirement for enhanced scrutiny.

²⁶⁴ See also the Wolfsberg Principles for additional reading on the topic of ‘PEPs’. For eg. PEP FAQ states viz. “that, the following may also be considered to fall within the definition (of PEPs) but may be excluded in areas where the risk of corruption or abuse is considered to be relatively low as they do not have the ability to control or divert funds—

- Heads of Supranational Bodies (eg. UN, IMF, WB)
- Members of Parliament, or National Legislatures, senior members of the Diplomatic Corps. Eg. (Ambassadors, Ch’arges D’ Affaires, Members of the Boards of Central Banks)”

- (ii) the function undertaken by the individual exists in relation to an environment in which the risk of corruption or abuse is considered to be very high (e.g. little or no established procedures or protocols that are designed to implement stringent internal controls and accountability measures; absence of effective disciplinary sanctions or a framework which does not include penalties that are effective, proportionate and dissuasive);
- (b) the individual’s prominence or position (as a prominent public figure)—
 - (i) facilitates the ability to influence or control (directly or indirectly) the access to and/or use of public property (including funds or benefits — whether in cash or kind); or
 - (ii) the individual is either known to be corrupt or is suspected of being corrupt, or the individual’s name is associated with incidences of corruption or abuse; or
 - (iii) the individual meets the criteria of a close associate of a person at a, or b, above. It should be noted that a person who qualifies for classification as a PEP can remain subject to a “PEP” based risk profile even after his/her appointment ends or is terminated, as the basis for such treatment would be based on risk and not on prescribed time limits.²⁶⁵

Using a risk-based approach presumes that based on the risk assessments conducted, a financial institution would not be precluded from applying commensurate measures (for persons previously meeting the category of a PEP) where the risk assessment confirms that the profile of the person warrants such an approach to be taken. In relation therefore to those specified categories of persons who meet the definition of a PEP as articulated at Regulations 6A and 7A of the AML/CFT Regulations, applying reduced, lenient or measures other than enhanced due diligence measures, shall not occur unless that approach is specifically permitted in the AML/CFT laws.

176. Financial institutions shall not establish business relationships with PEPs if the financial institutions know or have reason to suspect that the funds are derived from corruption or misuse of public assets. Senior management approval must also be obtained to continue an existing relationship with a person who becomes a PEP after the establishment of the relationship or whose status as a PEP is confirmed, realized or discovered subsequent to the establishment of the relationship. Senior management must ensure that the personal circumstances, income sources and sources of wealth of PEPs are known and verified as far as possible and shall also be alert to sources of legitimate third-party information. Whilst it is appreciated that efforts must be made to protect the confidentiality of PEPs and their businesses, these accounts must be available for review by the supervisory authority, the designated authority, and the financial institution’s internal compliance officers (including the Nominated Officer²⁶⁶) and internal auditors. The approval of business relationships involving PEPs must be obtained from at least one senior level officer, other than the banking officer/relationship manager.
177. To mitigate the significant legal and reputational risk exposures that financial institutions face from establishing and maintaining business relationships with PEPs, or continuing existing business relationships with PEPs, the following procedures must be followed prior to the commencement or continuation of such relationships:—
- (a) Information gathering forms/procedures shall be structured to reasonably allow the financial institution to ascertain whether a client is a PEP and to identify persons and companies/business concerns clearly related to or connected with the PEP. The financial institution shall also access publicly available information to assist in the determination as to whether or not an individual is a PEP;
 - (b) Obtain all the relevant client identification information as would be required for any other client prior to establishing the business relationship or to continuing the business relationship. Additionally, the decision to open an account for a PEP or to continue the relationship with a PEP must be taken at the senior management level;
 - (c) Assess the nature of the individual’s obligations and establish a risk profile for that individual. Even within a designation of ‘high risk’ it is possible that the specific circumstances of the individual can serve to either substantially mitigate the risks associated with being a PEP, or exacerbate those risks;
 - (d) Investigate and determine the income sources prior to opening a new account. Reference to income sources includes — source of funds; source of wealth and asset holdings; confirmation of the general salary and entitlements for public positions akin to the one held by the customer in question.
178. Following the commencement of banking relationships, there shall be:—
- (a) Regular reviews of customer identification and due diligence records commensurate with the risk profile²⁶⁷; and
 - (b) Ongoing monitoring of PEP accounts.
179. The abovementioned procedures shall also be followed for the ultimate beneficial owners of bodies corporate or legal arrangements who are confirmed to be PEPs, as well as for the existing²⁶⁸ client base to ensure that all current PEPs have been so identified and remain subject to enhanced customer due diligence processes²⁶⁹.

²⁶⁵ FATF Guidance on Politically Exposed Persons (R12 and 22) June 2013, “B” Time Limits of PEPs Status, paragraph 44, page 12.
²⁶⁶ See Regulation 5 of the POC (MLP) Regulations 2007 as amended in 2019 and section VI of these Guidance Notes.
²⁶⁷ POCA (MLP) Regulations, 2007 r. 7(1)(c).
²⁶⁸ POCA (MLP) Regulations, 2007 r. 19.
²⁶⁹ FATF Guidance on Politically Exposed Persons (R12 and 22) June 2013.

Non-face-to-face Customers/Remote On-boarding

180. Given the digital direction for the provision of services generally including financial services, where activities comprising financial transactions including opening or closing of accounts, extending additional services to existing customers, varying delivery channels for services etc., are executed or facilitated on a non-face-to-face basis, financial institutions must ensure that the standards of scrutiny applied to such non-face-to-face activities, appropriately address the risks of so proceeding. For e.g. the use of remote onboarding systems or programmes, or onboarding customers via online methods, whereby the user signs up through the financial institution's service using their own device, providing their details, must meet the CDD standards, including independent verification by a reputable third party²⁷⁰. There must be employment of mechanisms that allow for irrefutable confirmation that the person conducting the transaction or establishing the relationship is the intended applicant for business or customer.

At a minimum, financial institutions shall ensure that:—

- (a) Prior to the implementation of any initiative to facilitate or accommodate doing business with customers on a non-face-to-face basis, financial institutions should conduct ML/TF risk assessments in line with these Guidance Notes, and thereafter, monitor and manage the effectiveness of the technology adopted on an ongoing basis;
- (b) Any technology solution adopted for conducting transactions on non-face-to-face basis must at least be as robust as those steps undertaken when the customer is in front of the staff at the financial institution, such as:
 - i. identity authentication -where the measures applied satisfy the FI of the reliability of the document, data or information obtained for the purpose of verifying the customer's identity; and
 - ii. adequately link the customer to the identity provided in (a).

It may also be necessary for financial institutions to increase the number and timing of controls and checks applied during the course of the business relationship including selecting patterns of transactions that will be subject to further examination.

Emerging Technology²⁷¹

181. Financial institutions must proactively assess the AML/CFT/CPF risks posed by emerging technologies (for instance, in the use of new payment products and services) and design customer identification and verification procedures with due regard to such risks²⁷².
- (a) New payment products and services (NPPS) are described in the related FATF Guidance²⁷³ as new and innovative payment products and services that offer an alternative to traditional financial services, and which involve new ways of initiating payments through, or extending the reach of, traditional retail electronic payment systems, as well as products that do not rely on traditional systems to transfer value between individuals or organisations.
 - (b) Based on the FATF definition of a 'financial institution', the providers of NPPS fall within that definition where the activity occurs through conducting money or value transfer services, or through issuing and managing a means of payment, and according to FATF, should therefore be subject to AML/CFT/CPF preventive measures including CDD, record keeping and reporting of suspicious transactions.

Please further note that amendments to the PSCA are currently being pursued to provide the Bank with additional powers over payment service providers (non-DTIs). The proposed legislative amendments include a comprehensive definition of payment service providers and payment services which once enacted will be reflected in the relevant update to the Guidance Notes.

Under the BSA, NPPS activities would be captured under the definition of financial services which includes the activities of the transfer of money or value and the issue of electronic money.

- (c) Further considerations raised by FATF are that the provision of NPPS:—
 - (i) Usually requires a complex infrastructure involving several parties for the execution of payments. This raises a particular concern when it is not, or cannot be clearly established which of the entities involved is subject to AML/CFT/CPF obligations and subject to complying with those obligations and which country is responsible for regulating compliance with those obligations;
 - (ii) Sometimes involve the use of agents and reliance on unaffiliated third parties for establishing customer relationships and reloading services which can increase ML/TF/ PF risks particularly if the information collected is not shared with the entity responsible for AML/CFT/CPF requirements;
 - (iii) Often involve entities from sectors such as Mobile Network Operators (MNOs) which are unfamiliar with AML/CFT/CPF controls and whose CDD could be limited in comparison to, for e.g. the traditional banking sector and in respect of which, the chain of information could create difficulties for tracing the funds involved for e.g. the chain of information for

²⁷⁰ Refer to POC (MLP) Regulations, regulations 7 & 12; TP (Reprting Entities) Regulations, regulations 5 & 12.
²⁷¹ FATF Recommendation 15.
²⁷² See Appendix IX re BOJ's Advisory on Cyber Risk.
²⁷³ FATF Guidance on prepaid Cards, Mobile Payments and Internet-Based Payment Services, June 2013, para 3 pg 4.

- a single transaction could involve more entities, some of which may be located in different countries, (In Jamaica, MNOs tend to have major operations on a global basis, and are subject to a regulator whose primary focus is ‘market conduct’); and
- (iv) Generally involve the maintenance of bank accounts which are used for periodic transactions to settle accounts with agents and MVTs Partners, The issue here is that while a bank settling wholesale transactions between NPPS providers has CDD obligations in relation to the NPPS provider, it has no, or limited visibility into the NPPS providers’ customers and is unable to oversee transactions between the NPPS providers and their customers.
- (d) The FATF Guidance reflects that examples of emerging new payment methods include:
- (i) Prepaid cards, mobile payments, and internet-based payments (including virtual assets). For these activities the risks of ML/TF are increased by the anonymity that can occur when these products are being purchased, registered, loaded, reloaded, or used by the customer. These risks are also increased where cash funding, loading or reloading is possible otherwise than through a bank account for example via the internet, or where the technology permits, access benefits are passed on to third parties unknown to the issuer or can facilitate third party remittances. Products and mechanisms with cash and non-bank payment options open up the payment system access and also obscure the origin of the funds. It is also recognized that the compact physical size of prepaid cards increases the vulnerability of these products being used to conduct cross-border transfer of funds i.e. a discreet number of cards that have accounts loaded with high fund values which cannot be determined from the card itself as against transporting large, bulky amounts of cash using cash couriers. The foregoing risks are recognized as being relative to the functionality of the product or mechanism and the existence of AML/CFT/CPF risk mitigating measures such as funding or purchasing limits, reload limits, cash access limits and restricting the ability for the product or mechanism to be used outside the country of issue.
182. Given the foregoing, the NPPS that are high risk and which must be subject to enhanced due diligence measures are NPPS for which any one or more of the following characteristics is present:—
- (a) Where ‘airtime’ funds can be transferred and are accepted for payments or as an alternative currency; or
 - (b) Where the NPPS is functionally similar to that of a bank account due to the presence of one or more of the following features:
 - (i) the NPPS can be reloaded an unlimited number of times;
 - (ii) no funding limits or very high funding, loading or spending limits are envisaged;
 - (iii) it is possible to make and receive funds transfers cross-border, and within the country where product is issued;
 - (iv) the NPPS can be funded through cash, and cash can be withdrawn through the ATM network;
 - (v) the ability to add or withdraw funds to the account using cash or cash equivalents, whether directly or through another provider or intermediary;
 - (vi) using agents or unaffiliated third parties to establish customer relationships particularly where the CDD information is not shared or is not available to, or accessible by, the party with the AML/CFT/CPF responsibility;
 - (vii) segmentation of the service where one or more unaffiliated third parties are relied on for establishing customer relationships, the issuance or redemption of the currency involved.
183. The risks associated with the offer of NPPS may be managed with the application of certain risk mitigating characteristics such as:—
- (a) loading solely from a bank account;
 - (b) absence of funding through third parties;
 - (c) clear establishment and confirmation of the party/(ies) with the AML/CFT/CPF responsibilities and the country with AML/CFT/CPF responsibility (i.e. AML/CFT/CPF obligations are statutorily imposed; carry effective, proportionate and dissuasive sanctions for breaches and are equivalent or reflect a higher standard than the AML/CFT laws in Jamaica);
 - (d) the NPPS party is responsible for handling all aspects of the customer relationship (i.e. registration, cash-in/cash-out and transactions) and has AML/CFT/CPF responsibility as described above and is subject to regulatory oversight through a mechanism of licensing or registration; (e.g. a NPPS (which operates a MVTs or as a means of payment) who is also a designated FI under the POCA);
 - (e) functionally the following risk mitigating characteristics are incorporated—
 - (i) CDD Recordkeeping;
 - (ii) Value limits/thresholds;
 - (iii) Geographical limits;

- (iv) Usage limits (e.g. limiting the product to the acquisition of certain goods and services; application of transaction monitoring features;); and
 - (v) Usage safeguards (such as requiring unique identifier information to proceed with a transaction)
- 184. Where there are multiple entities involved in the provision of the NPPS or service, and it is not clear which entity is the provider, the following factors can be applied in deeming a party the appropriate NPPS provider(s):
 - (a) the entity which has visibility and management of the NPPS;
 - (b) the entity which maintains relationships with customers;
 - (c) the entity which accepts the funds from customer, and
 - (d) the entity against which the customer has a claim for those funds.

Virtual Assets²⁷⁴ (“VAs”) and Virtual Asset Service Providers (VASPs)

185. The Revision to FATF Recommendation 15, requires that virtual asset service providers, (VASPs) be regulated for AML/CFT purposes. Countries are therefore required to apply the relevant measures under the FATF Recommendations to virtual assets (VAs) and VASPs where operating within their jurisdiction. Currently, Jamaica has no legislative framework for VAs and VASPs and FIs are not in the business of providing these services. These sections on VAs and VASPs are being provided for information purposes and FIs should be reminded of their duty to identify and continually assess and be aware of any ML/TF risk exposures to virtual assets and new or developing technologies and payment channels²⁷⁵.

- 185A. Based on the FATF definition and FATF (Revised) Guidance on the Risk Based Approach to VAs and VASPs, a VA is a digital representation of value that is capable of inherently being used for payment or investment purposes and which can also be digitally traded or transferred. The VAs that do not inherently have the capability of functioning or being used for payment or investment purposes or being digitally traded or transferred are not the target of FATF R15. If therefore for e.g. the digital asset in essence is solely a declarative record of ownership or other position in a financial asset, then FATF does not require the definition of VA or the attendant VA related framework to be extended to that digital asset. Accordingly, based on the FATF Recommendations the term VA does not include digital representations of fiat currencies, securities or of any other financial assets.

It should also be noted that FATF does not intend for an asset to be treated as both a traditional financial asset and a VA. If therefore, based on a country’s framework, an asset is defined as a financial asset and is subject to the attendant legislative safeguards and regulatory regimes that FATF has outlined should apply to such assets, (including proper coverage under a country’s AML/CFT regulatory framework), then there is no expectation under the FATF Recommendations, for that asset to also be subject to a VA framework²⁷⁶. In this regard FATF seeks to ensure its Recommendations remain technology neutral.

186. The Glossary in the FATF Recommendations, defines a VASP as any natural or legal person which as a business conducts any of the following activities 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) Transfer²⁷⁷ 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.

- 186A. VASPs include VA exchanges and transfer services; some VA wallet providers, such as those that host wallets or maintain custody or control over another person’s VA’s wallet(s), and/or private key(s); providers of financial services relating to issuance, offer, or sale of a VA (such as in an Initial Coin Offering); and other possible business models.

- 186B. Based on the FATF definition of VASPs and discussion of VASP activities, existing activities or services in Jamaica’s banking system that could seem to be captured by such definitions include—
 - (i) The issuers of CBDCs
 - (ii) Operators of ATMs or ABMs

However, based on the discussions at paragraphs 38A-B and 185A above, Jamaica’s CBDC (officially JAMDEX) which functions solely as the digital representation of fiat currency in the banking system does not meet the definition of a VA as contemplated by the FATF Recommendations.

²⁷⁴ FATF Updated Guidance for a Risk-based Approach to Virtual Asset and vertical Service Providers, October 2021.
²⁷⁵ Recommendation 15, 15.1.
²⁷⁶ FATF Updated Guidance- A Risk-based Approach to Virtual Assets and Virtual Asset Service providers, October 2021 para 48-49.
²⁷⁷ Transfer means to conduct a transaction that moves a virtual asset from a VA address or account to another.

Similarly, unless and until the existing ATMs and ABMs are confirmed as being configured to accommodate the activities outlined in paragraph 186 (a), (b) and/or (c) above, and is actually accommodating such transactions with virtual assets, such ATMs and ABMs also would not meet the criteria to be defined or treated as VA.

Additionally, the FATF Guidance²⁷⁸ reflects that engaging in virtual asset services “*as a business*” is meant to exclude those who may carry out a function on a very infrequent basis for non-commercial reasons from coverage as VASPs. To satisfy this portion of the definition of a VASP, the entity must carry out this function for or on behalf of another natural or legal person as opposed to on behalf of itself, for commercial reasons, and must do so on at least a sufficiently regular basis, rather than infrequently. The Guidance also reflects that conducting a virtual asset service includes activities amounting to the provision or active facilitation of the service, which refers to the active involvement in the provision of the services outlined at paragraphs 186(a)-(d) above. Ancillary participants that do not engage in the provision or active facilitation of a VA service (e.g. Internet or Cloud services) are not intended to be captured.

187. Virtual assets are neither issued nor guaranteed by any jurisdiction, and functions only by agreement within the community of users of the virtual assets. Virtual assets are distinguished from fiat currency (a.k.a. “real currency,” “real money,” or “national currency”), which includes central bank digital currency that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency.²⁷⁹ E-money is a digital transfer mechanism for fiat currency - i.e., it electronically transfers value that has legal tender status.
- 187A. The FATF Guidance further reflects that virtual assets’ global reach likewise increases its potential for ML/TF/PF risks. Virtual Assets systems can be accessed via the internet (including via mobile phones) and can be used to make cross-border payments and funds transfers. In addition, virtual assets commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear. Moreover, customer and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them. This problem is exacerbated by the rapidly evolving nature of decentralized virtual assets technology and business models, including the changing number and types/roles of participants providing services in virtual assets payments systems, and importantly, components of a virtual assets system may be located in jurisdictions that do not have adequate AML/CFT/CPF controls. Centralized virtual assets systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT/CPF regimes. Decentralised convertible virtual assets allowing anonymous person-to-person transactions may seem to exist in a digital universe entirely outside the reach of any particular country²⁸⁰.

Virtual Currencies

- 187B. Virtual currency can be traded on the internet and are generally characterized by non-face-to-face customer relationships, and may permit anonymous funding (cash funding or third-party funding through virtual exchangers or related business that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified²⁸¹. Therefore, transfers using VC with limited or no information on the originator and beneficiary may present money laundering, terrorist financing and proliferation financing (ML/TF/PF) risks and other crime risks that must be identified and mitigated.
188. Using a risk-based approach presumes that based on the risk assessments conducted, a financial institution would not be precluded from providing relaxed measures for NPPS if the risk assessment confirms that the profile of the product or service or mechanism warrants such an approach to be taken and the appropriate risk mitigating measures are implemented. It should be noted that FATF recommends that the risks posed by NPPS should be identified, assessed and understood before financial institutions seek to establish their CDD processes and procedures and prior to the launch of such services products or mechanisms. This means looking at the ML/TF/PF risks while the product, service or mechanism is still in its project phase and designing said product, service or mechanism in such a way that the vulnerabilities are kept to a minimum.²⁸²

In conducting transactions that fall within the parameters of the Electronic Transactions Act, financial institutions must bear in mind the provisions of this Act particularly those treating with the issue of electronic signatures (See section 8 “Requirements for signature”). Financial institutions should also bear in mind that Jamaica has legislation in place treating with Cybercrimes²⁸³ and lotto scamming²⁸⁴ activities and must be cognisant of the obligations and offences described in these pieces of legislation.

²⁷⁸ FATF Updated Guidance -A Risk-based Approach to Virtual Asset and Virtual Asset Service Providers, October, 2021 (paragraphs 59 and 60).

²⁷⁹ Bank of Jamaica issued Jam-Dex, central bank digital currency (“CBDC”), IN 2022. see <https://boj.org.jm/wp-content/uploads/2022/08/CBDC-FAQs-Booklet.pdf>.

²⁸⁰ FATF Guidance for a Risk-Based Approach to Virtual Currencies, June, 2015, Appendix A “Potential AML/CFT Risks”. Virtual assets is a complex subject that implicates other regulatory matters, including consumer protection, prudential safety, tax and soundness regulation, and network IT security standards.

²⁸¹ Ibid.

²⁸² FATF Guidance fora risk-based approach to Prepaid Cards, Mobile Payments and Internet-Based NPPSs, June 2013 -paragraphs 61 and 62.

²⁸³ The Cybercrimes Act, 2015, see paragraph 46.

²⁸⁴ The Law Reform (Fraudulent Transactions) (Special Provisions) Act, 2013, see paragraph 45.

- 188B. In February 2018²⁸⁵ Bank of Jamaica published on its website, a statement on virtual currencies and published a reminder statement in July 2021²⁸⁶. These statements advise caution to the general public in interacting with VCs and highlight the following:
- Virtual currencies are not legal tender in Jamaica
 - The public should exercise caution in interacting with VCS due to the various risks surrounding same to include:—high volatility causing significant fluctuation in value, the use to facilitate criminal activities, higher degree of cyber-fraud/hacking and the settlement risks that may arise as tis currency is not issued or backed by a central bank or monetary authority.

*Correspondent Banking*²⁸⁷

189. Correspondent banking²⁸⁸ refers to the provision of banking services by one bank (the correspondent bank) to another (the respondent bank/other financial entity). The arrangement is used by respondent banks throughout the world to conduct business and access services (such as cash management; international wire transfers, cheque clearing, payable through accounts and foreign exchange services) that they cannot offer directly because of the lack of an international network²⁸⁹.

- (a) Generally, for a correspondent bank, the risks associated with this activity arise:—
- (i) where the respondent entity has no physical presence in the jurisdiction in which the correspondent bank is located; and
 - (ii) usually because the correspondent bank processes or executes transactions for customers of the respondent but does not generally have direct business relationships with the customers of the respondent bank, as well as the limited information available regarding the nature or purposes of the underlying transactions.
- (b) Correspondent banking relationships must therefore generally be subject to the appropriate risk assessment being undertaken in relation to for instance:
- (i) The jurisdiction in which the respondent entity is located;
 - (ii) The group to which the respondent entity belongs and the jurisdictions in which the subsidiaries and branches of the group may be located;
 - (iii) Information about the respondent entity’s management and ownership (especially the presence of beneficial owners), its reputation, major business activities, its customers (including target market) and their locations;
 - (iv) The purpose of the services requested by, or to be provided to, the respondent entity;
 - (v) Intended usage of the account by the respondent entity, e.g. to provide onward correspondent banking services to its own customers, ability of the customers of the respondent entity to directly access the account held by the correspondent bank, to address own corporate or settlement purposes, intended third party usage of the account, to accommodate, facilitate or extend ‘nested relationships’²⁹⁰ or payable through accounts;
 - (vi) The quality of the AML/CFT/CPF policies and procedures of the respondent bank (and the CDD applied by the respondent bank to its customers);
 - (vii) Compliance status with regulatory, prudential and national AML/CFT/CPF requirements and global AML/CFT/CPF standards;

²⁸⁵ [public_awareness_statement_re_virtual_currencies_1.docx](#)

²⁸⁶ [Bank of Jamaica Reminder Caution on Cryptocurrencies » Bank of Jamaica](#)

²⁸⁷ See FATF Recommendation 13.

²⁸⁸ An example of a correspondent arrangement gone bad - Re: Bank of New York (BONY) Derivative Complaint (Case No. 99 Civ. 10616 (DC) (Con.)) -Amongst the transgressions alleged is that “...Although contemporaneous government, press, and private-sector sources had sounded unmistakable warnings that Russia’s nascent private banking system was being infiltrated by organized crime, the BONY Board intentionally or recklessly failed to assure itself that BONY had implemented an adequate and independent system of monitoring and control of its correspondent wire transfer business and Eastern European business operations.”

²⁸⁹ Basel Committee on Banking Supervision - Sound Management of Risks Related to ML and TF, January 2014 rev July 2020 - Annex 2 - general considerations on cross-border correspondent banking.

²⁹⁰ The use of a bank’s correspondent relationship by a number of respondent banks through their relationships with the bank’s direct respondent bank to conduct transactions and obtain access to other financial services. Basel Committee on Banking Supervision - Sound Management of Risks Related to ML and TF, January 2014 rev July 2020 - Annex 2 -general considerations on correspondent banking.

- (viii) The ability to obtain from the respondent bank, the identity of any third party/parties that will be entitled to, or will be accessing or using the correspondent banking services²⁹¹; and
 - (ix) The potential use of the account by other respondent banks in a “nested” correspondent banking relationship.
- (c) Financial institutions must therefore apply appropriate levels of due diligence by gathering sufficient information from and performing enhanced due diligence processes on proposed respondent banks/ or entities prior to setting up correspondent accounts. This shall, at a minimum include:—
- (i) Obtaining authenticated/certified copies of Certificates of Incorporation and Articles of Association (and any other company documents to show registration of the institution within its identified jurisdiction of residence);
 - (ii) Obtaining authenticated/certified copies of banking licences or similar authorization documents, as well as any additional licences needed to deal in foreign exchange;
 - (iii) Confirming the supervisory authority which has oversight responsibility for the respondent bank and its compliance with regulatory, prudential and AML/CFT/CPF obligations;
 - (iv) Determining the ownership of the respondent bank or entity;
 - (v) Obtaining details of the respondent bank’s/ or entity’s board and management composition;
 - (vi) Determining the location and major activities of the respondent bank/ or entity;
 - (vii) Obtaining details regarding the group structure within which the respondent bank/ or entity may fall, as well as any subsidiaries it may have;
 - (viii) Obtaining proof of its years of operation, along with access to its audited financial statements (for the last 5 years if possible);
 - (ix) Ascertaining the respondent bank’s/or entity’s external auditors;
 - (x) Ascertaining whether the respondent bank/ entity has established and implemented sound customer due diligence, anti-money laundering, anti-terrorism financing and anti-proliferation financing policies and strategies and appointed a Compliance Officer (at senior management level), inclusive of obtaining a copy of its AML/CFT/CPF policy, procedures and guidelines;
 - (xi) Ascertaining whether the respondent bank has in the previous 7 years (from the date of the commencement of the business relationship or negotiations therefore), been the subject of or is currently subject to any regulatory action or any AML/CFT/CPF prosecutions or investigations. Primary sources from which this information can be sought and ascertained include the Banking Regulatory Authority for the jurisdiction in which the respondent bank is resident. Information may also be available from the respondent bank’s website as well as published information such as the AML/CFT/CPF Mutual Evaluation Reports;
 - (xii) Ascertaining that the respondent banks/or entities do not permit their accounts to be used by shell banks. In this regard a correspondent bank would also need to pay attention to the following indicators:—
 - 1. whether the respondent bank/or entity provides intermediary services to its customers such as “payable through accounts”²⁹², nested relationships or other third-party type access to the correspondent accounts. This would be one likely way in which respondent shell banks could take advantage of correspondent banks;

²⁹¹ Financial institutions should be aware that Section 319(B) of the USA Patriot Act requires that financial institutions maintain records of the owners and the US agents of foreign respondent banks. Subsection (k) also authorizes the relevant authorities in the US to issue a summons or subpoena to any foreign financial institution that maintains a correspondent account in the US and to request records relating to such account, including records maintained outside the US-relating to the deposit of funds into the foreign bank. If a foreign bank fails to comply with or contests the summons or subpoena, any financial institution with which the foreign bank maintains a correspondent account must terminate the account upon receipt of notice from the authorities. Section 313 of that Act prohibits US banks from establishing correspondent banking relationships with shell banks. Financial institutions also need to be particularly mindful of the requirements of the USA Patriot Act, which effected several changes to the anti-money laundering and terrorist financing provisions of that country’s Bank Secrecy Act.

²⁹² According to the FATF (Revised) Interpretive Note to Recommendation 13, the term ‘payable-through accounts’ refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

The USA PATRIOT Act Section 311 (1) BANK DEFINITIONS (C) defines PAYABLE-THROUGH ACCOUNT- “as an account, including a transaction account (as defined in section 19(b)(1)(C) of the Federal Reserve Act), opened at a depository institution by a foreign financial institution by means of which the foreign financial institution permits its customers to engage, either directly or through a sub-account, in banking activities usually in connection with the business of banking in the United States.”

Section 19(b) 1(C) - The Federal Reserve Act

- (C) The term “transaction account” means a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others. Such term includes demand deposits, negotiable order of withdrawal accounts, savings deposits subject, to automatic transfers, and share draft accounts.)

2.

the respondent bank’s inability or reluctance to provide ultimate beneficiary/customer information in relation to pooled arrangements or collective investment schemes or aggregate accounts whereby only the KYC on the agent of the beneficiaries of the pooled arrangement, collective investment scheme or aggregate account will be or can be provided by the respondent bank;
3.

the country in which the respondent bank resides; (see note on countries with inadequate AML/CFT/CPF frameworks and the Specified Territories Notice issued by BOJ). Jurisdictions with CDD information or which laws secrecy laws that prohibit the release of any present an obstacle to the CDD process may pose a particular problem in this regard.
- (xiii)

Establishing the purpose and interested and expected usage of the correspondent account;
- (xiv)

Documenting the respective responsibilities of each institution in the operation of the correspondent account;
- (xv)

Identifying any third parties that may use the correspondent banking services; (in this regard the correspondent bank must be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank and that the respondent bank is able to provide relevant CDD information to the correspondent bank, on request²⁹³) and
- (xvi)

Ensuring that the approval of senior management is obtained for the account to be opened.
190.

Jamaica currently does not provide correspondent banking services; financial institutions should note however that in the event that correspondent banking services are provided then the financial institution will need to be bear in mind the matters outlined above.

Respondent Bank/Entity

191.

Equally important is the respondent bank’s/ or entities obligation to ensure that the institution identified to provide correspondent banking services is a reputable one, properly constituted and appropriately regulated. Financial institutions in their role as prospective respondent banks/or entities, shall therefore also note that similar assessments and the due diligence outlined above shall be undertaken in relation to the identification of appropriate or suitable entities with which correspondent banking relationships will be established. For respondent banks/or entities the risk associated with being a respondent bank/or entity, appear primarily to arise with:—
- (a)

Establishing a relationship with a correspondent bank which has a poor AML/CFT/CPF history and track record and which is subject to sanctions that may result in the funds and other assets held by that entity being frozen which can adversely impact the services of the respondent bank/or entity to its customers as well as the reputation of the respondent bank/or entity in being associated with such a correspondent bank;
- (b)

Establishing a relationship with an entity which is not licensed; or which has a poor history of regulatory compliance;

“The arrangement comprising a “payable thru” account usually involves an account service offered by a US banking entity to foreign banks. That is the US banking entity opening a checking account for the foreign bank, and the foreign bank then soliciting customers that reside outside of the US who for a fee, are provided the means to conduct banking transactions in the US through the foreign bank’s account at the US banking entity. Typically, the foreign bank will provide its customers (‘sub-account holders’), with cheques to enable them to draw on the foreign bank’s account at the US banking entity.” (See FDIC Guidelines on Use of Payable Through Accounts — March 30, 1995, <http://www.fdic.gov/news/news/financial/1995/fi19530.html>).

US banking entities are mandated to ensure that where payable through account services are provided they—

➤

Must be able to sufficiently identify the ultimate users of its foreign bank customers’ payable through accounts, including obtaining (or having the ability to obtain) in the US substantially the same type of information on the ultimate users as the US banking entity obtains for its domestic customers;

➤

May be required to review the foreign bank’s own procedures for identifying and monitoring sub-account holders as well as the relevant AML statutory and regulatory requirements with which a foreign bank must adhere in relation to customer –related transactions;

➤

Should terminate the payable through arrangement with the foreign bank as quickly as possible where—

1.

Adequate information on the ultimate users of the payable through account cannot be obtained; third-party type access to the correspondent accounts. This would be one likely way in which respondent shell banks could take advantage of correspondent banks;

2.

the respondent bank’s inability or reluctance to provide ultimate beneficiary/customer information in relation to pooled arrangements or collective investment schemes or aggregate accounts whereby only the KYC on the agent of the beneficiaries of the pooled arrangement, collective investment scheme or aggregate account will be or can be provided by the respondent bank;

3.

the country in which the respondent bank resides; (see note on countries with inadequate AML/CFT/CPF frameworks and the Specified Territories Notice issued by BOJ). Jurisdictions with secrecy laws that prohibit the release of any CDD information or which laws present an obstacle to the CDD process may pose a particular problem in this regard.

²⁹³ FATF (Revised) Recommendations, August 2024, Recommendation 13 sub-criterion 13.2(b).

- (c) Unexpected loss of the correspondent relationship due to the perception that the respondent bank/ or entity is either not AML/CFT/CPF compliant, or poses an unacceptable risk to the correspondent bank which can have adverse reputation and operating implications for the respondent bank/ or entity.

Shell Banks²⁹⁴

192. The FATF Recommendations last updated February, 2025 reflect that countries should not approve or accept the establishment or continued operation of shell banks and that countries should refuse to enter into or continue a correspondent banking relationship with a shell bank. FATF defines a ‘shell bank’ as “*a bank that has no physical presence²⁹⁵ in the jurisdiction in which it was incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.*”
- (a) The BSA, Section 11 prohibits operating as, or having dealings of any kind with, a shell bank. The definition in the BSA of shell banks also reflects that ‘physical presence’ is not established by the existence of any one of the following—
 - (i) the appointment of a local agent or the employment of non-managerial level staff;
 - (ii) the presence of resident staff who do not direct the policy and strategy of the bank; or
 - (iii) the establishment of the bank solely or principally by virtual means.

The definition also recognises the power of the Supervisor of banks, financial holding companies and other specified financial institutions, to deem an establishment as one that is consistent with establishment of a shell bank.

- (b) To be deemed as having a “physical presence”, a financial institution must therefore:
 - (i) Be physically located (i.e. “brick and mortar” presence) at a fixed address in the country in which it has been licensed to do banking business. This fixed address implies establishment of presence otherwise than by a post office box or electronic address;
 - (ii) Have mind and management located within the Country of operation. (The existence only of a local agent or of non-managerial staff or of staff not authorized or empowered to make decisions and bear legal responsibility for the daily operations of the location does not constitute physical presence²⁹⁶);
 - (iii) Maintain operating records relating to its banking activities at its fixed address;
 - (iv) Be subject to inspection by the banking authority by which it has been licensed;
 - (v) If the entity is a part of a financial group then that must also be a regulated financial group that is subject to effective consolidated supervision.
- (c) Financial institutions must undertake the required due diligence (see paragraph 189 above) to ensure that correspondent relationships are not established or continued with shell banks.

Countries With Inadequate AML/CFT/CPF Frameworks²⁹⁷

193. As earlier indicated in these Guidance Notes in Sections III, IV & V, the law requires financial institutions to exercise added care when dealing with clients residing in countries with weak or non-existent laws and regulations to detect and prevent money laundering and terrorist financing, or the financing of proliferation of weapons of mass destruction.

The POCA²⁹⁸ requires regulated businesses to apply enhanced due diligence for all business relationships and transactions with customers, resident, domiciled or incorporated in territories specified by the Supervisory Authority by Notice published in the Gazette. The requirement is Jamaica’s effort to comply with Recommendation 19 of the FATF Recommendations. Recommendation 19 states:

Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. ALSO, they should be able to apply countermeasures independently of any call by the FATF to do so. The countermeasures should be effective and proportionate to the risks.

A copy of the requisite Specified Territories Notice that was issued by BOJ can be found at Appendix VII to these Guidance Notes.

- 193A. Accordingly, a financial institution’s assessment and risk-based approach regarding the countries flagged or identified as posing AML/CFT/CPF risks shall be clearly outlined in the financial institution’s policy manual and updated whenever necessary.

²⁹⁴ FATF Recommendations 13 and 26 where the prohibition from operating as or dealing with a shell bank is discussed.
²⁹⁵ Physical presence is further defined in the Recommendations as meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.
²⁹⁶ Ibid.
²⁹⁷ See FATF Recommendation 19.
²⁹⁸ POCAA(2-19) Section 5 which incorporated Section 94A.

In identifying these jurisdictions, financial institutions may refer to the FATF’s website to access:

- (i) the list of countries, which have been identified as having strategic deficiencies in their AML/CFT/CPF frameworks (publication on the website in this case is otherwise known as a country on the FATF “Grey List”) and
- (ii) the list of countries for which the FATF has extended a call to the global network, for countermeasures to be applied) (publication on this list is known as the country being Blacklisted”).

Bank of Jamaica will also in writing, periodically update its licensees based on advisories received from the FATF and from the CFATF, and on advisories received from the United Nations (through the Ministry of Foreign Affairs and Foreign Trade and/or the Office of the DPP).

194. The commencement of business relationships with clients residing in countries with inadequate frameworks must be subject to the CDD processes discussed above in Section V and must have the prior approval of senior management. FATF indicated that possible countermeasures countries can employ to mitigate the risks the following²⁹⁹—

- (a) Requiring financial institutions to apply specific elements of enhanced due diligence;
- (b) Introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions;
- (c) Refusing the establishment of subsidiaries or branches or representative offices of financial institutions from the country concerned, or otherwise taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT/CPF systems;
- (d) Prohibiting financial institutions from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate AML/CFT/CPF systems;
- (e) Limiting business relationships or financial transactions with the identified country or persons in that country;
- (f) Prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the CDD process;
- (g) Requiring financial institutions to review and amend, or if necessary terminate, correspondent relationships with financial institutions in the country concerned;
- (h) Requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned;
- (i) Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

195. Under sections 94A of the POCA and 16A of the TPA institutions in the regulated sector in respect of its business relationships and transactions with any customer resident or domiciled or in the case of a body corporate, incorporated, in a specified territory³⁰⁰ must:

- i. apply the enhanced due diligence procedures;
- ii. ensure that the background and purpose of all such relationships and transactions are examined;
- iii. ensure that the findings under i. and ii. are set out in writing and made available, upon request, to the designated authority, the supervisory authority or the competent authority concerned, as the case may require; and
- iv. limit those business relationships or one-off transactions,

in accordance with enhanced money-laundering/terrorist financing counter-measures set out in the Regulations and discussed throughout these Guidance Notes.

²⁹⁹ FATF Recommendations last updated August 2024—Interpretive Note to R19.

³⁰⁰ POCA 94A (2) and TPA 16A (2) define specified territory to mean a territory specified in a list, published by Notice in the *Gazette*, by a Supervisory/Designated Authority, as being a territory in respect of which there is a greater associated risk of money laundering or terrorist financing.

Transactions Undertaken For Occasional Customers³⁰¹

196. An occasional customer (e.g. a non-account holder) falls within the definition of ‘applicant for business’ under the AML/CFT/CPF framework. An applicant for business ‘means a person seeking to form a business relationship, or carry out a one-off transaction with a regulated business’.³⁰² Accordingly, a transaction with an occasional customer is subject to the identification and transaction verification procedures, as well as the record keeping requirements and reporting obligations in the law.³⁰³ Where a financial institution undertakes these transactions, satisfactory evidence of identity must be obtained failing which, the transaction must be terminated. If the customer is not an account holder, that customer still remains subject to CDD requirements (as applicable in the circumstances) set out above, in these Guidance Notes and all copies, reference numbers and other relevant details relating to the transaction shall be recorded and retained by the financial institution for a minimum period of not less than seven (7) years³⁰⁴.

Custody Arrangements

197. A financial institution must take certain precautionary measures in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such facilities are made available to non-account holders, there must be strict adherence to the identification procedures set out in these Guidance Notes and the relevant statutes.

Electronic Funds Transfers (Wire Transfers, Money Transfers Etc.) Activities³⁰⁵

198. According to the interpretive note to FATF Recommendation 16 - the term ‘wire transfer’ refers to any transaction carried out on behalf of an originator (natural or legal) through a financial institution by electronic means, with a view to making an amount of money available to a beneficiary at another financial institution irrespective of whether the originator and the beneficiary are the same person. (The financial institution receiving the transfer is known as the ‘beneficiary financial institution’).
199. As discussed at paragraph 29 above, the POCA (MLP) Regulations, 2007 as amended in 2019 reflect that for wire or electronic fund transfers that are being conducted by regulated businesses, the information that must be obtained pertains to information throughout the payment process and chain and this information must be accurate and relevant information and must be retained for the applicable statutory period³⁰⁶. The information that must be obtained when conducting any electronic fund transfer³⁰⁷ (EFT) includes:—
- (a) the correct name, address and account number (if any) of the persons involved in the transfer;
 - (b) the reference number assigned to the transaction;
 - (c) any other reference number; and
 - (d) the instructions given in relation to the transfer; and
 - (e) where transfers exceed USD500 (or its equivalent in any other currency), the identity of every recipient of the funds transferred (including intermediary recipients) as well as the identity of the ultimate recipient/beneficiary. This information must also be verified.
200. Given the foregoing, FIs would need to have in place risk-based policies and procedures for determining whether to execute, reject or suspend any EFT where the identification contained at paragraph 198 (a) - (e) is not made and verified.
201. Given the differing transaction threshold triggers that may be applicable for the capture of such information and the differing information sharing laws and protocols that may be applicable in different jurisdictions, it would be prudent for financial institutions to ascertain certain details or confirmations (see list below) from the counterparty financial institution to be involved in the EFT, ahead of conducting the EFT to ensure that the requirements of regulation 9 of both the POC (MLP) Regulations and of the TP (Reporting Entities) Regulations, can be met. They are:
- (a) Transaction thresholds at which CDD information described at regulation 9(1) and (2A) of the POC(MLP) Regulations will be captured;
 - (b) CDD details that can routinely be disclosed in the course of conducting wire or other electronic fund transfers; and

³⁰¹ POC (MLP) Regulations, r.6; TP (Reporting Entities) Regulations, r.4.

³⁰² POC (MLP) Regulations, 2007 r.2; TP (Reporting Entities) Regulations, 2010 r.2.

³⁰³ POC (MLP) Regulations, 2007 r.6 (1)(a); FATF Recommendations R10(d). Note that the FATF recommendations (R10) reflect that CDD for occasional transactions should be applied for transactions above the designated threshold of USD/Euro 15000 where there is no suspicion of ML (R10 IN1). Jamaica’s requirements are therefore more stringent in this regard as no applicable threshold applies in relation to occasional transactions.

³⁰⁴ POC (MLP) Regulations, r. 14(5).

³⁰⁵ FATF Recommendation 5 and FATF Special Recommendation on Terrorist Financing POC (MLP) Regulations, 2007 r.7 and 9 (amended in 2019)

³⁰⁶ Refer to the POC (MLP) Regulations, regulation 14 (5) on record keeping procedures, seven years commencing on the date the business was completed or the business relationship terminated whichever occurs later or such other period specified by the designated authority in writing.

³⁰⁷ POC (MLP) Regulations, regulation 9; TP (Reporting Entities) Regulations, regulation 9, amended in 2019.

- (c) Persons from whom disclosures are possible (i.e. originators of the transaction, intended recipients/beneficiaries, and any financial intermediary involved (if one is used)).

202. The guidance in this paragraph is applicable to both domestic and cross border EFTs:—

- (a) Where a financial institution is not in control of both the sending and receipt of an EFT, then that financial institution is not expected to be in a position to verify the information provided in respect of the sending aspects of the transaction. However, where the financial institution does have control of both the ‘send and receipt’ aspects of a wire transfer or EFT, then that financial institution must be in a position to verify the accuracy³⁰⁸ of the information provided in respect of both the ‘send and receipt’ aspects of the transaction.

Further based on the amendment to POC (MLP) Regulation 9 there is a legal duty on an FI of identifying and verifying the identity of the *recipient* where the amount exceeds USD 500.

- (b) Where the information obtained is one which generates or raises a suspicion that ML, TF or breach of the designations regarding the proliferation of weapons of mass destruction is taking place, the financial institution shall ensure that the appropriate action is taken (i.e. the transaction is not done and the required disclosure is made as the case maybe).
- (c) Batch transfers—Unless the receiving or intermediary financial institution has the technical capability to immediately access from its records, the requisite originator and beneficiary details as discussed above, it must not accept batch transfers regardless whether such transactions qualify as ‘routine’ or ‘non-routine’ transactions.
- (d) Transfers not accompanied by the complete originator information—
These transfers must not be processed by the receiving or intermediary financial institution unless and until the complete originator information is available. Where a transfer of this nature is identified, it must be immediately red flagged for either termination or as one not to be acted on, until the requisite information is received. To this end it is the responsibility of financial institutions to ensure that they are legally in a position to discontinue or terminate the transaction, or to delay acting on the transaction until the requisite information has been received. In the interest of good customer relations, financial institutions must pursue methods of making customers aware from the outset that all EFTs must be accompanied by the information set out in the law as the absence of this information can cause the transaction to be delayed, declined, discontinued or terminated.
- (e) Where the receiving or intermediary financial institution finds that there is an ongoing situation of consistent or the frequent receipt of transfers of the nature described in (d) above, it must consider terminating its business relationship with the financial institution from which such transfers are consistently or frequently received (i.e. the sending or ordering financial institution).
- (f) The guidance in (c) - (e) above are also equally applicable to financial institutions conducting outgoing domestic or cross border EFTs.

*Transactions Conducted Through The Society For Worldwide Interbank
Financial Telecommunication (Swift)*

203. SWIFT operates an international financial message system which enables payment instructions between banks involved in an international funds transfer operation³⁰⁹, and related messages (i.e. statements, foreign exchange and money market confirmations, collections, documentary credits, inter-bank securities trading) to be sent between members and other connected financial institutions all over the world.

SWIFT is solely a carrier of messages. It does not hold funds nor does it manage accounts on behalf of customers, nor does it store financial information on an on-going basis. As a data carrier, SWIFT transports messages between two financial institutions. This activity involves the secure exchange of proprietary data while ensuring its confidentiality and integrity³¹⁰.

- (a) In December 2014, SWIFT introduced a KYC Registry Product for its members. The relevant factsheet on this product reflects that the SWIFT KYC Registry is a global platform to centrally store qualified documents and data that financial institutions can employ while on-boarding, updating or re-evaluating their correspondent relationships. It provides a secure portal for exchanging Enhanced Due Diligence (EDD) and Simplified Due Diligence (SDD) documents and data.

The KYC Registry offers a unique approach compared to current alternatives by providing access to a standard set of due diligence documents and data. All information in The K.YC Registry undergoes exhaustive quality control and transparent validation by a dedicated operational team at SWIFT. Each Registry user retains ownership of its data. Registry users can only access each other’s data when permission to do so has been granted by the data owner.

³⁰⁸ FATF Glossary - “accurate” is used to describe information that has been verified for accuracy.
³⁰⁹ Brindle & Cox-Law of Bank Payments-Cap. 3 —pageS 64 and 76 - SWIFT is a member-owned cooperative through which the financial world conducts its business operations. Over 8,300 banking organizations, securities institutions and corporate customers in more than 208 countries exchange millions of standardized financial messages through SWIFT. SWIFT has its headquarters in Belgium and has offices in the world’s major financial centres and developing markets.
³¹⁰ See the SWIFT website at www.SWIFT.com

- (b) The SWIFT Traffic Profile is a unique, value-added report that SWIFT offers in connection with The KYC Registry. It uses aggregated global payment data to help banks pinpoint areas of potential risk from specific jurisdictions and supports due diligence activities by providing an independent, fact-based overview of a specific bank’s direct and indirect/nested correspondent banking activities.³¹¹

The relevant fact sheet specifically reflects that SWIFT has no involvement in any type of judgmental activities such as due diligence, screening, risk scoring or recommendations about the closure of business relationships as those remain the responsibility of the financial institutions that use the Registry.
- (c) Local financial institutions that are participants in SWIFT therefore remain mandated to apply full KYC and enhanced due diligence requirements as participating in SWIFT or the SWIFT KYC Registry initiative is not an alternative to this requirement.

*Anonymous Accounts/Accounts In Fictitious Names/Numbered Accounts*³¹²

204. A financial institution must not in the course of business carried on by it, permit any person with whom it forms a business relationship, to conduct any transaction with it by means of an anonymous account, an account held in a fictitious name³¹³ or an account identified only by a numbered account.
- (a) An anonymous account includes an account for which there is no name by which the account holder can be identified. That is to say that in relation to such an account, even when that account is subjected to the identification and transaction verification processes outlined under the POC (MLP) Regulations; the identity of the account holder is still not satisfactorily established.
 - (b) An account held in a fictitious name includes an account name which when subjected to CDD identification and verification procedures, does not constitute the true name of the account holder or of the Principal on whose behalf the transaction is being done, or of the beneficiary of the legal arrangement through which the transaction is being conducted.
 - (c) A numbered account refers to an account that is identifiable solely by reference to the number or series of numbers assigned to that account.

Specific Additional Guidance For Cambios, (Exchange Bureaux) and Money Transfer and Remittance Agents and Agencies (Remittance Service Providers (Rsps)/Remittance Companies)

205. This section provides additional guidance on the identification and verification procedures that cambios and remittance companies are required to undertake before proceeding with a transaction or before establishing a business relationship. It is understood and accepted that the nature of the relationship between cambios, remittance companies and their respective customers can be fundamentally different from that established between banks and other regulated financial institutions and their customers. Cambios are entities, which are permitted with the approval of the Bank of Jamaica, to buy and sell foreign currency only. Remittance companies are entities which facilitate the movement of funds from one person to another person (whether intra-island or across national borders). The customer profile of cambios and remittance companies will therefore fall largely within the following categories:—
- (a) Customers (both individual and corporate), conducting one-off transactions;
 - (b) Customers constituting visitors to the country (i.e. tourists/visitors on business (entertainment/sporting events); persons in Jamaica on work permits etc.)
 - (c) Repeat customers which for the purposes of these Guidance Notes means the following:
 - (i) Repeat customers, for the purpose of Cambio transactions, are known regular customers who engage in transactions more than once in a three (3) month period;
 - (ii) Repeat customers, for the purpose of outbound remittance transactions, are defined as “Persons who transact business with a Primary Agent (and/or the sub-agent/(s) thereof) more than once within a three (3) month period irrespective of the transaction amount”.

Based on the customer profile of these entities there may be practical difficulties with enforcing the same level of KYC procedures in relation to the customers described above particularly in relation to (a) and (b).

206. The interpretive note to FATF R16 (wire transfers) reflects that money value transfer operators should be subject to all the requirements of FATF R16 on wire transfers in the countries in which they operate, whether these operations occur directly or through agents. The KYC and CDD requirements reflected in these Guidance Notes are therefore fully applicable to cambios and remittance companies.

³¹¹ compliance.services.sift.com/kyc-registry.
³¹² Regulation 16, POCA (MLP) Regulations and Regulation 16, TP (Reporting Entities) Regulations.
³¹³ FATF Recommendations 9 and 10; Section IV above.

However, considering the typical customer profile of Cambio and remittance businesses, it might not in all cases be practicable or feasible for the methodology applied by banks and banking institutions as regards establishing KYC procedures to be fully applicable to all cambios and remittance company transactions. Consequently, cambios and remittance companies will have to employ measures which are more compatible with the nature of the relationships generated by such businesses (whether customer-related or otherwise) to obtain CDD and KYC information. (One example of this is the Corporate Profile form developed by the Cambio Association of Jamaica in consultation with the Bank of Jamaica.)

KYC Guidance—

207. As cambios and remittance companies largely operate on a ‘one-off’ transaction basis and ‘walk-in- customers’ environment, these persons are not expected to apply the exact verification procedures that may be possible for other financial institutions which can establish account holding relationships with their customers. However, cambios and remittance companies are expected to employ verification processes more suited to their operations in order to satisfy themselves of the veracity of the information provided and of the authenticity and validity of the identification tendered. (Techniques to be employed may include but not be limited to checking the signature of the applicant for business with the signature on any transaction instrument or documentation offered by the customer; ensuring that identifications tendered are current and do not appear to be forged documents or documents that have been tampered with; that the picture in the identification used is consistent with the features of the person tendering the identification; questioning the customer for confirmation details where this becomes necessary in the circumstances and clearing all cheque transactions before proceeding to act upon such instruments.)
208. Transaction verification efforts that involve checking the nature of the transaction against the risk factors indicated below may also be employed to assist with a determination of the genuineness of the transaction. They are:
- (a) Transaction is unnecessarily complex for its stated purpose.
 - (b) Transfers being made on behalf of a third party.
 - (c) Transaction is inconsistent with financial standing or occupation indicated, or is outside the normal course of business for the customer in light of the information provided by the customer;
 - (d) EFT transaction:—
 - (i) involves EFT to one or more foreign countries with which there is no clear or apparent connection;
 - (ii) involves Transfers to the same person from different individuals or to different persons from the same individual;
 - (iii) involves EFTs not accompanied by complete originator information;
 - (iv) does not appear to match the recipient’s usual needs or receiving pattern.
 - (e) Unusual currency exchange (*e.g.* small denomination currency for high denomination currency; or transaction requested seems inconsistent with the customer’s expected requirements based on the information provided by that customer).

Additional MVTs (‘Money or value transfer services’) related operating risk factors can be found in the FATF Guidance- for a Risk-Based Approach for Money or Value Transfer Services, February 2016, paragraphs 46-50 (under the broad heading of Country/Geographic Risk, Customer Risk, Product/Transactions/Service Risk, Agent Risk.)³¹⁴

209. For inbound EFTs, beneficiary institutions, are required to ensure that all relevant KYC and CDD information pertaining to the sender (originator of the remittance) as well as the beneficiary (ultimate recipient of the remittance) is obtained but the verification of the information pertaining to the sender (originator) is the responsibility of the institution from which the remittance is sent or originates (the ordering institution). There is a responsibility however to obtain and verify all information pertaining to the ultimate beneficiary of the remittance proceeds who in this scenario, is the customer of the beneficiary institution.³¹⁵
210. For transactions with cambios and remittance companies amounting to, or exceeding USD500³¹⁶ identification and documentation pertaining to the source of the funds used in the transactions that are tendered, must be copied and the copies retained for the records of the cambio/remittance company. POCA also requires that EFTs exceeding this threshold of USD500, must also include the national identification number; customer identification number and the originator’s date and place of birth. The date and place of birth of the account holder from whose account the funds involved in the EFT originate, must also be provided.³¹⁷

³¹⁴ FATF describes Money or value transfer services (MVTs) as “financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTs provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods”.

³¹⁵ FATF Revised Recommendations Interpretive Note to R16 -Paragraph E - Responsibilities of Ordering, Intermediary and Beneficiary Financial Institutions. Paragraph F on Money or Value Transfer Service Operators reflects that these persons should be required to comply with all the relevant requirements of R16.

³¹⁶ POC(MLP) Regulation 9 (2A) was amended to USD500 in 2019.

³¹⁷ Regulation 9(2A), POC (MLP) Regulations, amended 2013.

211. All repeat customers must submit the requisite KYC and CDD information including documentation pertaining to the source of the funds used in the transaction regardless of the transaction amount.
212. The applicant for business/customer identification requirements could be considered to be satisfied where the applicant for business/customer identification is an Authorised Foreign Exchange Dealer or a Cambio, unless the transaction is red flagged for closer scrutiny or the transaction amounts to a suspicious or unusual transaction.
213. In the case of body corporates doing business with cambios, the information requirements of paragraph 131 (c), (d), (f), and (g) - will be satisfied if the corporate customer completes and submits to the Cambio with which business is to be transacted, the Corporate Profile Form. The minimum financial information that cambios shall obtain from corporate customers are:—
- (a) Total Capital as at the end of the last financial year for the customer;
 - (b) Total Assets as at the end of the last financial year for the customer;
 - (c) Total Liabilities as at the end of the last financial year for the Customer;
 - (d) Change of Directors/Principals/significant shareholders/ signing officers/ since the completion of the last corporate profile form;
 - (e) Main business to be carried out/services to be offered by the customer;
 - (f) Whether the customer is in possession of any special authorizations under the BOJ Act Section IVA pertaining to foreign exchange activities; (Details of the authorization and duration thereof are to be provided if the customer indicates such authorization exists);
 - (g) Purpose of FX activities the company expects to conduct with the cambio i.e.—
 - (i) Bill payments for services rendered by overseas based parties; or for items purchased from overseas for the customers own use;
 - (ii) Importation of commercial goods;
 - (iii) Own account investment activities;
 - (iv) Other (details to be provided as to what the activity entails)

In outlining the purpose of the FX activities to be conducted, a general estimation of the frequency with which the company expects to be conducting or actually conducted these activities for the relevant period to be included e.g. daily; weekly; fortnightly; monthly; bi-monthly; quarterly; bi-yearly; annually; occasionally; or as the need arises.

214. For the purposes of the additional guidance for cambios and remittance companies in these Guidance Notes, a “*significant transaction*” which is defined in Section V paragraph 98 of these Guidance Notes includes any transaction amounting to or exceeding US\$8,000 (in the case of business done with cambios) and US\$5,000 (in the case of business done with remittance companies) or the equivalent thereof in any other currency. Accordingly—
- (a) In addition to the copies of identification and source of funds information that must be obtained, and retained, the more fulsome KYC particulars and as far as possible verification processes akin to those outlined in Section V, applies; and
 - (b) Transaction purpose must be documented (copies of documents which explain or outline the transaction must also be obtained and retained) and the transaction shall be subject to further reviews:—
 - (i) obtaining and verifying additional information on the customer from wider sources and reviewing the customer’s profile;
 - (ii) more rigorous review of the customer’s background (financial, professional and personal as far as is reasonable);
 - (iii) subjecting transaction history information to consistency checks with earlier information provided and new information provided by the customer; and
 - (iv) looking at customer’s willingness to provide sources to allow for independent verification of information supplied to the cambio or remittance company;
 - (v) ascertaining the reason for conducting the transaction with a MSB as against a bank; and
 - (vi) whether the transaction was attempted elsewhere and refused and the reasons for that refusal.

Implementation is perhaps better accommodated by establishing minimum advance notification requirements for customers intending to conduct a significant transaction to allow the information to be provided to the cambio or remittance company and the requisite verification to be undertaken prior to the transaction being facilitated.

Cheque Transactions

215. As regards the process of ensuring cheques are cleared before acting on them, cambios/remittance companies could consider that there are inherent risks generally associated with the presentation and clearing of cheques because a collecting bank is unable to verify the genuineness of a cheque or ascertain the availability of funds

at the time of accepting the deposit. For purposes of the Clearing House rules there is no distinction between a Manager’s Cheque and personal or company cheques. A commercial bank therefore has the discretion to make a credit decision to release funds sooner depending on the customer’s circumstances; however, the incidence of frauds perpetrated against banks with the use of manager’s cheques has caused many banks to discontinue exercising their discretion in this manner. Cambios and remittance companies which therefore make the business decision to advance funds to customers against cheque payments must note that they do so at their own risk of the cheque not being paid.

216. Cambios and remittance companies shall consider employing the following measures when conducting cheque-related transactions—
- (a) Ensuring sight of sufficient documentation to satisfy the cambio/remittance companies that the cheque tendered is the result of a genuine transaction with a commercial bank (e.g. sight of passbook and copying the receipt tendered as being that issued by the bank (whether via ATM or over the counter)); or
 - (b) Contacting the issuing bank to confirm the fact that the cheque was drawn on the bank and cross-checking details to establish a reasonable level or degree of certainty that the transacting customer is the genuine party authorized to be transacting business with that cheque; and
 - (c) Ensuring the cheque is subjected to inspection to determine whether it is technically in order which includes inspections to determine that:
 - (i) The cheque is properly signed;
 - (ii) The cheque is properly dated;
 - (iii) Numbers and figures correspond;
 - (iv) There are no unsigned alteration/s;
 - (v) Other essential features are present (e.g. serial number of the cheque; code identifying the branch of the paying bank on which the cheque is drawn) etc.; and
 - (d) Employing the following operational measures to limit exposures to cheque-related transactions—
 - (i) Limiting acceptance of cheques subject to third party arrangements as obtaining clearance for these cheques would be significantly more difficult than for cheques that are direct (i.e. payable to the cambio or remittance company, or to the person tendering the cheque);
 - (ii) Limiting acceptance of personal cheques as the same difficulty above arises in these circumstances;
 - (iii) Applying transaction limits for cheque-related transactions;
 - (iv) Refusing to conduct cheque-related transactions in circumstances where the transaction is so out of the ordinary course that it raises doubts about the genuineness or accuracy of the transaction (e.g. cheques payable to a company being tendered by that company’s agent for a cambio transaction), or it appears that the bearer’s title to the cheque may be defective, or it appears to be a transaction in respect of which a disclosure under section 94 or 95 of the POCA or under section 16 or 17 of the TPA must be made.

Customer operating through a Bearer or Agent

217. Where the applicant for business is a corporate customer seeking to act through an agent/bearer (whether employed or contracted) the cambio or remittance company must also enforce the customer identification requirements in relation to the agent/bearer. Additionally, the agent/bearer must submit a copy of the corporate customer’s certificate of incorporation and a letter from the corporate customer on the corporate customer’s official letterhead and bearing the signature of an authorised officer.³¹⁸ The letter must clearly indicate the business to be transacted, that the agent/bearer is acting on the corporate customer’s behalf for this matter and that the person signing to the letter is authorized so to do. Where in relation to the corporate customer it appears to the cambio or remittance company conducting the transaction that the agent/bearer is not the usual agent/bearer, or the letter from the corporate customer is in any way defective, (e.g. it is not on the official letterhead; there have been alterations or amendments to the contents of the letter which are not signed by the author of the letter; or the letter itself is not signed) business shall either not be transacted at all, or must be delayed until the corporate customer is contacted by the cambio or remittance company and asked to confirm in writing or issue renewed written instructions and the confirmation or renewed instruction is in fact received. Even in the absence of these warning signals cambios must, as a matter of course, employ the practice of conducting random checks with the corporate customer to satisfy itself of the genuineness and accuracy of the transaction to be conducted.
- Similar practices shall be employed for agents or bearers acting for individual customers.

³¹⁸ For the purpose of these Guidance Notes “authorised officer” would mean a manager/senior officer of the company, and as such the letter should clearly indicate the name and position of the “authorised officer”.

Establishing Appropriate Identification

218. The “appropriateness test” of the identification obtained is that, from the records prepared and retained by the cambios or remittance companies, one must be able to compile a complete picture of the customer and of the business that customer transacted with the cambio or remittance company.
219. The type of identification tendered must be any one of the options described at paragraph 119 above. If an applicant for business has none of these forms of identification with him/her, then the cambio or remittance company may consider relying on the options outlined above in paragraphs 120-121. Additionally, the cambio could accept a customer’s client card (where the client card was issued to that customer by the specific cambio or remittance company itself). Where however client cards are the sole source of identification relied on, the Cambio’s records or the records of the remittance company must contain a photocopy of the customer’s official identification as well as corroboration of the customer’s address and source of funds and these records will need to be updated from time to time (see paragraph 117 above); or accept:—
- (a) a birth certificate accompanied by a Declaration of Identification and a photograph both of which (i.e. the Declaration and the photograph) must be signed by a Justice of the Peace (JP), a Minister of Religion or an Attorney-at-Law, to whom the customer is personally known, and who is reasonably capable of confirming the identity of the customer; (This identification evidence must be collected from the customer and retained by the cambio/remittance company and the reference number on the birth certificate clearly indicated on the document evidencing the transaction and the Declaration and copy birth certificate stapled to the document evidencing the transaction).
 - (b) In the case of Remittance Companies when conducting inbound transactions only, with a customer who is a student, a valid school ID, where the student customer is enrolled in a secondary or tertiary institution, may be accepted where the student customer identified as the recipient beneficiary, is maintained through remittances sent by overseas parents or guardians responsible for him/her. The ID must have the features outlined in paragraph 119.
 - (c) The customer’s complete residential address must be recorded (see also paragraph 146 above). The address must be sufficient for the customer to be contacted by mail or by hand (i.e. bearer) and (should the need arise) by telephone (see note further down). If a business address is being given as the official address of contact (where the applicant for business is a corporate customer) then the name of the business must also be given and the full business address stated. Descriptions such as “business place” will not be acceptable. If there is any uncertainty about the address, a contact number must be obtained from the customer.

It is likely the customer base for a cambio or remittance company is likely to have a higher incidence of persons falling within the category of persons reflected at paragraph 120 above. Accordingly, the assumption discussed at paragraph 123 regarding a financial institution’s reliance on the exceptions as the normal acceptable identification as acting contrary to its KYC obligations will not apply to cambios and remittance companies unless the reliance occurs outside the parameters outlined in paragraphs 120-121 and paragraphs 216-217 of these Guidance Notes.

Suspicious Transactions

220. It should be noted that paragraphs 27 and 28 above are also applicable to cambios and remittance companies. Where a transaction appears to be one in relation to which a disclosure must be made pursuant to section 94 or 95 of the POCA (i.e. suspicious), or pursuant to section 16 or 17 of the TPA, the transaction shall not be conducted. Transactions that are not at the stage of being regarded as suspicious but which appear unusual, and therefore raise questions or are flagged for closer scrutiny and which in that case are still conducted, must be subject to full KYC banking standards and reported to the designated authority in accordance with the POCA or the TPA (where applicable).

The ability to discontinue transactions or terminate business relationships.

221. As cambios and remittance companies will not be opening or operating on-going accounts for customers, it may be unlikely that prolonged business relationships such as those established with customers by other financial institutions, (banks, insurance companies, unit trusts, mutual funds, securities dealers, cooperative societies), will be established in the case of cambios and remittance companies. Cambios and remittance companies must nonetheless seek to employ procedures that make it abundantly clear that they can refuse to do business with a customer and this is probably best achieved by a bold notice to this effect being displayed perhaps by the window of the teller. In the case of persons who have obtained client cards, the documentation issued with the card or the card itself must make it abundantly clear that the card privileges and the card can be withdrawn at any time without notice where the cambio or remittance company believes that its discretion in this regard needs to be exercised.

Section V(A)—Special Guidance Regarding Treatment of Listed Entities

222. Financial institutions are required to determine whether they are in possession of property for persons on the U.N. lists of terrorists or persons linked with terrorists (refer to section 15 of the TPA³¹⁹). Financial institutions are further required to flag accounts where these are held in the names of persons included on the above referred U.N. lists, and to report the matter to the FID.
- Institutions must note that once a person has been designated a ‘listed entity’, by order of the Supreme Court in accordance with s.14 of the TPA, this designation will be published by the DPP in a daily newspaper in circulation in the Island. This section prohibits directly or indirectly dealing of any kind with any property owned or controlled by a listed entity which increases the possibility of breaching Sections 4 - 6 of the TPA. Since the passage of amendments to the TPA in 2011, printed publications pursuant to section 14 of the TPA have been made³²⁰.
223. Financial institutions may find that they are in possession of property for, or in relation to, the following:—
- (a) Persons affiliated/connected³²¹ with listed entities; (i.e. the customer is a director, or shareholder of a company that is connected with the listed entity; or the customer includes the listed entity as one of its trading Partners; customers; investors; consultants; etc.)
 - (b) Persons for which the names are very similar to those appearing on the list of listed entities (i.e. constituting a 97% match, for example, in the case where individuals’ Christian/First Names and Surnames match but Middle Names are different; or where Full Names match but the customer is female whereas the person on the listed entity list is identified as male; in the case of incorporated/unincorporated entities, the names are sufficiently similar to consider that entity a related entity; or the name constitutes the English version of the name on the listed entity list);
 - (c) Persons whose business documentation reflect that commercial activities are conducted in territories that are generally featured as “generators or producers of terrorists”; or “sympathetic to terrorists” as indicated in official advisories from the U.N.; FATF; Ministry of Foreign Affairs and Foreign Trade; designated authorities (viz AML/CFT typologies); or the competent authority;
 - (d) Persons resident or domiciled in a territory specified in a list of applicable territories published by notice in a Gazette by a supervisory authority³²².
224. It is likely that the view might be formed that transactions/accounts with such persons may not be at the stage of being regarded as suspicious but do in fact raise questions. These accounts or transactions must be flagged for closer scrutiny and subject to enhanced due diligence checks. For example, if the scenario at paragraph 223(b) above should exist, the institution should consider taking steps to ascertain date of birth information; customer gender and possibly have the customer come into the financial institution with a view to updating the KYC information on file. Scenarios at paragraph 223(c) and (d) above may require the institution to link with an industry representative body within the jurisdiction from which the documentation originated (such as the Bankers’ Association), with a view to ascertaining guidance on how checks can be done to satisfy the institution of the bona fides of the documentation. Where the business relationship is continued or the transaction is conducted, the account or transaction should be subject to KYC standards and additionally reported to the designated authority without delay. Resorting to full KYC checks in such circumstances means conducting enhanced due diligence and independent verification of information received in addition to any reliance on the due diligence that may have been undertaken by the originator of the transaction documentation.
225. While cambios and remittance service providers do not hold accounts or assets for their customers (such as bank accounts, investment accounts or any other ongoing entitlements) these entities would still be required to file a report under section 15, TPA. In most cases these entities would probably be filing a ‘nil report’ pursuant to section 15(3)(a) - “that it is not in possession or control of any property referred to in subsection 15(2)”. It is also possible a cambio or remittance service provider may be in a position to file a report under section 15(3)(b) “that it is in possession or control of such property, in which case it shall also report the number of persons, contracts or accounts involved and the total value of the property.”— One such circumstance could possibly arise where the cambio or remittance service provider retains possession of negotiable instruments (i.e. money order, and cheques, which are not ‘bearer instruments’ and which have been accepted from a customer in the course of conducting a transaction. This point is only made to reflect that cambios and remittance service providers still need to review their transactions to determine whether a report is required under section 15(3)(b), TPA as against 15(3)(a), TPA.
226. A failure to carry out requirements at paragraph 222 shall constitute a breach of the BOJ’s AML/CFT/CPF Supervisory Rules.

³¹⁹ See TPA amendments in 2019.

³²⁰ See Appendix VIII for BOJ’s Internal procedure for communicating Listed Entity Designations and the List of designations as of June 2025.

³²¹ *Connected* has the same meaning as defined in section 2(1) and (2) of the BSA.

³²² The POCA as amended in 201, Section 94(4). As signatories to various UN Conventions and CFATF, it would seem that Jamaica may need to ensure that jurisdictions that are flagged or blacklisted by the UN or CFATF should be included in a gazetted Notice.

Section V(B)—Special Guidance—UNSEC Resolutions on the Proliferation of Weapons of Mass Destruction

227. Financial institutions shall ensure enhanced due diligence programmes, policies, procedures and controls that are utilized pursuant to CPF obligations³²³ also incorporate measures to allow for the identification of high-risk customers and transactions in relation to or involving the DPRK and DPRK nationals or citizens (including financial institutions, and other legal persons and arrangements (including branches and subsidiaries).
228. Noncompliance with the requirement at paragraph 227 above shall constitute a breach of the Supervisory AML/CFT/CPF Rules.

Implementation under The United Nations Security Council Resolutions (Democratic People’s Republic of Korea Sanctions Regime) Regulations, 2021

Freezable Assets

229. Where, after November 15, 2013³²⁴, freezable assets have been identified (whether in the form of accounts established, funds held, transactions facilitated, lines of credit established; wire transfers accommodated (whether inbound or outbound) or otherwise, then, in relation to the DPRK:—
- (a) the requisite reporting must be done to the CTD of the FID; and
 - (b) an application must be done to the Minister of Foreign Affairs and Foreign Trade pursuant to Regulation 35 under f the UNSCRI (DPRK Sanctions Regime) Regulations, either requesting that the financial institution be permitted to use or deal with the freezable asset in a specified way (e.g. honouring contractual obligations to the point where termination or discontinuation of services or activities can be undertaken without penalty or without prejudicing the rights of a bona fide third Party or counterparty) or to permit the asset to be made available to the designated entity (e.g. return of funds to the account holder if an account is closed).
 - (c) A copy of the application to the Minister shall be provided to the CTD of the FID and when a response to that application is received by the financial institution, a copy of that response shall also be provided to the CTD of the FID.

It is imperative that a financial institution employ the requisite checks to ascertain whether or not it is in possession or control of freezable assets as quickly as possible. Once such assets have been identified, any dealings that occur in relation to such assets must immediately be contained to the sole purpose of preserving the value of such assets. Regulation 18(3) stipulates that it is a defence against a charge under regulation 18(1), if the person charged proves that the use or dealing was solely for the purpose of preserving the value of the freezable asset.

Sanctioned Services and Sanctional Commercial Activity

230. As mentioned above in paragraph 55 and as of March 16, 2026, **Sanctioned Services** are defined in Regulation 13. In relevant part, financial institutions should take note of Regulation 13 (1) (c), (f), (g), (j) and the definition of financial services, and public or private financial support in Regulation 13 (2)³²⁵. A person shall not provide a sanctioned service unless the service is provided in relation to an Authorised supply. (See Regulation 14 (1). Authorised supply is defined in accordance with Regulation 2 and construed in accordance with Regulation 6.
- Sanctioned Commercial Activity** is defined in Regulation 15. This list is expansive and ranges from the opening by a financial institution of a representative office in DPRK (Regulation 15 (f)) to the establishment by a financial institution of a correspondent banking relationship with a person, or entity mentioned in subsection 2 of Reg 15. See Regulation 15(1)(e) and 15(3) for the definition of correspondent banking relationship³²⁶. A person shall not knowingly engage in any sanctioned commercial activity without Authorisation as defined by Regulation 2 and Part III of the Regulations.
- 230B. Regulations 29, 34 and 36 are relevant to the process to be employed to obtain a grant of permit authorising the provision of sanctioned services or engaging in sanctioned commercial activity. Per Regulation 29 the Minister has the power generally to grant a permit on application by a person or on the Minister’s own initiative and with or without conditions.

It is imperative that a financial institution introduce measures to ensure that it is not knowingly engaging in a sanctioned service or commercial activity without the requisite Authorisation.

Other Powers of Minister - Regulation 19

231. Pursuant to Regulation 19, financial institutions should be aware that the Minister may by written notice direct the closure off a bank account if the provider is—
- (a) a financial institution resident in DPRK;
 - (b) a branch or subsidiary, wherever located, of a financial institution domiciled in DPRK; or

³²³ Regulation 5 of the UNSCRI (Reporting Entities) Regulations, 2019.

³²⁴ Date of Assent to the UNSCRIA, 2013.

³²⁵ Please be reminded that there is an ongoing duty of financial institutions to be aware of all legal obligations including any legislative changes that may arise.

³²⁶ See also Regulation 15(1)(g), (h), (i), (j), and (k).

- (c) a financial institution, wherever resident, that is controlled by a person or entity, domiciled in DPRK.

Please take further note of the without notice exceptions contained in section 2. Where a notice is given under section 1 a failure to comply by a financial institution is an offence. Strict liability attaches to this regulation and as such financial institutions should ensure that the proper operational procedures are in place to comply with these notices.

Iran (Re-application of UNSEC Resolutions)

- 231A. Pursuant to the process set forth in paragraphs 11 and 12 of United Nations (UN) Security Council resolution 2231 (2015), as of 27th September, 2025, all of the provisions of resolutions 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2008), and 1929 (2010) related to Iran have been re-applied in the same manner as they applied before the adoption of resolution 2231 (2015).

By way of Court Order issued pursuant to section 3 A of the UNSCRIA on March 12th 2026, Jamaica gave effect to the targeted financial sanctions under the abovementioned resolutions. Financial Institutions are therefore to note that assets of those proscribed individuals and entities are to be treated as freezable assets under the UNSCRIA. (See **Appendix X** as referenced in footnote 29 above.

Updated Guidance Regarding the 2019 Amendments to the UNSCRIA

- 231B. Reference is made to paragraphs 51-56 above which highlight the 2019 amendments.
Importantly,
 - (a) The Act now expressly prohibits dealings, facilitations, provision of financial or related services or making any property or financial or related services available or conversions or attempted conversions or attempted conversions of property owned or controlled by or on behalf of a proscribed person or entity, whether directly or indirectly but removes the strict liability element of the offence (Section 8A incorporated under the 2019 Amendment Act).
 - (b) Implementing Regulations pursuant to any designations by the UN must be done within 30 days of such designation (New Section 3(1) incorporated under the 2019 Amendment Act).

Section V(C)—Additional Guidance-Financial Holding Companies

- 232. With the 2013 amendments to the POCA, the Fourth Schedule thereto extended the category of ‘regulated business’, to include Financial Holding Companies and therefore now refers to “*an entity with corporate responsibility for the development and implementation of group wide AML/CFT policies and procedures for the group of entities of which it forms a part.*” Accordingly, a financial holding company or such other person bearing this responsibility is fully subject to the statutory AML obligations under the POC legislation.

Accordingly, a financial holding company under the BSA, is also subject to the mandates outlined in Section IV above and especially paragraphs 87-91, 222, and 227-228 in relation to local and overseas branches and subsidiaries.

Section V(D)—Additional Guidance-Branches and Subsidiaries

- 233. In complying with the mandates at Section IV above in relation to local branches and subsidiaries and the corresponding mandates under the POCA and TPA in relation to overseas based branches and subsidiaries, a financial institution shall in relation to its subsidiaries and branches, ensure—
 - (a) the CDD details for customers are well documented (i.e. identification and other customer information as defined under the POC(MLP) Regulations,) is submitted and recorded); source of wealth is obtained as a part of the financial history of the customer as well as transaction details (including nature of the transaction, transaction amount; currency used; method of payment [cheque/cash/credit card/debit card/wire transfer] and source of funds used to make the payment) are recorded;
 - (b) AML/CFT/CPF internal regulatory controls (i.e. employee training, designation of a nominated officer, auditing of internal controls etc.) are documented (where applicable), approved and implemented;
 - (c) required disclosures (i.e. STRs) are made and any other reporting obligations are met;
 - (d) AML/CFT measures are employed in a risk-based manner, (e.g. processes that include the imposition of transaction limits beyond or below which enhanced or reduced monitoring measures may be applied; and in relation to branch and subsidiary operations³²⁷ in Jamaica, measures that track cash transactions are implemented, as such transactions facilitate anonymity in relation to financing of transactions and source of funds.
- 234. A failure to carry out these requirements will constitute a breach of the BOJ’s AML/CFT/CPF Supervisory Rules.

³²⁷ Agents not included. POCA exemptions from cash transaction limits (s.101A) apply only to banks or DTIs licensed and regulated by BOJ and cambios; or persons specifically exempted by the MNS. Agents are persons authorized to undertake some banking services for appointing DTIs but that authorization does not equate to a licence. Nor can an agent undertake banking services in its own right.

Section V(E)—Additional Guidance-Agent Banks

235. A deposit taking institution under the BSA which has appointed an agent pursuant to section 108 of the BSA shall in relation to that agent, be subject to the same mandate as outlined at Section IV above in relation to its branch operations. (See Additional Guidance- Branches & Subsidiaries).
236. In this regard, an agent found to be operating in breach of the AML/CFT/CPF policies and procedures of its appointing deposit taking institution shall be in breach of the AML/CFT/CPF Supervisory Rules.
- An appointing deposit taking institution whose agent is found to be operating in breach of the appointing deposit taking institution’s AML/CFT/CPF policies and procedures shall also be in breach of the AML/CFT/CPF Supervisory Rules.
- A breach of the AML/CFT/CPF Supervisory Rules may result in the revocation of the appointing deposit taking institution’s approval to offer basking services through an agent.

Section VI—The Nominated Officer Regime

Reporting Obligations and The Appointment of Nominated Employees/Officers

237. Appointment of **Nominated Officer**³²⁸—A financial institution must designate an employee of the institution who performs management functions as its Nominated Officer taking into account the size and nature of the business concerned, to be responsible for ensuring the effective implementation of the established policies, programmes, procedures and controls to prevent and detect money laundering and terrorist financing activities in accordance with the relevant statutes, the BOJ Guidance Notes and the licensee’s own policies and procedures.
238. In practice the function of nominated officer is most effective if that function is a position that:—
- (a) is sufficiently senior to allow for reporting to the Board, (or such other governing body by whatever name called) of the institution either directly (at Board meetings) or through a sub-committee of the Board, on the institution’s AML/CFT/CPF compliance³²⁹;
 - (b) requires an awareness of the AML/CFT/CPF laws, framework, global practices and trends that can guide the institution in establishing and maintaining the requisite controls, policies and procedures in accordance with the statutory requirements and related framework;
 - (c) requires the ability and capacity to undertake the responsibility for ongoing monitoring of the fulfilment of AML/CFT/CPF duties by the institution (including sample testing of compliance, reviewing exception reports and being the contact point regarding all AML/CFT/CPF issues for internal and external authorities including supervisory authorities or the FIU/FID)³³⁰; and
 - (d) is independent of the business lines of the institution to allow for an objective assessment and monitoring and enforcement of the compliance of the institution’s operations and decision making with its AML/CFT/CPF obligations under the country’s framework and with the institution’s own AML/CFT/CPF policies and procedures. Basel’s recommendation is that regardless of the institution’s size or its management structure, potential conflicts of interest must be avoided. Therefore, to enable unbiased judgments and to facilitate impartial advice to management, the chief AML/CFT/CPF officer should, for example, not have business line responsibilities and should not be entrusted with responsibilities in the context of data protection or the function of internal audit³³¹. The Basel’s recommendation also reflects that where any conflicts between business lines and the responsibilities of the Chief AML/CFT/CPF officer arise, procedures must be in place to ensure AMLCFT/CPF concerns are objectively considered at the highest level.
239. The Nominated Officer is responsible for reporting to the designated authority³³², all such activities as required by the relevant statutes and the Guidance Notes, and must be in a position to provide advice and guidance to the Staff of that institution, on the identification of suspicious transactions (See Appendix IV (updated) - List of Duties and Responsibilities of the Nominated Officer). In providing such advice and guidance, the Nominated Officer must pay attention to any advisories or guidance that may be issued by the designated authority in relation to reporting obligations under the AML/CFT/CPF laws and should consult with the designated authority accordingly.
240. An institution’s policy manual must require the preparation and submission of reports by the Nominated Officer to the Board of Directors (or such other governing body by whatever name called which performs such functions) at least once a year or at more frequent intervals as warranted by the risk profile of the financial institution and

³²⁸ See POCA (MLP) Regulations, 2007 r. 5(3) as amended in 2019; TPA section 18(3). In 2019 an amendment was made to R. 5(3) to replace the word officer with employee to signal that the officer should be an employee of the business. None of the roles in keeping with the nominated officer has changed.

³²⁹ Basel Committee on Banking Supervision – Sound management of risks related to ML and FT, January 2014 (Assessment, understanding management and mitigation of risks – page 5)

³³⁰ Ibid, The Basel Committee on Banking Supervision also reflects the chief AML/CFT officer should also have responsibility for reporting suspicious transactions.

³³¹ Ibid.

³³² POCA section 95; TPA section 18(3).

which ensures the board is at all times fully aware of the ML, TF and PF risks faced by the institution and of the effectiveness of the institution’s measures to address these risks. This report must, at a minimum include:—

- (a) an overview and evaluation of the overall effectiveness of the institution’s AML/CFT/CPF framework, the effectiveness of AML/CFT/CPF measures implemented under each of the various operational areas and/or product and service types as well as AML/CFT/CPF training exercises completed (training exercises should extend to training regarding compliance with directives to apply targeted financial sanctions notified by the United Nations Security Council) and initiatives pursued for that licensee’s financial year;
 - (b) The licensee’s compliance with relevant legislation and BOJ’s Guidance Notes and guidance issued by the designated authority in relation to the institution’s AML/CFT/CPF reporting obligations, reporting obligations pertaining to compliance with directives to apply targeted financial sanctions as notified by the United Nations Security Council as well as the licensee’s own policies and procedures and the programmes and policies for the financial group (where applicable);
 - (c) particulars of the risk assessment and risk management activities (see Section IV above) including:—
 - (i) Report on the adequacy and effectiveness of the licensee’s risk assessment processes;
 - (ii) Detailed assessment of effectiveness of monitoring of high-risk customers and information as to any challenges posed by that area of the licensee’s operations;
 - (iii) Report on the financial institution’s level of compliance in updating its customer records for pre-existing customers; and in obtaining the approval of senior management for transacting business with, or involving products, services, customers of jurisdictions assessed as posing a high risk of ML, TF or PF to the financial institution;
 - (iv) Continued relevance of measures employed to mitigate, minimise or otherwise manage risks identified;
 - (d) Number and frequency of threshold reports, required disclosures (suspicious transactions/activities) detected and other reportable matters reported to the designated authority;
 - (e) Any significant and/or unusual trends and typologies in evidence arising from a review of transactions detected and reported (e.g. trends in relation to specific branches, geographic areas - local and/or overseas, or types of transactions; customer profiles etc.);
 - (f) Report on the financial institution’s compliance in relation to customer due diligence and know your customer standards as set out in these Guidance Notes as well as in the financial institution’s own policy;
 - (g) Report on the findings of the annual and any other intervening AML/CFT/CPF audits undertaken by the institution’s external and internal auditors, and findings emanating from reviews by BOJ examiners; as well as steps taken to effectively address AML/CFT/CPF weaknesses or deficiencies detected or identified;
 - (h) Update on programmes employed over the reporting period for targeting employee awareness and integrity - including training programmes for the Board (or other governing body by whatever name called) executives, senior management, staff (and wider application as deemed appropriate) and the effectiveness of such programmes;
 - (i) Update on the financial institution’s overall relationship with the designated authority and general guidance received from that body;
 - (j) Advice on any proposed/impending legislative/regulatory changes as regards AML/CFT/CPF, with an assessment of how the institution will be impacted and advice as to how necessary operational changes will be implemented to ensure continuing adherence by the financial institution.
241. This report must be readily available to or accessible by the BOJ. Financial institutions will note that the current AML/CFT/CPF examinations include and will continue to include specific checks to ensure compliance with AML/CFT/CPF training requirements for employees.
242. A failure to comply with the requirements at paragraphs 237, 238 or 239 will constitute a breach of the BOJ’s AML/CFT/CPF Supervisory Rules.
- 242A. A financial institution is not prevented from organizing its operations to include Deputy Nominated Officers, however, regardless of how the business is structured the law requires one employee to be the person who functions as the Nominated Officer and *who bears the statutory responsibilities* of undertaking those functions. That is the individual with which BOJ will engage in relation to the AML and/or CFT and CPF responsibilities of the financial institution.

- 242B. While there is no express stipulation in the UNSCRIA legislation, it would be prudent for financial institutions to ensure their respective CPF obligations are matters for which the Nominated Officer undertakes responsibility as outlined in this section and also report on to the Board.

Section VII—Compliance Monitoring
Internal Compliance Programme

243. An effective internal compliance programme is essential to a financial institution’s endeavour to comply with its obligations under the law, prevent involvement in illicit activities and adhere to international standards.

244. The POCA and the TPA specifically require that financial institutions make arrangements for an independent audit, in order to ensure that the statutory requirements and the programmes itemized in these Guidance Notes and adopted in policy manuals, are being implemented. An employee or officer at the senior management level must have explicit and ultimate responsibility for the financial institution’s internal compliance program (Refer to Section VI above), which at a minimum would involve:—

- (a) Establishment of an adequately resourced unit responsible for day to day consideration and monitoring of compliance;
- (b) Establishment of a strong compliance plan that is approved by the Board of Directors of the institution and that provides for ongoing independent review and testing of staffs compliance with AML/CFT/CPF requirements;
- (c) Proactive follow-up of exceptions to ensure that timely corrective actions are taken;
- (d) Regular reporting of compliance levels, including exception reporting to senior management. Senior management must also be made aware of any corrective measures being implemented;
- (e) Regular consultation with the designated authority to ensure that the institution is carrying out its obligations under the law.
- (f) Regular or periodic reviews of the AML/CFT/CPF program including (the Compliance Unit) by both the internal and external audit functions. The internal audit function, which is a third line of defense function designed and implemented to give the Board of Directors assurance that the compliance programme is functioning as intended, must ensure AML/CFT/CPF audits and reviews are included in its annual audit plans, and that on a risk-basis there is appropriate and adequate coverage of the compliance programme areas over a reasonable cadence. The external auditors are also required to be fully independent of the financial institution, and be in a capacity to carry out a full scope audit/review of the compliance programme on a reasonable cadence contingent on the last external review rating. More frequent (at least annual) assessments are required for high risk audit rated institutions. Moderate to lower previous audit ratings may require a cadence of two to five years respectively. The Board of Directors must ensure the scope of these audits and reviews are comprehensive to guide its strategic oversight of the compliance programme and also guide management operationally in ensuring the programme is fit for purpose³³³.

245. Each financial institution shall:—
- (a) establish clearly defined policies and operational procedures in regard to the matters at paragraphs 102 and 103 above;
 - (b) ensure that AML/CFT/CPF policies and procedures are informed by the financial institution’s assessment of its risks as discussed in Section IV above.
 - (c) ensure that the AML/CFT/CPF policies and procedures are:—
 - (i) properly documented in the form of a manual for distribution among, or which is readily available to all relevant staff. The distribution process may be evidenced by the employee’s signing in confirmation that the manual has been received or accessed or an alternative process which is equally effective;
 - (ii) reviewed and the manual updated at least on an annual basis and make appropriate revisions and enhancements when necessary;
 - (iii) within the manual, and all subsequent revisions thereto, are reviewed and approved by the Board of Directors.

Non-compliance with these requirements will amount to a breach of the AML/CFT/CPF Supervisory Rules.

246. A financial institution shall ensure that the policies and programmes contained in its manual include the following:
- (a) measures and procedures which are commensurate to the risks that have been identified from the institution’s assessment of its risks;
 - (b) the establishment of procedures to ensure high standards of integrity for employees at all levels including senior and executive management levels;

³³³ Independent Auditors must be qualified and competent external auditors.

- (c) the development of a system to evaluate the personal employment history and financial history of all employees at all levels including senior and executive management levels. Financial institutions are expected to establish specific procedures for such evaluation at the point of hiring, although ongoing evaluation would also be expected throughout the period of employment;
- (d) the establishment of programmes for the training of employees on a continuing basis, and for instructing all employees, as to their responsibilities in respect of the law, regulatory guidance and ‘best practice’ standards; (In considering the impact of the regime in this regard, financial institutions must bear in mind the defences that can be raised by a person charged with any of the foregoing offences. For example, under POCA, not only can a person raise the defence that he or she did not know or suspect that another is engaging in money laundering, he/she can also claim that additionally the requisite training was not provided to him or her by the employer. The defence appears to require proof of both elements (i.e. lack of knowledge/suspicion and lack of training) in order to be successfully raised³³⁴.
- (e) the establishment of comprehensive customer due diligence policies and procedures, incorporating adequate customer acceptance policies and a multi-tiered customer identification programme that involves more extensive and rigorous due diligence to allow for adequate identification of ultimate beneficial owners; and are applied to high risk customers/accounts, as well as transactions with non-face-to-face and overseas customers and counter-parties;
- (f) designation of an officer of the institution at the senior management level to be the institution’s Nominated Officer, responsible for ensuring the effective implementation of the policies, programmes, procedures and controls including reporting to the appropriate authorities, of threshold and suspicious transactions and asset holdings re: listed entities or entities designated in relation to the UNSEC resolutions regarding the prevention of the proliferation of weapons of mass destruction;
- (g) full co-operation and consultation with the relevant authorities, primarily the designated authority and the Competent Authority, for the purpose of carrying out the institution’s obligations under law and best practice standards;
- (h) procedures for analysis of clients’ transactions to ascertain trends and to recognize indicators of unusual and/or suspicious activity over time, e.g. multiple small transactions aggregating to a specified limit in a month, or annually;
- (i) procedures for analysis of transactions (other than customer related transactions) that are undertaken in the course of business to determine whether the transaction is one in relation to which a required disclosure must be made. Examples of such transactions would include the following:
 - (i) correspondent banking arrangements (both within the island and cross border);
 - (ii) proprietary transactions such as securities transactions;
 - (iii) fixed asset acquisitions and disposals; and
 - (iv) custody arrangements.
- (j) arrangements for regular and timely internal and external audit reviews in order to ensure that there is adherence to the documented policy and procedures;
- (k) provision for the heightened scrutiny of certain categories of customers and types of transactions when necessary, as well as the continuous review of existing practices and procedures in this area as part of the general internal/external audit and control processes.

Non-compliance with these requirements will amount to a breach of the AML/CFT/CPF Supervisory Rules.

247. The procedures discussed at paragraphs 242-243 and 245-246 above must include measures for:

- (a) customer (including beneficial ownership) identification and verification prior to the commencement of business relationships³³⁵ and on an ongoing basis thereafter, using reliable independent source documents, data or information;
- (b) as part of its enhanced due diligence (EDO) obligations for high risk customers, taking reasonable measures to establish the source of the customer’s wealth as well as the source of funds involved in the transaction and transaction verification in respect of customer and other transactions prior to the commencement of the commercial arrangement, business relationship or transaction;
- (c) documenting and maintaining records of transactions³³⁶;
- (d) recognizing and recording suspicious transactions as well as threshold transactions and applicable property under the TPA or freezable assets under the UNSEC Implementation Act and establishing clear procedures for ensuring the required reports are made in relation to these matters;
- (e) ensuring compliance with relevant legislation, and co-operation with enforcement authorities;
- (f) internal audit checks to ensure compliance with policies and procedures relating to money laundering, terrorist financing and proliferation of weapons of mass destruction;

³³⁴ Section 94(6), POCA.

³³⁵ Reference POC (MLP) Regulations, Reg 7 and the fourteen-day time period discussed throughout the Guidance Notes.

³³⁶ POC (MLP) Regulations, r. 14(4).

- (g) the training of staff in the operation and implementation of procedures and controls relating to the combatting of money laundering, terrorist financing, the prevention of the proliferation of weapons of mass destruction activities and their obligations under the law;
 - (h) communication of group policies and procedures on the detection and prevention of money laundering, terrorist financing, and the proliferation of weapons of mass destruction activities and the monitoring of compliance by all subsidiaries and branches whether located in Jamaica or overseas.
248. A financial institution shall adopt a consolidated approach to the establishment and implementation of its AML/CFT/CPF policies and procedures, which shall cover the activities of all local and foreign branches, subsidiaries³³⁷. In this regard financial institutions should note the relevant sections of these Guidance Notes regarding the obligations for financial holding companies, and responsibilities in respect of branches and subsidiaries.
249. A failure to carry out the requirements at paragraph 245 or 246 above will constitute a breach of the BOJ’s AML/CFT/CPF Supervisory Rules.

Section VIII—Board Responsibility and Employee Integrity and Awareness

Board Responsibility

250. The board of directors of a financial institution must have a clear understanding of the ML/TF/PF risks faced by the financial institution³³⁸. This includes a good working knowledge of the operating risks faced by the institution (i.e. based on the services and products offered, customer base, strength of internal controls and hiring policies). The board must also be actively aware of risks posed to the financial institution where it resides within a financial group or within a broader corporate structure as well as the broader risks posed to the financial institution from a national perspective. Risks from the national perspective include broader concerns:
- i. performance of the economy; levels of crime and types of crimes to which financial services are most vulnerable;
 - ii. the country’s external ratings in the areas of- credit risk; and
 - iii. transparency, cooperation, and inclusion in watch lists or lists which require other countries to apply certain economic measures (including financial sanctions) before or when undertaking dealings with the country.
- (a) The board of a financial institution must therefore be satisfied that:—
- (i) the institution’s risk assessment accurately and appropriately reflects the ML, TF and PF risks faced by the institution and accurately reflects the effectiveness of the institution’s measures to address these risks, and is updated to ensure that this objective is met on an ongoing basis;
 - (ii) the employee who is appointed to carry out the function of the nominated officer is appropriately qualified and has the requisite stature and authority to undertake the responsibilities of that function and to effectively execute that function³³⁹ (refer to Section VI). In this case ‘authority’ means, sufficient authority within the financial institution such that issues raised by this employee receive the necessary attention from the board, senior management and business lines;
 - (iii) that the reports by the nominated officer are provided in a frequency that accords with the risk profile of the financial institution and ensures the board is at all times fully aware of the ML/TF/PF risks faced by the institution and of the effectiveness of the institution’s measures to address these risks; and
 - (iv) that the institution has adequate policies and processes for screening prospective and existing staffer employees to ensure high ethical and professional standards.
- (b) the board must ensure that the institution’s AML/CFT/CPF policies and procedures are effectively implemented. This means—
- (i) implementation in a manner which accords with functional implications, i.e. areas comprising front line functions; high levels of interaction with the public; sensitive functions (such as cash transactions, cash management functions, treasury functions; preparation of accounts, data input and analysis), compliance and oversight functions should be subject to the more intensive and most frequent levels of AML/CFT/CPF training and information;
 - (ii) ensuring the internal audit function assesses the risk management practices and internal controls of the institution including periodically assessing the effectiveness of the institution’s compliance with its AML/CFT/CPF policies and procedures;
 - (iii) compliance and oversight functions are provided with adequate or sufficient resources to ensure that AML/CFT/CPF policies and procedures are effectively implemented; and
 - (iv) ensuring the institution’s compliance with its AML/CFT/CPF policies and procedures are reviewed by external auditors³⁴⁰.

³³⁷ FATF Recommendation 18.
³³⁸ Basel Committee on Banking Supervision – Sound management of risks related to ML and FT, January 2014 – www.bis.org.
³³⁹ Ibid.
³⁴⁰ POC(MLP)Regulations regulation 5(1)(d); TPA section 18(2)(d).

- (c) the board must ensure it receives training and adequate and appropriate exposure to training materials and updates on the local AML/CFT/CPF laws and framework as well as the international standards and best or sound practices which impact AML/CFT/CPF obligations for financial institutions³⁴¹.
- (d) A failure to carry out the requirements at (b) or (c) will constitute a breach of the BOJ’s AML/CFT/CPF Supervisory Rules.

Employee Integrity and Awareness

251. Financial institutions need to be cognizant of the risks attached in having inadequate hiring policies and in having inadequate systems to deal with for instance, dishonest employees, since the success of an institution’s AML/CFT/CPF programme depends to a large extent on the integrity of its employees. Additionally, financial institutions are mandated to establish and implement appropriate policies and procedures³⁴² to ensure that (where applicable and as far as possible) employees are “fit and proper” persons.

Tolerating the continued rotation of unscrupulous or dishonest employees within the financial system exposes financial institutions to AML/CFT/CPF risks and to increased possibilities of AML/CFT/CPF breaches. As such unscrupulous or dishonest employees should be subject to the appropriate disciplinary action and prosecution, where the circumstances warrant this. Such persons should not be permitted to move through the financial system due to the insufficient disclosure or the absence of full and frank disclosure of the activities of such employees. (A classic example of this is an employee who has been found to be colluding with customers to commit fraud against the financial institution and who, instead of being fired and prosecuted, is given the option of resigning quietly, leaving this person to continue to seek employment within the financial system with another unsuspecting financial institution. In some cases, employer references are still provided in relation to such persons.) This will no doubt remain an issue that must be balanced against the hazards of lawsuits by such employees and as such financial institutions will need to work closely with their legal advisors on how such matters should be addressed.

Know Your Employee

252. Potential candidates for employment must be subject to a comprehensive screening process, which shall involve a thorough investigation of that candidate’s background (including employment and financial history (including credit history), and criminal background), honesty, competence and integrity.
- (a) In relation to staff or employees, financial institutions are expected to have in place the requisite policies and procedures that permit or facilitate or allow ongoing monitoring of an employee’s—
 - (i) Competence to undertake the role or position to which the employee is assigned;
 - (ii) Legal compliance with the statutory obligations that may apply to the employee specifically (such as income tax requirements, professional standards and requirements, obligations under the corruption prevention laws);
 - (iii) General character (e.g. tendencies to commit minor infractions and outright offences);
 - (iv) General compliance with the institution’s policies and procedures;
 - (v) Adherence with ethical practices and conduct;

- 252A. Behaviours exhibited which accord with ethical and moral standards - behaviours in this category generally include:
- 1. The ability to be forthright;
 - 2. Absence of or prompt declaration of conflict of interest issues;
 - 3. Absence of a culture of loophole mining -whether with internal policies or in relation to the institution’s statutory obligations;
 - 4. Culture of compliance - with internal policies and with the institution’s statutory obligations;
 - 5. Absence of tendency or propensity to lie, cheat, mishandle the institution’s property-including borrowing without permission, stealing, handling the property so recklessly or negligently - whether or not this results in damage to the property.

A failure to carry out appropriate preventive measures such as or akin to those described above at paragraph 252 above will constitute a breach of the BOJ’s AML/CFT/CPF Supervisory Rules.

253. Financial institutions must also institute processes geared towards ensuring the continued maintenance of a high level of integrity and competence among staff. These must include:—
- (a) Establishment of a Code of Ethics to guide employee conduct;
 - (b) Establishment of a ‘whistle blower’ policy and processes to guide whistleblowing³⁴³;

³⁴¹ Please see the BOJ’s Standards of Sound Practice for Corporate Governance issued 2025 for general principles on the duties and responsibilities of the Board. Non-compliance with these standards may be deemed an unsafe and unsound practice which may result in Supervisory action being taken pursuant to section 109 of the Banking services Act, 2014.

³⁴² POC (MLP) Regulations, r. 5; TPA section 18.

³⁴³ Jamaica’s whistleblowing legislation - The Protected Disclosures Act, 2011 took effect in August 2012 and mandates employers to implement a protected disclosures framework for the workplace (Section 13).

- (c) Regular review of employee’s performance and adherence to internal policies and procedures including codes of conduct and AML/CFT/CPF requirements;
- (d) Imposition of appropriate disciplinary actions for breaches of the institution’s AML/CFT/CPF policies and procedures;
- (e) Imposition of appropriate disciplinary actions or taking other appropriate action where an employee is convicted for committing an offence that involves dishonesty or for committing an offence which can result in a designation of criminal lifestyle being applied in accordance with section 5 of the POCA; and
- (f) Close scrutiny and investigation of employees whose lifestyles cannot be supported by his or her known income.

A failure to carry out appropriate preventive measures such as or akin to those described above at paragraph 253 will constitute a breach of the BOJ’s AML/CFT/CPF Supervisory Rules.

*Education and Training*³⁴⁴

- 254. In order to ensure full implementation of the procedures, recommendations, and requirements contained in these Guidance Notes, the staff/employees of financial institutions must be made fully aware of the serious nature of money laundering crimes, terrorism financing activities and proliferation of weapons of mass destruction activities. Furthermore, efforts must be made to ensure that all staffer employees understand the basic provisions of the POCA, the POC (MLP) Regulations, the TPA and the TP (Reporting Entities) Regulations and the UNSCRIA.
- 255. Members of staff/employees must also be sensitised as to their personal obligations under the POCA and the TPA and the UNSCRIA and the fact that they can be held personally liable for failing to report relevant information to the designated authority (in the case of nominated officers) or otherwise failing to carry out their responsibilities under the relevant statutes. Against this background, training must be designed and disseminated on an on-going basis.
- 256. In considering the impact of the regime in this regard, financial institutions must bear in mind the defences that can be raised by a person charged with any of the foregoing offences. Under the POCA, not only can a person raise the defence that he or she did not know or suspect that another is engaging in money laundering, he/she can also claim that additionally, the requisite training was not provided to him or her by the employer³⁴⁵. The defence appears to require proof of both elements (i.e. lack of knowledge/suspicion and lack of training) in order to be successfully raised. Under the TPA a defence of having a reasonable excuse for not making a report (re: assets held for listed entities or STRs) can be raised in relation to proceedings for an offence under section 15 or section 16). The term ‘reasonable excuse’³⁴⁶ is not defined in the TPA. Additionally, a staff member (other than the nominated officer), who is charged with an offence of not making a report under section 16, can raise the defence that the information or other matter, was disclosed to the nominated officer in accordance with the procedures established pursuant to section 18 of the TPA.
- 257. Compliance with this requirement to train employees is perhaps best achieved in systems which trigger automatic training requirements on the occurrences of certain events e.g.—
 - (a) Employment;
 - (b) Promotion/lateral movement to sensitive or frontline duties;
 - (c) Expiration of minimum period since last training session which triggers refresher requirements;
 - (d) Where new products, services and delivery channels are onboarded;
 - (e) Where new processes are designed and implemented;
 - (f) Legislative, regulatory and guidance amendments;
 - (g) Where risk assessment vulnerabilities/control breakdowns are identified; and
 - (h) Where emerging risk typologies are observed and new threats emerge.
- 258. Training initiatives can either be confined to scheduled sessions or expanded to include spontaneous spot checks within randomly selected areas of operation both in-house (i.e. via Department, or via frontline staff operations, or via sensitive operations) or randomly selected branches and subsidiaries. A mixture of such processes is likely to result in a more robust system that can quickly reveal shortfalls for the managements’ attention as against relying on a system that is confined to scheduled, standard one style of training method which is less likely to readily reflect shortfalls and areas of weakness that can be quickly addressed.

³⁴⁴ See POCA (MLP) Regulations MLA section 7(2)(c).
³⁴⁵ See the POCA section 94(6).
³⁴⁶ Stroud’s Judicial Dictionary of Words and Phrases - discusses the meaning of the term ‘reasonable excuse’ with case law speaking to the meaning of the term — in a number of circumstances including ignorance of a requirement to act; honestly and reasonably believing the activity does not amount to a prohibited activity; failure to comply with a requirement on the basis of fear of self-incrimination. (8th edition. Volume 3).

259. Financial institutions must ensure that satisfactory steps are taken to confirm/prove that training of employees took place. Such steps may include, but are not limited to the following:
- (a) Ensuring such sessions are subject to rigorous registration systems (including online registration) that require signing by trainees and or trainers and true records of the training session documented and retained in formal training registers; and /or
 - (b) Online recordings/documentation of scheduled training sessions (best used in seminar type training scenarios). Where training is provided in an online setting and there is a recording of the session, participants must be aware that the session is being recorded; and
 - (c) Delivery of documented certifications to employees evidencing satisfactory completion of training session; and
 - (d) Separate verification of the training sessions having taken place by the nominated officer; and/or
 - (e) Sign off on the sessions taking place by the Board of the financial institution as a part of the audited annual report of the financial institution.
260. Financial institutions must therefore introduce programmes to ensure that staffer employees, are informed of their responsibilities, and encouraged to provide prompt notification of suspicious as well as threshold transactions. The timing and content of training for staff or employees shall cover all critical areas of operation from senior management through to ‘rank and file’ and be tailored according to the risk profile of the institution, job functions and responsibilities and the risk factors to which employees are exposed due to their functions and responsibilities. This means ensuring ease of access to the requisite policies and manuals is afforded to staffer employees at all levels by for instance:—
- (a) ensuring such documents are available on internal electronic access (e.g. intranets);
 - (b) ensuring sufficient copies are placed in resource centres or libraries in-house; and
 - (c) ensuring the timely circulation of updates and amendments throughout the institution network (i.e. head office to branches and representative offices and parent companies to subsidiaries.)
261. Training/education programmes must be designed and implemented on an ongoing basis by individual institutions to ensure employees’ awareness of:—
- (a) Current as well as new and developing AML/CFT/CPF laws, regulations, standards and guidelines being established both locally and internationally;
 - (b) Their legal obligations and responsibilities to prevent and detect money laundering and terrorism financing and proliferation of weapons of mass destruction;
 - (c) New money laundering and terrorism financing techniques, methods, typologies and trends;
 - (d) The institution’s own AML/CFT/CPF policies and procedures.
262. In developing education and training programmes³⁴⁷, particular emphasis needs to be placed on the following categories of staff:
- (a) **New Employees/Staff.** All new employees/staff, irrespective of their level of seniority, must be informed as to the background and nature of money laundering and terrorist financing and proliferation of weapons of mass destruction and the need for reporting suspicious and threshold transactions to the designated authority, through the institution’s Nominated Officer. They shall be made aware of their personal legal obligation as well as that of the institution, to report suspicious transactions. As mentioned above, institutions must also institute appropriate screening processes so as to thoroughly investigate the background, honesty, and integrity of prospective employees.
 - (b) **Front Line Staff/Employees.** The first point of contact of an institution with potential money launderers or persons attempting to finance terrorist activities and proliferation of weapons of mass destruction, is usually through staff/employees who deal directly with the public. ‘Front-line’ staff members/employees (such as Tellers, Cashiers and Foreign Currency Staff, and Receptionists) shall therefore be provided with specific training on examples of suspicious transactions and how these may be identified. They must also be informed about their legal responsibilities and the institution’s reporting systems and procedures to be adopted when a transaction is deemed to be suspicious. Additionally, they must be informed as to the institution’s policy for dealing with occasional customers and ‘one-off’ transactions, particularly where large cash transactions are involved.
 - (c) **Account Opening/Customer Service Staff/Employees.** Members of staff/employees who deal with account opening or the approval of new customers must receive the training given to tellers etc. in (b) above. They must also be trained as to the need to verify the identity of a customer and the institution’s account opening and customer verification procedures. They must further be advised that a business relationship or ‘one-off transaction shall not be established or continued beyond the statutory period of fourteen days³⁴⁸ until the identity of the customer is verified. Staff or employees must also be made aware that the offer of suspicious funds or the request to undertake a suspicious transaction must be reported to the Nominated Officer, whether the funds are accepted or not, or the transaction proceeded with, or terminated.

³⁴⁷ Interpretive Note to FATF Recommendation 18.
³⁴⁸ R. 7 (l)(ii)POC (MLP) Regulations as amended in 2019.

- (d) Administration/Operations Supervisors and Managers. A higher level of instruction covering all aspects of AML/CFT/CPF procedures shall be provided to persons with the responsibility for supervising or managing staff. Such training must include familiarisation with the offences and penalties arising under the POCA, TPA and UNSCRIA, the procedures relating to account monitoring orders and production orders, and customer information order and disclosure orders, the requirements for non-disclosure and for retention of records, and management’s specific responsibility vis-a-vis dealings with customers in accordance with the risk profiles applicable to those customers.
263. A failure to carry out any of these requirements at paragraphs 258, 259 or 260, 261 or 262 will constitute a breach of the BOJ’s AML/CFT/CPF Supervisory Rules.

Section IX—Transaction Monitoring and Reporting

Required Disclosures - Recognition And Reporting of Suspicious Transactions
and Findings in Relation to Unusual Transactions

264. A suspicious transaction will often be inconsistent with a customer’s known legitimate business or personal activities or with the normal business for that type of account or with the nature of the transaction indicated. Hence, general knowledge of the nature of the industry or sector in which the customer operates and the nature and pattern of the customer’s own business, and a good understanding of the operating environment and the banking processes that would be applicable to the various services and products offered, are the first set of elements in recognizing a suspicious transaction or an unusual transaction or series of transactions.
265. Section 94(3) of the POCA states that a required disclosure *is a disclosure of information or other matter on which the knowledge or belief is based or which gives reasonable grounds for the knowledge or belief that another person has engaged in a transaction that could constitute or be related to money laundering, that is made to either the nominated officer³⁴⁹ or to the designated authority*. Under the TPA the suspicious transaction reporting obligation is Stated a little differently, it refers to each entity reporting to the designated authority, all transactions, whether completed or not, which the entity suspects, or has reasonable cause to suspect involves property connected with or intended to be used with the commission of a terrorism offence or involve, or are for the benefit of, any listed entity or terrorist group. Reporting to the designated authority is subject to use of a statutory form³⁵⁰. The UNSCRIA as amended in 2019 imposes similar obligations to POCA and the TPA. Under the UNSCRIA each entity is required to report to the designated authority any transaction or attempted transaction believed or known to be related to a person or entity proscribed by the regulations or an order made under the UNSCRIA.³⁵¹ Reporting to the designated authority is subject to use of a statutory form³⁵².
266. The law reflects that a required disclosure under the POCA, TPA or UNSCRIA is one that should be made to the nominated officer or designated authority³⁵³. In practice, and for good order reports of regulated businesses and reporting entities must be made to the designated authority through the nominated officer who will thereafter be required to make a disclosure in the statutory form to the designated authority; and
267. In complying with the obligation to report suspicious transactions under the POCA, TPA and UNSCRIA, a financial institution is also required to:—
- (a) pay attention to ³⁵⁴ (or identity and take notice of)—
 - (i) complex, unusual or large business transactions or unusual large transactions carried out by the customer with the financial institution; and
 - (ii) unusual patterns of transactions whether completed or not which appear inconsistent with the known business history of that customer.
 - (b) make and retain a record of the transactions whether complete or not at (a) and the related findings for a period not less than seven years³⁵⁵;
 - (c) where the circumstances occur in relation to s. 16(2) of the TPA ensure that the findings and transactions are made available, on request, to its auditors and to the designated authority³⁵⁶. The POCA and TPA require findings and transactions to be treated in the same manner whereby such information should be available on request to auditors, a supervisory authority or the competent authority and reported to the designated authority under POCA and TPA³⁵⁷.

³⁴⁹ See also Part VI above the legislative amendments to the Nominated Officer Regime.

³⁵⁰ Regulation 17(2) of the TP (Reporting Entities) Regulations, 2010.

³⁵¹ See paragraphs above outlining the full suite of obligations.

³⁵² Section 5 (3) and 3A as amended in 2019 and UNSCRIA (Reporting Entities) Regulation 6.

³⁵³ POCA section 94(3); TPA section 18(3) re: a section 16(3) report (unusual transactions) & section 16(3A) re: a STR).

³⁵⁴ Section 94(4)(a)-POCA; section 16(3)(a) TPA, section 5(3) and (3A) UNSCRIA.

³⁵⁵ Section 94(4)(a) POCA as amended in 2019 and; section 16(2) TPA as amended in 2019. As a reminder these records should be kept for not less than 7 years or some other period as the competent authority indicates in writing.

³⁵⁶ Section 94(4)(b) POCA...(but only in relation to transactions involving customers in territories listed in accordance with this section. In this case findings should be available on request to a supervisory authority or competent authority concerned. Auditors are not mentioned in the POCA; section 16(3)(b) of the TP(Amendment) Act, 2011.

³⁵⁷ UNSCRIA requires all reports made under subsection 3A to be disclosed to the BOK as regulator of FIs. Discussed above.

- (d) apply enhanced due diligence measures to all business relationships and transactions with any customer resident or domiciled in a territory specified in a list of applicable territories published by notice in the Gazette by a supervisory authority for the purposes of section 94A of the POCA and 16A of the TPA and ensure that the findings are in writing and available upon request to the Designated Authority, Supervisory Authority or the Competent Authority.
268. When a financial institution is faced with a situation or circumstances in respect of which it would be reasonable for a required disclosure (i.e. STR) to be made, that institution must either—
- (a) refuse to conduct the transaction; refuse to commence the relationship or decline from undertaking any business arrangements in respect of the customer or transaction or arrangement that is deemed suspicious; or
 - (b) if the institution is placed in a position where it is of the view that it must proceed with the transaction, relationship or arrangement, then the institution must ensure that the relevant disclosure has been made and appropriate consent from both the Nominated Officer and Designated Authority to proceed is in place (see POCA sections 93(2), 99(1 & 2) and 100 (4) & (5))
269. A financial institution must ensure that reports made to the Designated Authority by the institution are followed up by the Nominated Officer or his/her highly ranked designate, such that at any time an institution is called on, it is in a position to provide more information than merely that “the matter was reported to the designated authority”. The institution shall also ensure that the account or transaction is followed up and regularly analysed and it must be clear from the records of the institution, the point at which a determination was made by the institution to Seek the appropriate consent of the Designated Authority to apply appropriate counter measures to safeguard the institution. Countermeasures include action to:
- (a) close the account;
 - (b) end the business relationship;
 - (c) terminate the transaction;
 - (d) scale down services;
 - (e) refuse to undertake transactions above or under a certain amount;
 - (f) refuse to undertake new business with the customer;
 - (g) refuse to accept introduced business from that customer or in relation to that customer.

A failure to comply with this requirement will amount to a breach of the AML/CFT/CPF Supervisory Rules.

270. The application of appropriate Countermeasures by a financial institution will be indicative of a financial institution acting to protect itself and the integrity of the overall financial system. Such steps may ultimately be the determining factor in whether an institution is viewed as “complicit” in its dealings generally or with the customer; and whether it is negligent or is recklessly aiding and abetting the customer/(s) in question. In complying with their obligations under the POCA, or the TPA (whichever is applicable) in this regard, Financial institutions must consult closely with their respective legal advisors.
271. Financial Institutions shall also note the following—
- (a) if the institution is placed in a position where it is of the view that it must proceed with the transaction, relationship or arrangement, and in the institution’s view the circumstances do not permit the institution to make the relevant disclosure and secure the appropriate consent before proceeding, then the institution must ensure that the relevant disclosure is made on its own initiative and as soon as is reasonably practical for this to be done. (Section POCA 100(4) & (5)³⁵⁸);
 - (b) acting in accordance with (a) above does not necessarily absolve the institution from making the requisite disclosure or obtaining the appropriate consent, in relation to the continued offering of any service or facility or in transacting further business in relation to the customer or the property in respect of which the knowledge or belief that criminal activity is taking place was formed. For the avoidance of all doubt, institutions must actively seek the necessary guidance, directive or consent from the designated authority before proceeding in any manner.

A financial institution must therefore satisfy itself that the direction or consent obtained from the designated authority clearly permits or prohibits the doing or undertaking of any activity in relation to accounts, transactions, customers or property in respect of which authorised disclosures have been made.

272. Financial institutions shall have adequate systems in place to ensure the timely, ongoing detection and reporting of complex, unusual or large transactions, or of holdings of property owned or controlled by a listed entity, or a proscribed entity, suspicious and threshold transactions, and bring these to the attention of the relevant authorities.

³⁵⁸ A similar provision is found at section 93(2) which from the general wording appears applicable generally to persons other than a person who is a business in the regulated sector.

- (a) Financial Institutions must also be in a position to make their findings in this regard available to BOJ, whether during on-site examinations which includes an assessment of the institutions’ AML/CFT/CPF systems or otherwise on request. These findings must also be available to the Designated Authority³⁵⁹.
 - (b) Financial institutions are reminded that not only is an institution’s failure or inability to comply with its statutory reporting obligations an offence under POCA, the TPA and UNSCRIA but that, such failures can also constitute behaviour in respect of which remedial action can be directed or imposed on institutions under their respective governing statutes, for instance by the Supervisor pursuant to section 109 of the BSA. Additionally, under paragraph 2 of Part A to the Fifth Schedule to the BSA, an institution which is a licensee under the BSA can also be deemed to be engaging in unsafe or unsound practices. Any deficiencies in the systems, which place the institution in breach of its obligations under the governing statutes may also be reported to the Designated Authority.
 - (c) The POCA is silent on the matter of the availability of an institution’s records pertaining to documented findings being available to its external auditors. An institution may be guided by section 97(2)(b) of the POCA which outlines disclosures made under certain circumstances, which would not be deemed as “tipping off. Note that the POCA section 97(2) (a-d) lists the categories of persons to whom disclosures can be made and this list does not include Auditors. Subsection (b) specifically speaks to circumstances where the disclosure is made in carrying out a function the person has relating to the enforcement of any provision of the POCA or of any other enactment relating to criminal conduct or benefit from criminal conduct. A financial institution will however be expected to exercise discretion and judgement to ensure that in-house disclosures to internal auditors and disclosures to external auditors³⁶⁰ occur only to the extent and in a manner that will allow those critical functions to carry out their obligations under POCA and its Regulations. In addressing this issue financial institutions must consult closely with their respective legal advisors.
273. There are certain categories of activities that are suspicious by their very nature, and should alert a financial institution as to the possibility that a customer is seeking to conduct illegal activities at/through the institution. Examples of such suspicious conduct and activities are outlined in Appendix V. This listing is not intended to be exhaustive, and only provides examples of the most basic ways by which money may be laundered and forms the catalyst for prompting enquiries about the source of funds and source of wealth and for applying enhanced due diligence measures. Financial institutions must also keep themselves informed as to the constantly evolving methods (i.e. typologies) of money laundering and terrorist financing and proliferation of weapons of mass destruction. Financial institutions must note that under the POCA and TPA, any offence in Jamaica can constitute a *predicate offence*. This is an expansion of the category under the repealed Money Laundering Act of offences in respect of which a charge of money laundering could be laid. Therefore, required disclosures (STRs) should be made in cases where there is suspicion that the transaction being conducted is facilitating theft of funds, funds received through, for instance, insider trading activities, funds diverted to evade the payment of taxes or to otherwise deprive the Government of revenues, funds comprising bribes or diversion of public funds and so forth.
274. The reception point for disclosures under the POCA, the TPA and UNSCRIA (whether these are suspicion-based reports or reports of transactions at or above threshold limits or reports re: asset holdings) is the Designated Authority. Financial institutions also need to ensure that the requisite statutory reporting forms are properly completed to facilitate the investigatory process that may be undertaken as a consequence of the report and to ensure compliance with reporting obligations is achieved.
275. Financial institutions shall establish systems that ensure all matters identified for reporting under the POCA, TPA and UNSCRIA, are brought to the attention of the Nominated Officer. Each case must then be reviewed at that level to determine whether the suspicion is justified, and in the absence of factual information to negate the suspicion, the Nominated Officer should expeditiously submit a report to the Designated Authority, within the stipulated statutory period, where applicable. In this regard it should be noted that both the POCA and TPA speak to making the required disclosure or report “*as soon as is reasonably practicable and in any event within fifteen days*”³⁶¹. The specific steps that must be followed for the reporting of such transactions must be clearly outlined in the policy manual and communicated to all relevant personnel. The following must also be noted:—
- (a) The POC (MLP) Regulations, UNSCRI (Reporting Entities) Regulations and TP (Reporting Entities) Regulations, provide for the use of standard reporting formats³⁶², which must be adopted.
 - (b) The POCA has established the following reporting and feedback regime for required disclosures.
 - (i) Where circumstances in which a required disclosure must be made arise, then in the case of persons operating in a regulated business (e.g. financial institutions) the matter must be brought to the attention of the Nominated Officer within fifteen days of the incident occurring (i.e. the suspicious transaction, and/or the realization being formed that the transaction is suspicious).

³⁵⁹ Section 94(4)(b) - POCA.

³⁶⁰ POC (MLP) Regulation 5(2)(d); TPA section 18(2)(d).

³⁶¹ POCA section 94(2)(c); and the TPA section 16(3) as amended in 2019.

³⁶² POCA (MLP) Regulations, 2007 Schedule to r. 17 Forms I and II; and TP (Reporting Entities) Regulations, 2010 Schedule to regulation 17 Forms 1 and 2; UNSCRI(Reporting Entities) Regulations, 2019 Regulation 6 and referenced Schedule.

- (ii) After assessment/analysis of the matter with the institution’s Nominated Officer, if the determination made is that the matter qualifies as one in which a required disclosure shall be made then the Nominated Officer must make the required disclosure within fifteen days after the information or matter comes to that officer’s attention.
- (iii) The required disclosure takes place in the form prescribed by the POC(MLP) Regulations and is made to the Designated Authority.
- (iv) The financial institution’s treatment of the matter subsequent to the required disclosure being made must be in accordance with the statutory feedback regime termed “appropriate consent” which can be found under sections 91 and 99 of the POCA.

Appropriate consent regime

276. In the case of financial institutions- “appropriate consent” exists.

- (a) After the Nominated Officer makes a disclosure to the Designated Authority, and that employee has received a response from the designated authority within seven days (exclusive of weekends & public holidays and starting the day after the disclosure is made), consenting to the Nominated Officer undertaking a prohibited act; (s.99(1)(a)) subject to 91(3) of the Proceeds of Crime Act.
- (b) After the Nominated Officer makes a disclosure to the Designated Authority, and that Nominated Officer has not received notification from the Designated Authority within the seven days’ notice period prohibiting the Nominated Employee Officer from undertaking a prohibited act; (s. 91(2)(b)(i) and 99) (1)(b)).
- (c) After the Nominated Officer makes a disclosure to the Designated Authority, and that Nominated Officer has received notification from the Designated Authority within the seven days’ notice period prohibiting the Nominated Officer from undertaking a prohibited act but ten days have passed since the receipt of that notice; (s. 91(2)(b)(ii) and 99(1)(c). It should be noted that the relevance of this ten-day period is used to ensure that if by the expiration of that period no further action has been taken by the relevant authorities in relation to the matter disclosed, the financial institution is deemed to have attained the status of “having the appropriate consent” to undertake the prohibited act. Further action would include steps such as obtaining a court order restraining the financial institution from dealing with the property in question³⁶³.
- (d) The POCA provides for the consent or refusal of consent by the Designated Authority to be verbally communicated to the reporting regulated business, however this must be followed up within five days by the written notification. (S. 99(4)).
- (e) If the institution is placed in a position where it is of the view that it must proceed with the transaction, relationship or arrangement, and in the institution’s view the circumstances do not permit the institution to make the relevant disclosure and secure the appropriate consent before proceeding, then the institution must ensure that the relevant disclosure is made on its own initiative and as soon as is reasonably practical for this to be done. (Section 93(2), 99(1 & 2) and 100(4) & (5)).

277. The detailed reporting and feedback regime for required disclosures established under the POCA are not in place under the TPA or the UNSCRIA. It is therefore expected that in so far as business efficiency is concerned and the extent to which the practicalities and legality of the situation permits, financial institutions may consider implementing a similar reporting and feedback regime for matters arising under the UNSCRIA and TPA frameworks in consultation with the Designated Authority. However, financial institutions must bear the following in mind—

- (a) The concept of appropriate consent is not statutorily established under the UNSCRIA or TPA as such the statutory indemnities that accompany that regime will not be applicable. In relation to the 2021 UNSCRIA (DPRK Sanctions Regime), there is an approval mechanism that may be engaged by application to the Minister.³⁶⁴
- (b) STRs arising under the TPA framework must be reported to the Designated Authority within fifteen days. (Under the POCA framework there is a maximum thirty days window within which a regulated business must report a suspicious transaction to the Designated Authority - i.e. for the discovering officer to report the matter giving rise to the suspicion to the Nominated Officer within fifteen days of the matter that is the cause of the suspicion; and then the Nominated Officer has to report the matter to the designated authority within fifteen days of the matter coming to the attention of that officer.) Under the UNSCRIA as amended in 2019, the obligation is simply to report to the Designated Authority, in which case it is best the financial institution remains vigilant and makes a report as soon as it has identified or becomes aware of any instance or circumstance in which a report should be made.

³⁶³ K. Ltd. v. National Westminster Bank plc. [2006] EWCA Civ. 1039 70KB All ER.(D) 131 (Jul).

³⁶⁴ The UNSCRIA (DPRK -Sanctions Regime) Regulations, 2021 regulations 34-36.

278. Onward disclosures pertaining to suspicious transaction reports made, or investigations (whether pending or ongoing), under the POCA or under the TPA will not amount to an offence if³⁶⁵—

The circumstances of disclosure	POCA/TPA	Section
At the time of the disclosure the person did not know or suspect that the disclosure would be prejudicial to any investigations under the Act;	POCA	97(2)(a)
The disclosure is made pursuant to functions being carried out under the POCA or any other enactment relating to criminal conduct or benefit from criminal conduct;	POCA	97(2)(b)
The disclosure is to an attorney- at-law for the purpose of obtaining legal advice or for the purpose of the attorney- at-law giving legal advice and only where disclosures in this regard are not made with the intention of furthering a criminal purpose;	POCA TPA	97(2)(c); 97(3)(a) 17(1)(a); 17(2)(a); 17(3)(a)
The disclosure is made for the purpose of facilitating the investigation;	TPA	17(1)(b); 17(2)(b); 17(3)(b);
The disclosure is made pursuant to functions being carried out under the POCA or any other enactment relating to criminal conduct or benefit from criminal conduct;	POCA	97(2)(b)
The disclosure is to the competent authority;	POCA	97(2)(e)
The disclosure is to any person in connection with legal proceedings or contemplated legal proceedings;	POCA	97(3)
The disclosure is made for the purpose of any proceedings which might be conducted following the investigation	TPA	17(1)(b); 17(2)(b); 17(3)(b);

279. Apart from the foregoing exceptions, a financial institution is under strict obligations not to disclose to any person, the fact that it has made a required disclosure pursuant to sections 94 and 100 of the POCA, or made a disclosure pursuant to section 16(2) or 16(3) of the TPA and must comply with all directions given to it by the relevant authorities³⁶⁶. Based on the wording of the tipping off provisions in the POCA and TPA, the obligations thereunder are also applicable to the officers and employees of financial institutions. A financial institution is also under Strict obligations not to disclose to any person, the fact that it has made a disclosure pursuant to sections 5(3) and 5(3 A) of the UNSCRIA³⁶⁷.

Protected disclosures

280. The POCA has two provisions treating with the issue of protected disclosures. The first of these provisions can be found at section 100(3). This section states that disclosures made in the circumstances outlined in section 100 are protected from being interpreted as breaches of any disclosure restraints however imposed. The second provision is section 137 which contains a more broadly worded all-embracing statement that no civil or criminal proceedings for breach of confidentiality may be brought, nor any professional sanction for such breach taken, against any person, or a director or employee of an institution, who provides or transmits information requested by or submits reports to, the enforcing authority or competent authority under POCA³⁶⁸. A similar provision to section 137 can be found at section 16(7) of the TPA and at section 5(5) of the UNSCRIA.
281. A financial institution must decline to do any business (including opening an account) with a potential customer or take the measures outlined above at paragraph 113 in relation to existing customers if there are serious doubts about the bona fides of the individual or criminal involvement is suspected³⁶⁹. Where criminal involvement is suspected, the financial institution shall also seek to retain copies of relevant identification or other documents,

³⁶⁵ POC Section 97(2); TPA Section 17(2)

³⁶⁶ POC (MLP) Regulations, regulation 3(6); TP (Reprting Entities) Regulations, regulation 19

³⁶⁷ UNSCRIA, 2013 section 5(6)

³⁶⁸ Se 2019 amendment to POCA

³⁶⁹ POC (MLP) Regulations, 2007 & amended 2013, regulation 7(1)(b); See also TP (Reporting Entities) Regulations, 2010 regulation 5 (a); See also FATF Recommendation 10.

which may have been presented, and must consider reporting the offer of suspicious funds to the Designated Authority as discussed above.³⁷⁰ Where a business relationship has already commenced and the customer fails to provide requested follow-up information, the relationship shall be legally terminated unless otherwise advised by the law enforcement authorities. (See paragraph 114).

In seeking to terminate the relationship, financial institutions must be mindful of the prohibition against “tipping off” or unauthorised disclosures outlined under the POCA³⁷¹ and the TPA³⁷² and shall therefore be careful not to “tip off” customers, potential customers or any unauthorized person, where a suspicion has been formed by the financial institution that an offence is being attempted or has been or is being committed. Under POCA a “tipping off” offence occurs where a disclosure is made to another person containing any information or any other matter relating to a disclosure made under section 100, that is, a protected disclosure either in relation to a required disclosure or a money laundering investigation, has taken place. Under the TPA a similar offence occurs where information on actions or proposed actions of the Designated Authority relating to an investigation being conducted or about to be conducted in relation to a terrorism offence, or in relation to a report made under the TPA, is disclosed.

Where an institution forms the suspicion that criminal activity is taking place after a business relationship is established with a customer, the institution must seek to legally terminate arrangements where it is of the view that continuing the relationship could lead to legal or reputational risks due to the suspected criminal activity. (See paragraph 110 and paragraph 216(d) for guidance on transactions that though not suspicious, raise questions or are flagged for closer scrutiny and which in that case are still conducted.)

Section X

Record Keeping

- 282.(a) Once a business relationship has been formed, the financial institution is required to make and retain records of client information (KYC and CDD and transactions - refer to paragraphs 99 and 100 of these Guidance Notes as well as to the POCA, TPA and UNSCRIA legislation).
- (aa) The financial institution must also retain other particulars including records business correspondence exchanged between the financial institution and the customer, account files and the results of any analysis undertaken in relation to the customer or the account (including enquiries to establish the background and purpose of complex, or unusual large transactions)³⁷⁴. Clear standards must be outlined within the policy manual pertaining to record keeping including the minimum seven years retention period from the termination of the business relationship or after the transactions have been completed.
 - (b) Client files must contain account numbers and full customer identification information, account opening forms, copies of identification documents, business correspondence and other relevant CDD details. Transaction records must be maintained in such a form that would allow for reconstruction of individual transactions, to provide audit trails and if necessary, evidence for prosecution of criminal activity. At a minimum, this would therefore include the date and nature of the transaction and the amounts and types of currency used, if any.
 - (c) The FIDA, POCA, TPA, UNSCRIA and BSA each have provisions which require the retention and production of records, documents etc. to, or the access to records, documents etc. of financial institutions by, the designated authority or the competent authority. Financial institutions must therefore ensure that the records it retains are available to the designated authority and competent authority.
 - (d) Retention may be by way of original hard copies or original documents stored electronically or in digital form. Institutions which store original documents in a computerized form must bear in mind the requirements of the Evidence Act as regards the admissibility of documents via computer evidence.
 - (e) In circumstances where the records relate to on-going investigations by the law enforcement authorities, or to transactions that have been the subject of a disclosure order, they should be retained beyond the statutory period of seven (7) years at least until it has been confirmed by the Designated Authority that the case has been concluded or further retention is unnecessary.

In this regard, institutions that have made required disclosures pursuant to sections 94 and 95 of the POCA, or under section 5 of the UNSCRIA- or section 16 (3) of the TPA (i.e. suspicious transaction reports) to the Designated Authority must make it a point of duty to follow up with the Designated Authority for guidance on how future business with the accounts/ account holders in question must be conducted.

Financial Institutions must note that the **Electronic Transactions Act 2006** has been in effect since April 2007, In addressing record keeping requirements under the POCA, UNSCRIA or TPA in relation to electronic record retention, institutions must bear in mind the provisions of this Act particularly those treating with the issue of electronic retention of records (section 11); “requirements in keeping information” (section 12) “Admissibility and evidential weight of information in electronic form”.

³⁷⁰ POC (MLP) Regulations, regulation 7(1)(b); See also FATF Recommendation 10.

³⁷¹ POCA sections 97 and 104.

³⁷² TPA section 17 (2) & (3).

³⁷³ S 97(1)(a) of POCA as amended in 2019.

³⁷⁴ See POCA (MLP) Regulations, 2007 r. 14; TP (Reporting Entities) Regulations, 2010 regulation 14; UNSCRIA (Reporting Entities) Regulations, regulation 5; FATF Recommendation 11.

283. A failure to carry out any of the requirements in paragraph 282 will constitute a breach of the BOJ’s AML/CFT/CPF Supervisory Rules.

Section XI—Conclusion

284. These Guidance Notes are intended to bring to the attention of financial institutions, the minimum standards required of an effective programme to detect and deter money laundering and terrorist financing and proliferation of weapons of mass destruction. The Bank of Jamaica wishes to emphasize that the AML/CFT/CPF policies and procedures of financial institutions should be developed in accordance with the law and these Guidance Notes inclusive of Appendices, giving consideration to each institution’s risk profile, internal procedures and policies, and where applicable the policies of the financial group in which the financial institution resides.

Section XII—Appendices

1. APPENDIX I—Criteria for Designation as a ‘Permitted Person’ Under Section 101A of the POCA
2. APPENDIX II—Advisory issued by BOJ in May 2014-paragraph 25(c)
3. APPENDIX III—Designation Orders (Paragraph 96)
4. APPENDIX IV—Basic Duties and Responsibilities of the Nominated Officer (Section VI)
5. APPENDIX V—Examples of Unusual/Suspicious Activities
6. APPENDIX VI—Mandatory Obligations
7. APPENDIX VII—Bank of Jamaica’s Specified Territories Supervisory Authority Notice -(Paragraphs 75A and 193)
8. APPENDIX VIII—
 - i. BOJ’s Internal Procedure for Listing Entity Designations under Section 14 of the Terrorism Prevention Act
 - ii. UNSCR Sanctions list as at June 2025
9. APPENDIX IX—Advisory to Licensees on The Management of Cyber-Risks
10. APPENDIX X – Formal Order Dated March 12, 2026 pursuant to section 3a(2) of UNSCRIA Re: proscribed persons and entities relevant to iran reapplied as of September 27, 2025. (Paragraphs 13A and 231A)

Appendix I

Criteria for Designation as a ‘Permitted Person’ Under Section 101A of the POCA

1. According to the Guidance from the Ministry of National Security³⁷⁵, the criteria stipulated below must be fulfilled in order for the applicant to qualify for ‘permitted person’ status under section 101A of the Act.
 - (a) Demonstration of a true need for ‘permitted person’ status. Information provided in support of this requirement must include data on the frequency of cash transactions in excess of the prescribed amount carried out by the applicant over the past 3 years preceding the application;
 - (b) In the case of financial institutions, the applicant must have a Regulator, which monitors the entities day to day operations on an active basis. It must be licensed and the substantial owners, directors and managers (as applicable) should be subject to statutory ‘fit and proper’ requirements and processes;
 - (c) In the case of financial institutions, such applicants should produce written confirmations from the respective Regulator and the Financial Investigation Divisions (FID) that there is no objection to the granting of ‘permitted person’ status to the applicant³⁷⁶;
 - (d) In all cases, the applicant must have proper and demonstrable systems and mechanisms in place against money laundering and counter-terrorism financing (ML/CTF), that protect the applicant from the risks of the applicant being involved in money laundering or the financing of terrorism. The Ministry has indicated further that at a minimum, this should include documented measures to ascertain the identity of persons carrying out transactions of this nature; recording of transactions in detail; staff training; appointed officer to monitor compliance with the procedures, as well as procedures for reporting suspicious transactions to the designated authority under POCA; and obtaining authorized consent where necessary.
2. The Ministry has further indicated that—
 - (a) all applications for ‘permitted person’ status are considered on the individual merit of each case.

³⁷⁵ Developed by the Ministry of National Security in August, 2014

³⁷⁶ This now has to be looked at against the background of the amendment in 2019 to section 1011 A which in relevant part states that that the Minister in exercising his discretion does so after written consultation with the designated and competent authorities and the competent authority shall for that purpose submit a written assessment of the risks of money laundering and terrorist financing relating to the person or transaction concerned.

- (b) the Minister may withdraw or rescind any Order granted under section 101A in any case where:
 - (i) The applicant has provided misleading information in making an application;
 - (ii) Either the FID or the Regulator advises the Minister that the exemption should no longer apply to the Applicant;
 - (iii) The applicant has failed to implement or adhere to the procedures referred to at 1 above; and
 - (iv) The applicant or any of its principals, shareholders or managers has been charged or convicted of any crime relating to the operations of the Applicant.

Full details of the criteria to be met to obtain ‘permitted person’ status and the requisite application procedure and other details can be accessed from the Ministry of National Security.

Appendix II - Advisory issued by BOJ in May 2014

(Paragraph 25 (C))

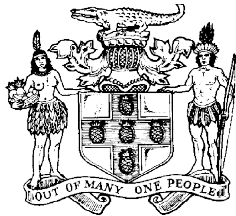
Advisory

Section 101A Proceeds of Crime Act

Based on information that has come to the Bank’s attention, the Bank wishes to provide the following advisory on carrying out banking cash transactions in excess of J\$1,000,000.00.

Section 101A of the Proceeds of Crime Act states that, a person shall not carry out a cash transaction in excess of J\$1,000,000.00, unless such transaction is undertaken with a permitted person. A ‘permitted person’ includes a bank licensed under the Banking Services Act, a licensed deposit taking institution regulated by Bank of Jamaica, a person licensed under the Bank of Jamaica Act to operate an exchange bureau or any other person that may be designated by the Minister as a ‘permitted person’ by Ministerial Order.

The Bank wishes to clarify that ‘permitted persons’ may carry out cash transactions in excess of the cash transaction limit threshold. While therefore a permitted person will need to ensure that in transacting business with the public or its customers, it does not facilitate a breach of the law, banks and other licensed deposit taking institutions should not refuse to carry out cash transactions solely on the basis of a cash transaction exceeding the threshold limit.



THE
JAMAICA GAZETTE
SUPPLEMENT

PROCLAMATIONS, RULES AND REGULATIONS

740A

Vol. CXXXVI

FRIDAY, NOVEMBER 29, 2013

No. 132A

No. 259A

PUBLIC BUSINESS

Extract from the Minutes of the Honourable House of Representatives on the 19th day of November, 2013:

The Minister of National Security, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(ATTORNEYS-AT-LAW) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as “the Act”) the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution of this Honourable House:

NOW THEREFORE, BE IT RESOLVED by this Honourable House as follows:

- (i)

This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order Resolution, 2013.
- (ii)

The Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order, 2013, which was laid on the Table of the House on the 19th day of November, 2013, is hereby affirmed.

(Mr. Jolyan Silvera, MP, St. Mary, Western, entered and took his seat).

(Mr. William J. C. Hutchinson, CD, MP, St. Elizabeth, North Western, entered and took his seat).

Seconded by: Mr. Mikael Phillips.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259B

PUBLIC BUSINESS

Extract from the Minutes of the Honourable Senate on the 29th day of November, 2013:

The Minister of Justice, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(ATTORNEYS-AT-LAW) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as “the Act”) the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution:

NOW THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:

- (i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order Resolution, 2013.
- (ii) The Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order, 2013, which was laid on the Table of the Senate on the 28th day of November, 2013, is hereby affirmed.

Seconded by: Senator Alexander Williams.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259C

THE PROCEEDS OF CRIME ACT

THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(ATTORNEYS-AT-LAW) ORDER, 2013

In exercise of the powers conferred upon the Minister by paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act, the following Order is hereby made:—

1. This Order may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order, 2013.
2. With effect from the 1st day of June, 2014, any person to whom paragraph 3 applies is hereby designated as a non-financial institution for the purposes of the Act.
3. This paragraph applies to any person whose name is entered on the Roll of attorneys-at-law pursuant to section 4 of the Legal Profession Act, and who carries out any of the following activities on behalf of any client—
 - (a) purchasing or selling real estate;
 - (b) managing money, securities or other assets;
 - (c) managing bank accounts or savings accounts of any kind, or securities accounts;
 - (d) organizing contributions for the creation, operation or management of companies;
 - (e) creating, operating or managing a legal person or legal arrangement (such as a trust or settlement); or
 - (f) purchasing or selling a business entity.
4. For the purposes of paragraph 3, “securities” has the meaning assigned to it under the Securities Act.

Dated this 15th day of November, 2013.

PETER BUNTING
Minister of National Security.

No. 259D

PUBLIC BUSINESS

Extract from the Minutes of the Honourable House of Representatives on the 19th day of November, 2013:

The Minister of National Security, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(REAL ESTATE DEALERS) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as “the Act”) the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Real Estate Dealers) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution of this Honourable House:

NOW THEREFORE, BE IT RESOLVED by this Honourable House as follows:

- (i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Real Estate Dealers) Order Resolution, 2013.
- (ii) The Proceeds of Crime (Designated Non-Financial Institution) (Real Estate Dealers) Order, 2013, which was laid on the Table of the House on the 19th day of November, 2013, is hereby affirmed.

Seconded by: Dr. Dayton Campbell.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259E

PUBLIC BUSINESS

Extract from the Minutes of the Honourable Senate on the 29th day of November, 2013:

The Minister of Justice, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(REAL ESTATE DEALERS) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as “the Act”) the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Real Estate Dealers) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution:

NOW THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:

- (i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Real Estate Dealers) Order Resolution, 2013.
- (ii) The Proceeds of Crime (Designated Non-Financial Institution) (Real Estate Dealers) Order, 2013, which was laid on the Table of the Senate on the 28th day of November, 2013, is hereby affirmed.

Seconded by: Senator Alexander Williams.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259F

THE PROCEEDS OF CRIME ACT

**THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(REAL ESTATE DEALERS) ORDER, 2013**

In exercise of the powers conferred upon the Minister by paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act, the following Order is hereby made:—

1. This Order may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Real Estate Dealers) Order, 2013.
2. With effect from the 1st day of April, 2014, any person to whom paragraph 3 applies is hereby designated as a non-financial institution for the purposes of the Act.
3. This paragraph applies to any person who is issued a licence under the Real Estate (Dealers and Developers) Act authorizing that person to engage in the practice of real estate business in the capacity of a real estate dealer.

Dated this 15th day of November, 2013.

PETER BUNTING
Minister of National Security.

No. 259G

PUBLIC BUSINESS

Extract from the Minutes of the Honourable House of Representatives on the 19th day of November, 2013:

The Minister of National Security, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

**THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(GAMING MACHINE OPERATORS) ORDER RESOLUTION, 2013**

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as “the Act”) the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution of this Honourable House:

NOW THEREFORE, BE IT RESOLVED by this Honourable House as follows:

- (i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order Resolution, 2013.
- (ii) The Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order, 2013, which was laid on the Table of the House on the 19th day of November, 2013, is hereby affirmed.

(Miss Olivia Grange, MP, St. Catherine, Central, entered and took her seat).

(Mr. Andrew Holness, MP, St. Andrew, West Central and Leader of the Opposition, entered and took his seat).

Seconded by: Mr. Richard Parchment.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259H

PUBLIC BUSINESS

Extract from the Minutes of the Honourable Senate on the 29th day of November, 2013:

The Minister of Justice, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(GAMING MACHINE OPERATORS) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as “the Act”) the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution:

NOW THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:

- (i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order Resolution, 2013.
- (ii) The Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order, 2013, which was laid on the Table of the Senate on the 28th day of November, 2013, is hereby affirmed.

Seconded by: Senator Alexander Williams.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259I

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(GAMING MACHINE OPERATORS) ORDER, 2013

In exercise of the powers conferred upon the Minister by paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act, the following Order is hereby made:—

1. This Order may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order, 2013.
2. With effect from the 1st day of April, 2014, any person to whom paragraph 3 applies is hereby designated as a non-financial institution for the purposes of the Act.
3. This paragraph applies to any person who is issued a licence under the Real Estate (Dealers and Developers) Act authorizing that person to engage in the practice of real estate business in the capacity of a real estate dealer.

Dated this 15th day of November, 2013.

PETER BUNTING
Minister of National Security.

No. 259J

PUBLIC BUSINESS

Extract from the Minutes of the Honourable House of Representatives on the 19th day of November, 2013:

The Minister of National Security, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(CASINO OPERATORS) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as “the Act”) the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution of this Honourable House:

NOW THEREFORE, BE IT RESOLVED by this Honourable House as follows:

- (i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order Resolution, 2013.
- (ii) The Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013, which was laid on the Table of the House on the 19th day of November, 2013. This paragraph applies to any person who is issued a licence under the Real Estate (Dealers and Developers) Act authorizing that person to engage in the practice of real estate business in the capacity of a real estate dealer.

Dated this 15th day of November, 2013.

PETER BUNTING
Minister of National Security.

No. 259K

PUBLIC BUSINESS

Extract from the Minutes of the Honourable Senate on the 29th day of November, 2013:

The Minister of Justice, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(CASINO OPERATORS) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as “the Act”) the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution:

NOW THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:

- (i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order Resolution, 2013.
- (ii) The Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013, which was laid on the Table of the Senate on the 28th day of November, 2013, is hereby affirmed.

Seconded by: Senator Alexander Williams.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259L

THE PROCEEDS OF CRIME ACT

**THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(CASINO OPERATORS) ORDER, 2013**

In exercise of the powers conferred upon the Minister by paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act, the following Order is hereby made:—

1. This Order may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013.
2. With effect from the 1st day of April, 2014, any person to whom paragraph 3 applies is hereby designated as a non-financial institution for the purposes of the Act.
3. This paragraph applies to any person who operates a casino pursuant to a licence issued under the Casino Gaming Act.
4. For the purposes of paragraph 3, “casino” has the meaning assigned to it under the Casino Gaming Act.

Dated this 15th day of November, 2013.

PETER BUNTING
Minister of National Security.

No. 259M

PUBLIC BUSINESS

Extract from the Minutes of the Honourable House of Representatives on the 19th day of November, 2013:

The Minister of National Security, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

**THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(PUBLIC ACCOUNTANTS) ORDER RESOLUTION, 2013**

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as “the Act”) the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution of this Honourable House:

NOW THEREFORE, BE IT RESOLVED by this Honourable House as follows:

- (i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order Resolution, 2013.
- (ii) The Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order, 2013, which was laid on the Table of the House on the 19th day of November, 2013, is hereby affirmed.

(The Minister of State in the Office of the Prime Minister, the Honourable Luther Buchanan, entered and took his seat).

(Dr. Winston Green, MP, St. Mary, South Eastern, entered and took his seat).

Seconded by: Mr. Joylyan Silvera.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259N

PUBLIC BUSINESS

Extract from the Minutes of the Honourable Senate on the 29th day of November, 2013:

The Minister of Justice, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(PUBLIC ACCOUNTANTS) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as “the Act”) the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution:

NOW THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:

- (i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order Resolution, 2013.
- (ii) The Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order, 2013, which was laid on the Table of the Senate on the 28th day of November, 2013, is hereby affirmed.

Seconded by: Senator Alexander Williams.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259O

THE PROCEEDS OF CRIME ACT

THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(PUBLIC ACCOUNTANTS) ORDER, 2013

In exercise of the powers conferred upon the Minister by paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act, the following Order is hereby made:—

- 1. This Order may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order, 2013.
- 2. With effect from the 1st day of April, 2014, any person to whom paragraph 3 applies is hereby designated as a non-financial institution for the purposes of the Act.
- 3. This paragraph applies to any person registered as a public accountant under the Public Accountancy Act, and who carries out any of the following activities on behalf of any client—
 - (a) purchasing or selling real estate;
 - (b) managing money, securities or other assets;
 - (c) managing bank accounts or savings accounts of any kind, or securities accounts;
 - (d) organizing contributions for the creation, operation or management of companies;
 - (e) creating, operating or managing a legal person or legal arrangement (such as a trust or settlement); or
 - (f) purchasing or selling a business entity.
- 4. For the purposes of paragraph 3, “securities” has the meaning assigned to it under the Securities Act.

Dated this 15th day of November, 2013.

PETER BUNTING
Minister of National Security.



THE
JAMAICA GAZETTE
SUPPLEMENT

PROCLAMATIONS, RULES AND REGULATIONS

162A

Vol. CXLVFRIDAY, JANUARY 28, 2022No. 7A

No. 9A
Extract from the Minutes of the meeting of the Honourable House of Representatives, held on Tuesday, January 11, 2022:
PUBLIC BUSINESS

Dr. the Honourable Horace Chang, CD, MP, Deputy Prime Minister and Minister of National Security, having obtained suspension of Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(TRUST AND CORPORATE SERVICES PROVIDERS) RESOLUTION, 2022

WHEREAS paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as “the Act”), provides that a “designated non-financial institution” means a person who is—

- (a) not primarily engaged in carrying on financial business; and
- (b) designated as a non-financial institution for the purposes of the Act by the Minister by order subject to affirmative resolution;

AND WHEREAS on the 10th day of January, 2022, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Trust and Corporate Services Providers) Order, 2022;

AND WHEREAS it is desirable that the Proceeds of Crime (Designated Non-Financial Institution) (Trust and Corporate Services Providers) Order, 2022, be affirmed:

NOW, THEREFORE, BE IT RESOLVED by this Honourable House as follows:—

1. This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Trust and Corporate Services Providers) Order, 2022, Resolution.
2. The Proceeds of Crime (Designated Non-Financial Institution) (Trust and Corporate Services Providers) Order, 2022, which was laid on the Table of the House on the 11th day of January, 2022, is hereby affirmed.

Mr. Mark Golding also spoke on the motion.

Seconded by: Miss Tamika Davis

Agreed to.

I certify that the above is a true extract from the Minutes.

VALRIE A. CURTIS, CD, BH(M), JP
Clerk to the Houses.

No. 9B

Extract from the Minutes of the meeting of the Honourable Senate held on Friday, January 21, 2022:

PUBLIC BUSINESS

The Hon. Matthew Samuda, Minister without Portfolio in the Ministry of Economic Growth and Job Creation, moved:

THE PROCEEDS OF CRIME ACT

THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(TRUST AND CORPORATE SERVICES PROVIDERS) RESOLUTION, 2022

WHEREAS paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as “the Act”), provides that a “designated non-financial institution” means a person who is—

- (a) not primarily engaged in carrying on financial business; and
- (b) designated as a non-financial institution for the purposes of the Act by the Minister by order subject to affirmative resolution;

AND WHEREAS on the 10th day of January, 2022, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Trust and Corporate Services Providers) Order, 2022;

AND WHEREAS it is desirable that the Proceeds of Crime (Designated Non-Financial Institution) (Trust and Corporate Services Providers) Order, 2022, be affirmed:

NOW, THEREFORE, BE IT RESOLVED by this Honourable House as follows:—

1. This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Trust and Corporate Services Providers) Order, 2022, Resolution.
2. The Proceeds of Crime (Designated Non-Financial Institution) (Trust and Corporate Services Providers) Order, 2022, which was laid on the Table of the Senate on the 14th day of January, 2022, is hereby affirmed.

Senator Donna Scott Mottley and Senator Natalie Campbell-Rodriques also spoke on the motion.

Seconded by: Senator Kavan Gayle

Agreed to.

I certify that the above is a true extract from the Minutes.

VALRIE A. CURTIS, CD, BH(M), JP
Clerk to the Houses.

THE PROCEEDS OF CRIME ACT

THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(TRUST AND CORPORATE SERVICES PROVIDERS) RESOLUTION, 2022

WHEREAS paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as “the Act”), provides that a “designated non-financial institution” means a person who is—

- (a) not primarily engaged in carrying on financial business; and
- (b) designated as a non-financial institution for the purposes of the Act by the Minister by order subject to affirmative resolution.

AND WHEREAS on the 10th day of January, 2022, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Trust and Corporate Services Providers) Order, 2022:

AND WHEREAS it is desirable that the Proceeds of Crime (Designated Non-Financial Institution) (Trust and Corporate Services Providers) Order, 2022, be affirmed:

NOW, THEREFORE, BE IT RESOLVED by this Honourable House as follows:—

1. This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Trust and Corporate Services Providers), Resolution, 2022.

2. The Proceeds of Crime (Designated Non-Financial Institution) (Trust and Corporate Services Providers) Order, 2022, is affirmed.

THE PROCEEDS OF CRIME ACT

**THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(TRUST AND CORPORATE SERVICES PROVIDERS) ORDER, 2022**

In exercise of the power conferred on the Minister by paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as “the Act”), the following Order is hereby made:—

1. This Order may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Trust and Corporate Services Providers) Order, 2022.
2. Any person to whom paragraph 3 applies is hereby designated as a non-financial institution for the purposes of the Act.
3. This paragraph applies to any person who provides—
 - (a) a trust service; or
 - (b) a corporate service.
4. For the purposes of paragraph 3, “trust service” and “corporate service” have the meanings assigned to them under the Trust and Corporate Services Providers Act.

Dated this 10th day of January, 2022.

HORACE A. CHANG
Minister of National Security.



THE
JAMAICA GAZETTE
SUPPLEMENT

PROCLAMATIONS, RULES AND REGULATIONS

407

Vol. CXLV

FRIDAY, MARCH 25, 2022

No. 29

No. 49

Extract from the Minutes of the meeting of the House of Representatives held on Tuesday, February 1, 2022:

PUBLIC BUSINESS

Dr. the Honourable Horace Chang, CD, MP, Deputy Prime Minister and Minister of National Security, having obtained suspension of the Standing Orders, moved:

THE TERRORISM PREVENTION ACT

THE TERRORISM PREVENTION (DESIGNATED REPORTING ENTITY)
(TRUST AND CORPORATE SERVICES PROVIDERS) ORDER, 2022, RESOLUTION

WHEREAS section 15 of the Terrorism Prevention Act (hereinafter referred to as “the Act”), imposes reporting duties on certain specified entities;

AND WHEREAS section 15(2)(c) of the Act provides that the Minister may designate any entity as an entity to which the provisions of section 15 of the Act shall apply;

AND WHEREAS section 15(1)(c) of the Act provides for the aforementioned designation to be made by order subject to affirmative resolution;

AND WHEREAS on the 21st day of January, 2022, the Minister made the Terrorism Prevention (Designated Reporting Entity) (Trust and Corporate Services Providers) Order, 2022;

AND WHEREAS it is desirable that the Terrorism Prevention (Designated Reporting Entity) (Trust and Corporate Services Providers) Order, 2022, be affirmed:

NOW, THEREFORE, BE IT RESOLVED by this Honourable House as follows:—

1. This Resolution may be cited as the Terrorism Prevention (Designated Reporting Entity) (Trust and Corporate Services Providers) Order, 2022, Resolution.
2. The Terrorism Prevention (Designated Reporting Entity) (Trust and Corporate Services Providers) Order, 2022, which was laid on the Table of the House on the 1st day of February, 2022, is hereby affirmed.

Mr. Mark Golding and the Hon. Marlene Malahoo Forte, QC, MP, Minister of Legal and Constitutional Affairs also spoke on the motion.

Seconded by: Mr. Phillip Henriques

Agreed to

I certify that the above is a true extract from the Minutes.

VALRIE A. CURTIS, CD, BH(M), JP
Clerk to the Houses.

No. 50

Extract from the Minutes of the Honourable Senate held on the 28th day of January, 2022:

PUBLIC BUSINESS

Senator the Hon. Kamina Johnson Smith, Minister of Foreign Affairs and Foreign Trade and Leader of Government Business, moved:

THE TERRORISM PREVENTION ACT

THE TERRORISM PREVENTION (DESIGNATED REPORTING ENTITY)
(TRUST AND CORPORATE SERVICES PROVIDERS) ORDER, 2022, RESOLUTION

WHEREAS section 15 of the Terrorism Prevention Act (hereinafter referred to as “the Act”), imposes reporting duties on certain specified entities;

AND WHEREAS section 15(2)(c) of the Act provides that the Minister may designate any entity as an entity to which the provisions of section 15 of the Act shall apply;

AND WHEREAS section 15(1)(c) of the Act provides for the aforementioned designation to be made by order subject to affirmative resolution;

AND WHEREAS on the 21st day of January, 2022, the Minister made the Terrorism Prevention (Designated Reporting Entity) (Trust and Corporate Services Providers) Order, 2022;

AND WHEREAS it is desirable that the Terrorism Prevention (Designated Reporting Entity) (Trust and Corporate Services Providers) Order, 2022, be affirmed:

NOW, THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:—

1. This Resolution may be cited as the Terrorism Prevention (Designated Reporting Entity) (Trust and Corporate Services Providers) Order, 2022, Resolution.
2. The Terrorism Prevention (Designated Reporting Entity) (Trust and Corporate Services Providers) Order, 2022, which was laid on the Table of the Senate on the 21st day of January, 2022, is hereby affirmed.

Senator the Hon. Aubyn Hill, Minister without Portfolio in the Ministry of Economic Growth and Job Creation, also spoke on the motion.

Seconded by: Senator Natalie Campbell Rodriques

Agreed to

I certify that the above is a true extract from the Minutes.

VALRIE A. CURTIS, CD, BH(M), JP
Clerk to the Houses.

THE TERRORISM PREVENTION ACT

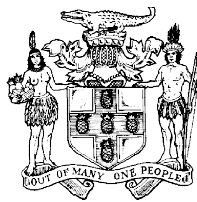
THE TERRORISM PREVENTION (DESIGNATED REPORTING ENTITY)
(TRUST AND CORPORATE SERVICES PROVIDERS) ORDER, 2022

In exercise of the power conferred on the Minister by section 15(2) of the Terrorism Prevention Act (hereinafter referred to as “the Act”), the following Order is hereby made:

1. This Order may be cited as the Terrorism Prevention (Designated Reporting Entity) (Trust and Corporate Services Providers) Order, 2022.
2. Any person to whom paragraph 3 applies is hereby designated as a reporting entity for the purposes of section 15(2) of the Act.
3. This paragraph applies to any person who provides—
 - (a) a trust service; or
 - (b) a corporate service.
4. For the purposes of paragraph 3, “trust service” and “corporate service” have the meanings assigned to them under the Trust and Corporate Services Providers Act.

Dated this 21st day of January, 2022.

KAMINA JOHNSON SMITH,
Minister of Foreign Affairs and Foreign Trade.



THE
JAMAICA GAZETTE
SUPPLEMENT

PROCLAMATIONS, RULES AND REGULATIONS

872A

Vol. CXL

WEDNESDAY, NOVEMBER 29, 2017

No. 84A

No. 184A

PUBLIC BUSINESS

Extract from the Minutes of the meeting of the Honourable Senate held on Friday the 13th day of October, 2017:

The Minister of Foreign Affairs and Foreign Trade and Leader of Government Business, having obtained suspension of the Standing Orders, further moved:

THE TERRORISM PREVENTION ACT

THE TERRORISM PREVENTION (DESIGNATED REPORTING ENTITY)
(GAMING MACHINE OPERATORS) ORDER, RESOLUTION, 2017

WHEREAS section 15 of the Terrorism Prevention Act (hereinafter referred to as “the Act”) imposes reporting duties on certain specified entities:

AND WHEREAS section 15(2) of the Act provides that the Minister may designate any entity as an entity to which the provisions of section 15 of the Act shall apply:

AND WHEREAS section 15(2) of the Act provides for the aforementioned designation to be made by order subject to affirmative resolution:

AND WHEREAS on the 12th day of October, 2017, the Minister made the Terrorism Prevention (Designated Reporting Entity) (Gaming Machine Operators) Order, 2017:

NOW, THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:—

1. This Resolution may be cited as the Terrorism Prevention (Designated Reporting Entity) (Gaming Machine Operators) Order, Resolution, 2017.

2. The Terrorism Prevention (Designated Reporting Entity)(Gaming Machine Operators) Order, 2017, which was laid on the Table of the Senate on the 13th day of October, 2017, is hereby affirmed.

Senator Lambert Brown also spoke on the motion.

Seconded by: Senator Matthew Samuda.

Agreed to.

I certify that the above is a true extract from the Minutes.

HEATHER E. COOKE, CD, JP, (MRS.)
Clerk to the Houses.

No. 184B

PUBLIC BUSINESS

Extract from the Minutes of the meeting of the Honourable House of Representatives held on the 29th day of November, 2017:

The Minister of Justice, having obtained suspension of the Standing Orders, moved:

THE TERRORISM PREVENTION ACT

THE TERRORISM PREVENTION (DESIGNATED REPORTING ENTITY)
(GAMING MACHINE OPERATORS) ORDER, RESOLUTION, 2017

WHEREAS section 15 of the Terrorism Prevention Act (hereinafter referred to as “the Act”) imposes reporting duties on certain specified entities:

AND WHEREAS section 15(2) of the Act provides that the Minister may designate any entity as an entity to which the provisions of section 15 of the Act shall apply:

AND WHEREAS section 15(2) of the Act provides for the aforementioned designation to be made by order subject to affirmative resolution:

AND WHEREAS on the 12th day of October, 2017, the Minister made the Terrorism Prevention (Designated Reporting Entity) (Gaming Machine Operators) Order, 2017:

NOW, THEREFORE, BE IT RESOLVED by this Honourable House as follows:—

1. This Resolution may be cited as the Terrorism Prevention (Designated Reporting Entity) (Gaming Machine Operators) Order, Resolution, 2017.

2. The Terrorism Prevention (Designated Reporting Entity)(Gaming Machine Operators) Order, 2017, which was laid on the Table of the House on the 29th day of November, 2017, is hereby affirmed.

Senator Mark Golding also spoke on the motion.

Seconded by: Mr. Alando Terrelonge.

Agreed to.

I certify that the above is a true extract from the Minutes.

HEATHER E. COOKE, CD, JP, (MRS.)
Clerk to the Houses.

THE TERRORISM PREVENTION ACT

THE TERRORISM PREVENTION (DESIGNATED REPORTING ENTITY)
(GAMING MACHINE OPERATORS) ORDER, 2017

In exercise of the powers conferred upon the Minister by section 15(2) of the Terrorism Prevention Act, and every of other power hereunto enabling, the following Order is hereby made:—

1. This Order may be cited as the Terrorism Prevention (Designated Reporting Entity) (Gaming Machine Operators) Order, 2017.

2. With effect from the specified date, any person to whom paragraph 3 applies is hereby designated as a reporting entity for the purposes of section 15 of the Act.

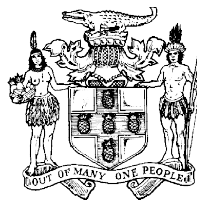
3. This paragraph applies to any person who operates twenty or more gaming machines pursuant to a licence under the Betting, Gaming and Lotteries Act.

4. For the purposes of—

- (a) paragraph 2, the specified date is the day falling six months after the date on which this Order comes into operation;
- (b) paragraph 3, “gaming machine” has the meaning assigned to it by section 43 of the Betting, Gaming and Lotteries Act.

Dated this 12th day of October, 2017.

KAMINA JOHNSON SMITH
Minister of Foreign Affairs and Foreign Trade.



THE
JAMAICA GAZETTE
SUPPLEMENT

PROCLAMATIONS, RULES AND REGULATIONS

876c

Vol. CXL

WEDNESDAY, DECEMBER 6, 2017

No. 85B

No. 185B

PUBLIC BUSINESS

Extract from the Minutes of the meeting of the Honourable Senate held on Friday the 6th day of October, 2017:

The Minister of Foreign Affairs and Foreign Trade and Leader of Government Business moved:

THE TERRORISM PREVENTION ACT

THE TERRORISM PREVENTION (DESIGNATED REPORTING ENTITY)
(CASINO OPERATORS) ORDER, RESOLUTION, 2017

WHEREAS section 15 of the Terrorism Prevention Act (hereinafter referred to as “the Act”) imposes reporting duties on certain specified entities:

AND WHEREAS section 15(2) of the Act provides for the aforementioned designation to be made by order subject to affirmative resolution:

AND WHEREAS section 15(2) of the Act provides that the Minister may designate any entity as an entity to which the provisions of section 15 of the Act shall apply:

AND WHEREAS on the 9th day of June, 2017, the Minister made the Terrorism Prevention (Designated Reporting Entity) (Casino Operators) Order, 2017:

NOW, THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:—

1. This Resolution may be cited as the Terrorism Prevention (Designated Reporting Entity) (Casino Operators) Order, Resolution, 2017.
2. The Terrorism Prevention (Designated Reporting Entity)(Casino Operators) Order, 2017, which was laid on the Table of the Senate on the 16th day of June, 2017, is hereby affirmed.

Senator Mark Golding, Senator Lambert Brown, Senator Ransford Braham and Senator Keith Knight also spoke on the motion.

Seconded by: Senator Dr. Sapphire Longmore.

Agreed to.

I certify that the above is a true extract from the Minutes.

HEATHER E. COOKE, CD, JP, (MRS.)
Clerk to the Houses.

No. 185B

PUBLIC BUSINESS

Extract from the Minutes of the meeting of the Honourable House of Representatives held on the 29th day of November, 2017:

The Minister of Justice moved:

THE TERRORISM PREVENTION ACT

THE TERRORISM PREVENTION (DESIGNATED REPORTING ENTITY)
(CASINO OPERATORS) ORDER, RESOLUTION, 2017

WHEREAS section 15 of the Terrorism Prevention Act (hereinafter referred to as “the Act”) imposes reporting duties on certain specified entities:

AND WHEREAS section 15(2) of the Act provides that the Minister may designate any entity as an entity to which the provisions of section 15 of the Act shall apply:

AND WHEREAS section 15(2) of the Act provides for the aforementioned designation to be made by order subject to affirmative resolution:

AND WHEREAS on the 9th day of June, 2017, the Minister made the Terrorism Prevention (Designated Reporting Entity) (Casino Operators) Order, 2017:

NOW, THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:—

1. This Resolution may be cited as the Terrorism Prevention (Designated Reporting Entity) (Casino Operators) Order, Resolution, 2017.

2. The Terrorism Prevention (Designated Reporting Entity)(Casino Operators) Order, 2017, which was laid on the Table of the House on the 13th day of June, 2017, is hereby affirmed.

Senator Mark Golding also spoke on the motion.

Seconded by: Mr. Alando Terrelonge.

Agreed to.

I certify that the above is a true extract from the Minutes.

HEATHER E. COOKE, CD, JP, (MRS.)
Clerk to the Houses.

THE TERRORISM PREVENTION ACT

THE TERRORISM PREVENTION (DESIGNATED REPORTING ENTITY)
(CASINO OPERATORS) ORDER, 2017

In exercise of the powers conferred upon the Minister by section 15(2) of the Terrorism Prevention Act, and every of other power hereunto enabling, the following Order is hereby made:—

1. This Order may be cited as the Terrorism Prevention (Designated Reporting Entity) (Casino Operators) Order, 2017.

2. With effect from the commencement date of this Order, any person to whom paragraph 3 applies is hereby designated as reporting entity for the purposes of section 15 of the Act.

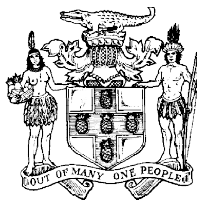
3. This paragraph applies to any person who operates a casino pursuant to a licence issued under the Casino Gaming Act.

4. For the purposes of—

- (a) paragraph 2, the commencement date is the day falling six months after the date on which this Order is affirmed by resolution pursuant to section 15(2) of the Act;
- (b) paragraph 3, “casino” has the meaning assigned to it under the Casino Gaming Act.

Dated this 9th day of June, 2017.

KAMINA JOHNSON SMITH
Minister of Foreign Affairs and Foreign Trade.



THE
JAMAICA GAZETTE
SUPPLEMENT

PROCLAMATIONS, RULES AND REGULATIONS

872G

Vol. CXL

WEDNESDAY, NOVEMBER 29, 2017

No. 84C

No. 184E

PUBLIC BUSINESS

Extract from the Minutes of the meeting of the Honourable Senate held on the 13th day of October, 2017:

The Minister of Foreign Affairs and Foreign Trade and Leader of Government Business, having obtained suspension of the Standing Orders, further moved:

THE TERRORISM PREVENTION ACT

THE TERRORISM PREVENTION (DESIGNATED REPORTING ENTITY)
(PUBLIC ACCOUNTANTS) ORDER, RESOLUTION, 2017

WHEREAS section 15 of the Terrorism Prevention Act (hereinafter referred to as “the Act”) imposes reporting duties on certain specified entities:

AND WHEREAS section 15(2) of the Act provides that the Minister may designate any entity as an entity to which the provisions of section 15 of the Act shall apply:

AND WHEREAS section 15(2) of the Act provides for the aforementioned designation to be made by order subject to affirmative resolution:

AND WHEREAS on the 9th day of June, 2017, the Minister made the Terrorism Prevention (Designated Reporting Entity) (Public Accountants) Order, 2017:

NOW, THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:—

1. This Resolution may be cited as the Terrorism Prevention (Designated Reporting Entity) (Public Accountants) Order, Resolution, 2017.
2. The Terrorism Prevention (Designated Reporting Entity)(Public Accountants) Order, 2017, which was laid on the Table of the House on the 13th day of June, 2017, is hereby affirmed.

Senator Mark Golding also spoke on the motion.

Seconded by: Mr. Alando Terrelonge.

Agreed to.

I certify that the above is a true extract from the Minutes.

HEATHER E. COOKE, CD, JP, (MRS.)
Clerk to the Houses.

THE TERRORISM PREVENTION ACT

**THE TERRORISM PREVENTION (DESIGNATED REPORTING ENTITY)
(PUBLIC ACCOUNTANTS) ORDER, 2017**

In exercise of the powers conferred upon the Minister by section 15(2) of the Terrorism Prevention Act, and every of other power hereunto enabling, the following Order is hereby made:—

1. This Order may be cited as the Terrorism Prevention (Designated Reporting Entity) (Designated Reporting Entity) (Public Accountants) Order, 2017.
2. With effect from the commencement date of this Order, any person to whom paragraph 3 applies is hereby designated as a reporting entity for the purposes of section 15 of the Act.
3. This paragraph applies to any person registered as a public accountant under the Public Accountancy Act, and who carries out any of the following activities on behalf of any client—
 - (a) purchasing or selling real estate;
 - (b) managing money, securities or other assets;
 - (c) managing bank accounts or saving accounts of any kind, or securities accounts;
 - (d) organizing contributions for the creation, operation or management of companies;
 - (e) creating, operating or managing a legal person or legal arrangement (such as a trust or settlement); or
 - (f) purchasing or selling a business entity.

AND WHEREAS on the 9th day of June, 2017, the Minister made the Terrorism Prevention (Designated Reporting Entity) (Public Accountants) Order, 2017:

NOW, THEREFORE, BE IT RESOLVED by this Honourable House as follows:—

1. This Resolution may be cited as the Terrorism Prevention (Designated Reporting Entity) (Public Accountants) Order, Resolution, 2017.
2. The Terrorism Prevention (Designated Reporting Entity)(Public Accountants) Order, 2017, which was laid on the Table of the Senate on the 16th day of June, 2017, is hereby affirmed.

Seconded by: Senator Matthew Samuda.

Agreed to.

I certify that the above is a true extract from the Minutes.

HEATHER E. COOKE, CD, JP, (MRS.)
Clerk to the Houses.

No. 184F

PUBLIC BUSINESS

Extract from the Minutes of the Honourable House of Representatives on the 29th day of November, 2017:

The Minister of Justice, moved:

THE PROCEEDS OF CRIME ACT

**THE PROCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION)
(PUBLIC ACCOUNTANTS) ORDER RESOLUTION, 2017**

WHEREAS section 15 of the Terrorism Prevention Act (hereinafter referred to as “the Act”) imposes reporting duties on certain specified entities:

AND WHEREAS section 15(2) of the Act provides that the Minister may designate any entity as an entity to which the provisions of section 15 of the Act shall apply:

AND WHEREAS section 15(2) of the Act provides for the aforementioned designation to be made by order subject to affirmative resolution:

AND WHEREAS on the 9th day of June, 2017, the Minister made the Terrorism Prevention (Designated Reporting Entity) (Public Accountants) Order, 2017:

NOW, THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:—

1. This Resolution may be cited as the Terrorism Prevention (Designated Reporting Entity) (Public Accountants) Order, Resolution, 2017.

2. The Terrorism Prevention (Designated Reporting Entity)(Public Accountants) Order, 2017, which was laid on the Table of the Senate on the 13th day of June, 2017, is hereby affirmed.

Mr. Mark Golding also spoke on the motion.

Seconded by: Mr. Alando Terrelonge.

Agreed to.

I certify that the above is a true extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

THE TERRORISM PREVENTION ACT

THE TERRORISM PREVENTION (DESIGNATED REPORTING ENTITY)
(PUBLIC ACCOUNTANTS) ORDER, 2017

In exercise of the powers conferred upon the Minister by section 15(2) of the Terrorism Prevention Act, and of every other power hereunto enabling, the following Order is hereby made:—

- 1. This Order may be cited as the Terrorism Prevention (Designated Reporting Entity) (Attorneys-at-law) Order, 2019.
- 2. With effect from the commencement date of this Order, any person to whom paragraph 3 applies is hereby designated as a reporting entity for the purposes of section 15 of the Act.
- 3. This paragraph applies to any person registered as a public accountant under the Public Accountancy Act, and who carries out any of the following activities on behalf of any client—
 - (a) purchasing or selling real estate;
 - (b) managing money, securities or other assets;
 - (c) managing bank accounts or savings accounts of any kind, or securities accounts;
 - (d) organizing contributions for the creation, operation or management of companies;
 - (e) creating, operating or managing a legal person or legal arrangement (such as a trust or settlement); or
 - (f) purchasing or selling a business entity.
- 4. For the purposes of—
 - (a) paragraph 2, the commencement date is the day falling six months after the date on which this Order is affirmed by resolution pursuant to section 15(2)of the Act;
 - (b) paragraph 3, “securities” has the meaning assigned to it under the Securities Act.

Dated this 9th day of June, 2017.

KAMINA JOHNSON SMITH,
Minister of Foriegn Affairs and Foreign Trade.

THE TERRORISM PREVENTION ACT

THE TERRORISM PREVENTION (DESIGNATED REPORTING ENTITY)
(ATTORNEYS-AT-LAW) ORDER, 2019

In exercise of the powers conferred upon the Minister by section 15(2) of the Terrorism Prevention Act, and of every other power hereunto enabling, the following Order is hereby made:—

- 1. This Order may be cited as the Terrorism Prevention (Designated Reporting Entity) (Attorneys-at-law) Order, 2019.
- 2. With effect from the commencement date of this Order, any person to whom paragraph 3 applies is hereby designated as a reporting entity for the purposes of section 15 of the Act.
- 3. This paragraph applies to any person whose name is entered on the Roll of Attorneys-at-law pursuant to section 4 of the Legal Profession Act, and who carries out any of the following activities on behalf of any client—
 - (a) purchasing or selling real estate;
 - (b) managing money, securities or other assets;
 - (c) managing bank accounts or savings accounts of any kind, or securities accounts;

- (d) organizing contributions for the creation, operation or management of companies;
 - (e) creating, operating or managing a legal person or legal arrangement (such as a trust or settlement); or
 - (f) purchasing or selling a business entity.
4. For the purposes of—
- (a) paragraph 2, the commencement date is the day falling six months after the date on which this Order is affirmed by resolution pursuant to section 15(2) of the Act;
 - (b) paragraph 3, “securities” has the meaning assigned to it under the Securities Act.

Dated this 6th day of February, 2019.

KAMINA JOHNSON SMITH,
Minister of Foreign Affairs and Foreign Trade.

*Appendix IV- Basic Duties and Responsibilities of the Nominated
Officer
(Section VI)*

The “Nominated Officer” should be responsible for the day-to-day monitoring of the financial institution’s compliance with AML/CFT/CPF laws, regulations and industry best practices. That Officer should be an employee of the business³⁷⁷ and should possess the requisite skills, qualification and expertise to effectively perform the assigned tasks; and most importantly, he/she should have access to all operational areas and have the requisite seniority and authority to report independently to the board. This duty must be independent of the internal audit function.

The duties and functions of the Nominated Officer should at a minimum include, inter alia, the following:

1. Act as liaison between the financial institution and the Bank of Jamaica and law enforcement agencies (FID, DPP, etc) with respect to compliance matters and investigations;
2. Ensure AML/CFT/CPF risk assessments are executed by the financial institution and reported to the Board within 90 days of its completion; and require the Board and senior management, proportionate and commensurate to its risk profile, design and implement appropriate measures and counter-measures, to treat with its AML/CFT/CPF risk exposures (threats and vulnerabilities). Once the required programme adjustments and improvements are carried out, the nominated officer must ensure a re-assessment of risks are carried out, and kept up to date and relevant.
3. Independently evaluate the risk assessment produced by management on new products and services to determine the level of ML/TF/PF risk(s) posed by such products and services to the financial institution and give an opinion on whether these are within the risk appetite and meet internal and regulatory compliance standards;
4. Evaluate reports of suspicious/unusual transactions and activities by personnel and ensuring the timely filing of Suspicious Transaction Reports/Suspicious Activity Reports;
5. Handle all communication with the designated authority on matters relating to consent, and advise the business on the process and steps to take thus ensuring there is no breach of POCA or the POC(MLP) Regulations as it relates to tipping off the customer.
6. Coordinate with the financial institution’s audit, legal, fraud and security departments on AML/CFT /CPF matters and investigations; and on matters pertaining to targeted financial sanctions notified by the United Nations Security Council;
7. Prepare report to the Senior Management, and the Board of Directors at least on an annual basis on the effectiveness of the AML/CFT/CPF framework. Where applicable this report should also speak to compliance levels with directives pertaining to targeted financial sanctions notified by the United Nations Security Council (This report should be subject to review by the Bank of Jamaica);
8. Advise business units of proposed or pending regulatory changes, and where adjustments to meet these new changes are required, ensure the business carries out these changes;
9. Prepare and update policies and procedures and disseminate information to the financial institution’s Board, Management, staff, and other relevant personnel and parties who may be directly or indirectly involved in the operations (and where applicable) the delivery of banking services of the financial institution³⁷⁸;
10. Oversee and ensure the implementation of its compliance plan as a key initiative of its broader compliance programme;
11. Oversee administrative matters related to Code of Conduct and Compliance with Anti-money Laundering and Terrorist Financing and Proliferation of Weapons of Mass Destruction Activities; and
12. Develop training material and coordinate anti-money laundering training/counter terrorist financing/proliferation financing training and training in relation to responding to directives to apply targeted financial sanctions notified by the United Nations Security Council.

³⁷⁷ Amendment to Regulation 5(3) of the POC (MLP) Regulations 2019
³⁷⁸ This grouping includes Consultants; Contractors (pursuant to outsourcing arrangements); Agents (pursuant to agent banking arrangements)

*Appendix V**Examples of Unusual/Suspicious Activities**(Paragraph 13)*

1. Provision of Insufficient or Suspicious Information.

2. Cash Transactions:

- (a) Cash deposits which are not consistent with the business activities of the customer.
- (b) Increases in cash deposits of the customer without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.
- (c) Unusually large cash deposits by a customer whose ostensible business activities would normally be generated by cheques and other instruments.
- (d) Cash deposits by a customer, by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.
- (e) Requests for the exchange of large quantities of low denomination notes for those of higher denomination.
- (f) The transfer by a customer of large sums of money to or from overseas locations with instructions for payment in cash.
- (g) Frequent exchange of cash into other currencies.
- (h) The constant pay-in or deposit of cash by a customer to cover requests for financial institutions' drafts, money transfers or other negotiable and readily marketable money instruments.
- (i) Large cash deposits using night depository facilities, thereby avoiding direct contact with financial institution staff.
- (j) Company accounts whose deposits and withdrawals are by cash rather than the forms of debit and credit normally associated with commercial operations (for example, cheques, Letters of Credit, Bills of Exchange, etc.) or in relation to which withdrawals are made therefrom and requests made for payment into personal accounts.
- (k) Frequent buying and selling of currency by any medium (cash, cheques, electronic purse or other telephonic or electronic medium etc.) in any manner that is indicative of foreign exchange trading and the transaction is not done by or on the behalf of a cambio/bureau de change or authorized dealer;

Note that this list is not exhaustive.

3. Operation of Accounts

- (a) The use of a number of trustees or clients' accounts which do not appear consistent with the customer's type of business, including transactions which involve nominee names.
- (b) Increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts especially if the deposits are promptly transferred between other client company and trust accounts.
- (c) Large number of individuals making payments into the same account without an adequate explanation.
- (d) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.
- (e) Matching of payments out with credits paid in by cash on the same or previous day.
- (f) Paying in large third-party cheques endorsed in favour of the customer.
- (g) High account turnover inconsistent with the size of the balance (suggesting that funds are being "washed" through the account).
- (h) Transactions constituting the co-mingling of company funds with an individual's account or constituting the conduct of company business through the account of an individual particularly where the individual is not named as a signatory to the corporate bank account.
- (i) See k in cash transactions above

4. Additional Considerations for Transactions Involving Terrorist Financing

- (a) Accounts that receive relevant periodic deposits and are dormant at other periods;
- (b) A dormant account with a minimal sum suddenly receiving a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed;
- (c) Customer refuses to provide information required by financial institution, or attempts to reduce the level of information provided or to provide information that is misleading or difficult to verify;

5. Investment Related Transaction

- (a) Purchasing of securities to be held by the financial institution in safe custody, where this does not appear appropriate given the customer's apparent standing.
- (b) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

- (c) Requests by customers for investment management services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customers’ apparent standing.

6. Off-Shore International Activity

- (a) Building up of large balances, not consistent with the known turnover of the customer’s business, and subsequent transfer to account(s) held overseas.
- (b) Use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer’s usual business.
- (c) Regular and large payments by customers, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receipt of regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs or money laundering, or which are regarded as tax havens.
- (d) Unexplained electronic fund transfers by customers on an In-and-Out basis and without passing through an account.

7. Secured and Unsecured Lending

- (a) Customers who repay problem loans unexpectedly.
- (b) Requests to borrow against assets held by the financial institution or a third Party, where the origin of the assets is not known or the assets are inconsistent with the customer’s standing.
- (c) Requests by customers for a financial institution to provide or arrange financing where the source of the customer’s financial contribution to the transaction is unclear, particularly where property is involved.
- (d) Requests for loans to offshore companies, or loans secured by obligations of offshore financial institutions.
- (e) Customers purchasing certificates of deposit and using them as loan collateral.

8. Overseas correspondents and other foreign counterparts seeking to conduct business from jurisdictions that are currently on FATF’s list of non-cooperative countries and territories (NCCT/blacklisted territories).

Overseas correspondents and other foreign counterparts with principals that are included on the U.N.’s list of terrorists and seeking to conduct business directly or indirectly through a separate corporate vehicle (e.g. special purpose vehicle (s.p.v.); or trustee; etc.)

9. Joint venture-type invitations from local or overseas companies or organizations with no discernible track record of legitimate operations; tax compliance; and in respect of which the true identities and sources of funding or wealth of the principal(s) are unknown.

10. Purposeless conversation requesting detailed disclosures of AML/CFT/CPF measures in respect of physical location measures and software and administrative measures.

11. Transactions which are started and then abandoned due to decision not to proceed or because an error was made in processing the transaction. (Such incidences should be carefully monitored and care should be taken to ensure completed and/or signed documentation in this regard are properly destroyed (i.e. shredded, or finely torn/cut up) in the presence of the signing parties.)

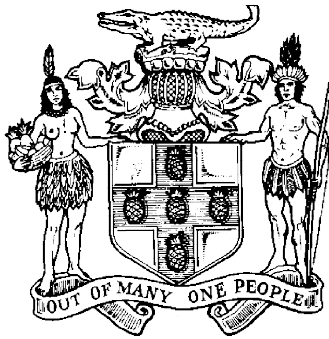
Appendix VI

Mandatory Obligations

- (a) Risk-based Framework - Section IV;
- (b) Know Your Customer Requirements- Section V;
- (c) Customer Due Diligence -Section V;
- (d) Special guidance - Listed Entities (Section V(B)& UNSEC Resolutions Section V(C);
- (e) Nominated Officer Regime - Section VI;
- (f) Compliance Monitoring - Section VII;
- (g) Board Responsibility and Employee Integrity and Awareness ~ Section VIII;
- (h) Transaction Monitoring and Reporting - Section IX;
- (i) Record Keeping- Section X; and
- (j) Special and Additional guidance - Listed Entities & UNSEC Resolutions.

Appendix VII

Bank of Jamaica’s Specified Territories Supervisory
Authority Notice
(Paragraphs 75A and 193)



THE
JAMAICA GAZETTE
EXTRAORDINARY

651

Vol. CXLVI

TUESDAY, MAY 2, 2023

No. 168

The following Notification is, by command of His Excellency the Governor-General, published for general information.

PATRICIA RODNEY EVERING, OD (MS.)
Governor-General’s Secretary and
Clerk to the Privy Council (Assigned).

GOVERNMENT NOTICE

MISCELLANEOUS

No. 184

THE BANK OF JAMAICA SPECIFIED TERRITORIES SUPERVISORY AUTHORITY NOTICE
The Proceeds of Crime (Amendment) Act (Section 94A)
and
The Proceeds of Crime (Money Laundering Prevention Amendment) Regulations, 2019
(Regulation 8)

1. This Notice may be cited as the Bank of Jamaica Specified Territories Supervisory Authority Notice, 2022 and is issued by Bank of Jamaica pursuant to section 94A of the Proceeds of Crime (Amendment) Act, 2019.
2. The Proceeds of Crime legislation requires regulated businesses, to—
 - (a) in relation to all business relationships and transactions with customers resident, domiciled or incorporated in a specified territory:
 - (i) apply enhanced customer due diligence procedures (section 94A(1) and (2) at section 5 of the Proceeds of Crime Amendment Act, 2019);

- (ii) ensure the background and purpose of such transactions is examined and the findings documented and made available to the designated authority the supervisory authority or to a competent authority under POCA; and to
 - (b) apply countermeasures in respect of any business relationship or transaction with any applicant for business resident or domiciled in a specified territory (regulation 7B at regulation 8 of the Proceeds of Crime (Money Laundering Prevention) (Amendment) Regulations, 2019).
3. *Enhanced Due Diligence and Countermeasures Procedures*
- (i) Enhanced due diligence procedures mean the measures outlined in regulation 7A(5) of the Proceeds of Crime (Money Laundering Prevention) Regulations.
 - (ii) Countermeasures mean the measures outlined in regulation 7B at regulation 8 of the Proceeds of Crime (Money Laundering Prevention) (Amendment) Regulations, 2019.
 - (iii) Financial Action Task Force is the independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction and the issuer of the international standards on combating money laundering and the financing of terrorism and proliferation (the FATF Recommendations)¹.
4. For the purpose of this Notice, the regulated businesses to which this notice refers are set out in the First Schedule to this Notice.
5. For the purpose of this Notice, a specified territory is a territory described in the Second Schedule to this Notice.

FIRST SCHEDULE (Paragraph 4)

The regulated businesses referred to in paragraph 1 of this Notice are the following financial institutions listed below at (a) - (f) as follows:—

- (a) Deposit taking institutions under *the Banking Services Act*;
- (b) Financial holding companies under *the Banking Services Act*;
- (c) Co-operative Societies;
- (d) Exchange Bureaux (i.e. cambios);
- (e) Money Transfer and Remittance Agents and Agencies approved under *the Bank of Jamaica Act*;
- (f) Microcredit Institutions.

These institutions are supervised by Bank of Jamaica for compliance with AML/CFT/CPF requirements and Bank of Jamaica is the Competent Authority specified by the Minister of National Security. Bank of Jamaica is also a Supervisory Authority as defined in the Fourth Schedule to the Proceeds of Crime Act.

SECOND SCHEDULE (Paragraph 5)

1. Territories identified by the Financial Action Task Force²
- (a) The Specified Territories for which transaction background and purpose checks and enhanced due diligence measures should be applied are the jurisdictions identified by the Financial Action Task Force as jurisdictions with strategic deficiencies in their AML/CTF regimes and which have been included in a public statement issued by the Financial Action Task Force; and
 - (b) The Specified Territories in respect of which counter measures should be applied are the jurisdictions identified by the Financial Action Task Force as ‘High Risk’ jurisdictions which are subject to *a call for action* and which have been included in a public statement issued by the Financial Action Task Force.

Both public statements at (a) and (b), are updated from time to time by the FATF, and can be accessed from the FATF’s website as well as through the link *Documents — Financial Action Task Force (FATF) (fatf-gafi.org)*.

2. Territories identified by the Supervisory Authority³
- The Specified Territories in respect of which countermeasures should be applied are the jurisdictions (other than those at 1. above), which have been otherwise identified by the Supervisory Authority, whether spontaneously as a risk mitigation measure for the protection of the financial system or in response to other international obligations.

Dated the 29th day of March, 2023.

RICHARD BYLES
Governor, Bank of Jamaica and
Supervisor of Banks, Financial Holding Companies
and other Specified Financial Institutions.

¹ Interpretive Note to FATF Recommendation 18.
² FATF (2012-2021), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, www.fatf-gafi.org/recommendations.html.
³ FATF Recommendation 19.

Appendix VIII

Internal Procedure for communicating Listed Entity Designations Under section 14 of the
Terrorism Prevention Act (“TPA”)

Objective

Developing in-house foster turn-around mechanisms to communicate these orders under the TPA to the financial system (i.e. our licensees - banks, merchant banks, building societies, remittance companies, cambios and credit unions¹) as now required under the TPAA (2019) section 14(4D).

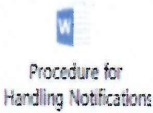
This Procedure seeks to document and streamline the existing procedure in order to fulfil The requirements of these obligations. This Procedure will be periodically reviewed and updated where deemed necessary to ensure the timeliness of communication of listed entity designations to persons regulated by BOJ

Steps to be Taken on Receipt of Notification By The Permanent Mission

A. Notification

1. Notification of the UN’s designation is received by BOJ (legal department - Senior Legal Counsel Regulation) from either or both Jamaica’s Permanent Mission to the UN and the ODPP by electronic mail with a copy of the UN designation attached.
2. The Senior Legal Counsel immediately alerts the regulatory authorities within BOJ of The notification of UN designation. This alert is done by email, it attaches a copy of the UN designation and reminds the Authorities, of their obligation under the TPA to alert their respective regulated entities of the designation and to the court order that will be done under the TPA.
3. The Regulatory Authorities within BOJ alert the officer dedicated to updating BOJ’s website with the UN designation and requisite court orders when these are received. That person posts the UN designation to BOJ’s website. This officer has the capacity to respond to these matters outside office hours and on weekends.
4. The dedicated officer then forwards the hyperlink to the relevant regulatory officer indicating the completion of the document uploaded on the website.
5. The Regulatory Authorities send out emails addressed to the CEOs and nominated officers of persons regulated by BOJ alerting these persons to the fact of the designation, that the designation is posted on BOJ’s website, to include the hyperlink for ease of access aad requests these persons to monitor BOJ’s website for the requisite order which will be posted as soon as it has been received.

- a. See internal processes for remittance and cambio sectors



- b. See internal processes for DTI and credit union sectors



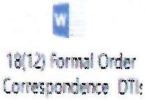
(Steps from first notification from Permanent Mission to posting order on BOJ’s website and communicating this to the financial sector occur within 24 hours).

Thereafter—

6. Formal writings to industry (i.e all persons regulated by BOJ) are subsequently done in relation these designations to reference to include reference to emails sent prior to the obligations of these entities under the TPA and the fact that BOJ will actively be monitoring compliance and licensees should be prepared to demonstrate compliance.

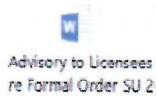
Appendices

Sample emails and communiques to the DTIs (commercial banks, merchant banks, building societies) and credit unions sector.



¹ Bank of Jamaica is the designated Competent Authority for co-operative societies for the purpose of the POCA and TPA. These designations occurred in 2007 and 2015 respectively. The Department of Friendly and Cooperative Societies is otherwise the statutory regulator for Co-operative Societies, Cabinet made a policy decision to place the cooprative societies that operate as financial co-oprative (i.e. credit unions) under the regulatory remit of Bank of Jamaica. The requisite legislation is now being developed.

Sample emails and communiques to the remittance and cambio sectors.



Bank of Jamaica
1267 Procedure 1/Oct2020

Register of Supreme Court Orders on UN Sanctions (For Amending/Adding/
Removing Entities or Individuals)

Date of Order	Date Dispatched to Entities and posted on website	Supreme Court Order No.	UN Sanctions List	Particulars
Listing for 2025				
17 June, 2025	17 June, 2025	SU2025 CV:02278	SCA/2/25 (01)	Order to add to add to Sanctions List: QDI.436 (1) Abubakar (2) Swalleh as a listed entity in keeping with UNSCR 1267 (1999), 1989 (2011) and 2253 (2015).
10 June, 2025	10 June, 2025	SU2025 CV:02204	SCA/2/25(3)	Order to remove from Sanction List QDI.095 Name: 1 : Hajjaj 23/4: Bin 3: Fahd 4: AlAjmi as a listed designated terrorist entity in keeping with UNSCR 1267 (1999), 1989 (2011) and 2253 (2015). Note: Whilst the Court Order is dated June 11, 2025, the notification was sent to the industry using the Sanction list sent by the Ministry of Foreign Affairs and Foreign Trade followed by the Court Order upon receipt.
25 February, 2025	25 February, 2025	SU2025 CV:00622	SCA/2/25 (04)	Order to remove from Sanction List QDi.095 Name: 1: Lionel 2: Dumont 3: NA4:Na as a designated terrorist entity in keeping with UNSCR 1267 (1999), 1989 (2011) and 2253 in keeping with UNSCR 1267 (1999), 1989 (2011) and 2253 (2015).
Listing for 2024				
04 December, 2024	04 December, 2024	SU2024 CV-04675	SCA/2/24(12)	Order to amend the Individual QDi.278 Name 1 : Muthana 2: Harith 3: Salman 4: Aldari as a terrorist entity and/or individual in keeping with UNSCR 1267 (1999), 1989 (2011) and 2253 (2015).
24 August, 2024	26 August, 2024	SU2024 CV:03180	SCA/2/24(09)	Order to remove: QDi.070 Name: 1: Yassine 2: Chekkouri 3 : na 4: na as a terrorist entity and/or individual in keeping with UNSCR 1267 (1999), 1989 (2011) and 2253 (2015).
27 April, 2024	29 April, 2024	SU2024 CV:01884	DPPA/SCADSC SOB/2024/SCA/ 2/24 (06)	Order to amend the individual QDi.431 Name: 1: Sanaullah 2: Ghafari 3 : na 4 na as a terrorist

				entity and/or individual in keeping with UNSCR 1267 (1999), 1989 (2011) and 2253 (2015).
Listing for 2023				
7 June, 2023	08 June, 2023	SU 2023 CV:01340	SCA/2/23 (08)	Order to remove: QDi.379 Name: 1:ABDAl-Aziz 2:Aday 3:Zimin4: Al-Fadhil QDi. 381 Name: l;Hamad2: Awad 3: Dahi Sarhan 4: Al-Shammari as a listed designated terrorist entity in keeping with UNSCR 1267 (1999), 1989 (2011) and 2253 (2015).
27 April, 2023	28 April, 2023	SU 2023 CV:01342	SCA/2/23 (06)	Order to add QDi.434 Name: Maulawi 2. Rajab 3. Na 4: na; QDi.435 Name: 1. Sultan Aziz 2, Azam 3. nan 4: na as a listed entity in keeping with UNSCR 1267(1999), 1989 (2011.) and 2253 (2015).
16 February, 2023	16 February, 2023	SU 2023 CV:00473	SCA2/23(01)	Order to add: QDi.443 Name 1 . Abdul 2. Rehman 3. Makki 4: na as a listed entity in keeping with UNSCR 1267(1999), 1989(2011) and 2253 (2015).
Listing for 2022				
1 June, 2022	01 June, 2022	SU 2022 CV:01744	SCA/2/22 (10)	Order to amend QDi.420 Name: 1: Taha 2: Ibrahim 3: Abdallah Bakr 4: Al KKhaway; QDi.426 Name: 1: Amir 2: Muhammad Sa'id3:Abdala-Rahman4:Al-Salbi as a listed entity in keeping with the decision of the UNSCR 1267(1999), 1989(2011) and 2253 (2015).
5 April, 2022	06 April, 2022	SU 2022 CV:01151	SCA/2/22 (08)	Order to amend: QDe.161 Name: Islamic State in Iraq and the Levan - Khorasan (Isil-K) A.k.a.:a) Isil Khorasan b) Islamic State's Khorasan Province c) ISIS Wilayah Khorasan d) Isil's South Asia Branch e) South Asian Chapter of Isil f) The Islamic State of Iraq and ash-Sham-Khorasan Province g) The Islamic State of Iraq and Syria-Khorasan h) Islamic State of Iraq and Levant in Khorasan Province i) Islamic State Khurasan j) Isis-K k) Isisk 1) Is-Khorasan as a listed entity in keeping with the decision of UNSCR 1267 (1999), 1989 (2011) and 2253 (2015).
9 March, 2022	9 March, 2022	SU 2022 CV:00821	SCA/2/22 (07)	Order to add QDe.168 Name Khatiba Al-Tawhid Wai- Jihad (KTJ) as a listed entity in keeping with the decision of UNSCR 1267 (1999), 1989 (2011) and 2253 (2015).
7 March, 2022	9 March, 2022	SU 2022 CV:00799	SCA/2/22 (06)	Order to remove: QDi.346 Name: 1: Abd Al-Malik2: Muhammad 3: Yusuf 4: 'Uthman" ABD Al-Salam QDi.402Name: l:Nayif 2: Salih 3: Salim 4: Al-Qaysi as a

Date of Order	Date Dispatched to Entities and posted on website	Supreme Court Order No.	UN Sanctions List	Particulars
				listed designated terrorist entity in keeping with the decision of the UNSCR 1267 (1999), 1989 (2011) and 2253 (2015).
26 January, 2022	26 January, 2022	SU 2022	SCA/2/22 (03) CV:00230	An Order to remove the individual listed as: QDi.099 with the Names: 1: Khalil 2: Ben Ahmed 3: Ben Mohammed 4; Jarraya as a listed designated terrorist individual in keeping with the decision of the UNSCR 1267(1999), 1989 (2011) and 2253(2015).
19 January, 2022	18 January, 2022	SU 2022 CV:00136	SCA/2/22 (02)	Order to remove: QDe.071 Name: Al-Haramain Islamic Foundation, QDe.072 Name: Al-Haramain Islamic Foundation (Somalia) and QDe.103 Name: Al-Haramain Foundation (Indonesia) as listed designated terrorist entities in keeping with the decision of the UNSCR 1267 (1999), 1989 (2011) and 2253(2015).
7 January, 2022	10 January, 2022	SU 2022 CV:0036 and SU 2022 CV:0034	SCA/2/21 (19) and SCA/2/22(01)	Order to add: QDi.431Name: 1: Ashraf, or Name: 2: Al-Qizani and QDe 167 Name Jundd Al-Khilaf in Tunisia as listed entities in keeping with the decision of UNSCR 1267 (1999), 1989 (2011) and 2253 (2015). Order to remove: QDi.302 Name: 1: Mevlüt 2: Kar QDi.347Name::l: Denis2: Mamadou 3: Gerhard 4: Cuspert QDi.390Name: l:Nayef2: Salam 3: Muhammad 4: Ujaym Al-Hababi QDi.391 Name: l:Turki 2: Mubarak 3: Abdullah 4: Ahmadd Al-Binali QDi.393 Name: l:Tuah2: Febriwansyah as listed designated terrorist entities in keeping with the decision of the UNSCR 1267 (1999), 1989 (2011) and 2253 (2015).
		Listing for 2020		
12 September, 2020	17 September, 2020	SU 2020 CV:03421	SCA/2/20(15)	Order to add 1 .QDi 096 Name:: 1 Moussa 2: Ben Omar 3: Ben Ali 4:: Essadi; 2) QDi.099 Name: 1 : Said 2: Ben Ahmed 3: Ben Mohamed 4: Jarraya 3) QDi: 138 Name 1: Said 2: Ben Abdel Hakim 3: Ben Omar 4: Al-Cherif 4)QDi:139 Name 1: Imed 2: Ben Mekki 3: Zarkaoui 5) QDi.140 Name 1: Kamal 2: Ben Maoeldi 3: Ben Hassan 4: Al-Haraoui 6) QDi. 143 Name 1: Hamadi 2: Ben Abdul Aziz 3: Ben Ali 4: Bouyehia as listed designated terrorist entities in keeping with the decision of the UNSCR 1267(1999), 1989 (2011) and 2253 (2015).

Date of Order	Date Dispatched to Entities and posted on website	Supreme Court Order No.	UN Sanctions List	Particulars
22 May, 2020	5 June, 2020	SU 2020 CV:01636	SCA/2/20(09)	Order to add entity QDi.426 Name 1: Amir Muhammad Sa'id Abdal-Rahmaan al-Mawla as a listed designated to entities from the revised ISIL (Da'esh) and Al-Qaida Sanctions Committee List.
7 February, 2020	17 February, 2020	SU 2020 CV:00459	SCA/2/20 (1)	Order to make an addition to the list of individuals namely: QDi.425; Name 1: Amadou 2: KOUFA; 3: na 4: na on the revised ISIL (Da'esh) and Al-Qaida Sanctions Committee List.
Listing for 2019				
24 April, 2019	21 May, 2019	SU2019 CV:01757	SCA/2/19 (10)	Order to remove individual: QDi. 160 Name: 1: Fethi 2: Benn Hassen 3: Ben Salem 4: Al-Haddad on revised ISIL (Da'esh) and Al-Qaida Sanctions Committee List.
23 April, 2019	24 April, 2019	SU2019 CV:01719	SCA/2/19 (09)	Order to amend individual: QDi. 187 Name: 1: ZulKarnaenaris 2: na Sumarsono 3: na 4: na on the revised ISIL (Da'esh and Al-Qaida Sanctions Committee List.
Listing for 2018				
7 June, 2018	18 June, 2018	HCV:02188 2018	SCA/2/18(15)	Order to amend entities and other groups AL-Nusrah Front For the People Of The Levant on the revised ISIL (Da'esh) and Al-Qaida Sanction Committee List.
11 May, 2018	11 May, 2018	2018HCV: 01831	SCA/2/18(12)	Order to amend A. Individuals: QDi247 Name: 1: Ruben 2: Pestano 3: Lavilla, JR 4: na and QDi29 1 Name: 1 :Ibrahim 2: Hassan 3: Tali 4: Al-Asiri. Entities: QDe.071: Name Al-Haramain Islamic Foundation and QDe.128 Name: Rajah Solaiman Movement on the revised ISIL (Da'esh) and Al-Qaida Sanctions Committee List.
13 March, 2018	26 March, 2018	2018 HCV:01045	-	Order to designate entities and individuals as terrorist entities and/or individuals associated with ISIL (Da'esh) and Al-Qaida.

Appendix IX

Advisory to Licensees on the Management of Cyber-Risks

- I. Cyber risks have become an ongoing threat to financial institutions and specifically the proliferation of synthetic media, particularly deep fakes, which poses a potential risk to financial systems and the AML/CFT regime. The use of artificial intelligence (AI) generated is now a very common and sophisticated tool widely used which is exploited by criminals to exploit the system for illicit financial flows. Deep fakes are synthetic media produced by Generative Artificial Intelligence (GenAI) tools which includes video, audio or images which are a ‘potent emerging threat’ to financial institutions, their customers and the economy. Deep fake audio, video, and documentation can be weaponized to compromise Know-Your-Customer (KYC) and Customer Due Diligence (CDD) processes, and digitally driven onboarding scenarios. The risks include but are not limited to market risk, information or cyber security risk, fraud risk, regulatory risk and reputational risk. The emerging risks include data breaches, synthetic identities, altering or creating fraudulent identity documents, photos/images and videos for opening accounts, exploitation of digital banking platforms, misuse of synthetic identities, deep fakes used in combination with social engineering to creates voices of employees and executives to will cause deception by customers causing them to divulge personal data.
- II. Against the background of emerging cyber threats, the Bank of Jamaica implemented Standards of Sound Practice on the Management of Cyber Risks (“Guidelines”) to establish minimum Standards and guidelines on the management of cyber risk under the Banking Services Act, 2014. The Guidelines instruct that licensees are expected to implement an effective framework to manage the cyber risk exposures inherent in their operations, whick may result in significant financial loss, legal liabilities and reputational damage. The Financial Action Task Force (FATF) in a publication entitled “*Illicit Financial Flows from Cyber-Enabled Fraud*” has indicated its global concern for cyber-enabled fraud (CEF) and recommends that financial institutions continuously assess vulnerabilities tied to generative AI. The Caribbean region as shared by FATF, is highly susceptible to CEF and related laundering with an increase in overall fraud related to CEF.

Digitalisation and the development of new technologies also serve as key drivers for CEF growth. By embedding these risks into Risk-Based Approach (RBA), FATF recommends that financial institutions continuously assess vulnerabilities tied to generative AI, update internal frameworks, and implement controls. Therefore, licensees are required to formulate and implement effective guidance on cyber risk including deep fakes and to implement the appropriate mitigation measures are employed and effectively applied.

- III. Countermeasures for deep fakes and synthetic media should be considered such as automated detection software and systems, customer awareness programmes, education and training for staff, multifactor authentication and verification, stronger KYC and CDD measures, reviewing of customer documents and transaction monitoring.

We recommend that licensees examine the risk indicators and utilise the information provided in the publications below for useful anti-fraud requirements and formulate controls to detect and prevent cyberthreats through deep fakes and other digitalization and technology driven frauds to combat ML/TF risks.

- Bank of Jamaica’s Standard of Sound Practice on Management of Cyber-Risks (September 2024) [Standard-of-Sound-Practice-Management-of-Cyber—Risks.pdf](#)
- FATF paper (November 2023) [Illicit-financial-flows—cyber-enabled-fraud.pdi.coredownload.inline.pdf](#)
- The IMF’s paper (2021): [The Global Cyber Threat to Financial Systems - IMF F and D](#)

Appendix X—Paragraphs 13A and 231A

Formal Order dated March 12, 2026 Pursuant to section 3A(2) of UNSCRIA Re: Proscribed persons and Entities Relevant to Iran reapplied as of September 27, 2025.

FORMAL ORDER

In the Supreme Court of Judicature of Jamaica
Claim No. SU2026CV:00982

In the matter of an application under section 3A (2) of the United Nations Security Council Resolutions Implementation Act.

AND

In the matter of an application by the Director of Public Prosecutions for an Order under section 3A (4) of the United Nations Security Council Resolutions Implementation Act to designate a person or entity as a proscribed person or entity in keeping with a decision of the United Nations Security Council

AND

In the matter of an application by the Director of Public Prosecutions for an Order to declare the proscribed persons, entities and other groups so specified in Sections A and B of UN document DPPA/SCAD/SCA/4/25(1) as proscribed persons or entities for the purposes of the United Nations Security Council Resolutions Implementation Act.

BETWEEN	The Director of Public Prosecutions	APPLICANT
AND	1: Fereidoun 2: Abbasi-Davani	1st DEFENDANT
AND	1: Dawood 2: Agha-Jani	2nd DEFENDANT

AND	1: Azim 2: Aghajani	3rd DEFENDANT
AND	1: Ali Akbar 2: Ahmadian	4th DEFENDANT
AND	1: Amir Moayyed 2: Alai	5th DEFENDANT
AND	1: Behman 2: Asgarpour	6th DEFENDANT
AND	1: Mohammad Fedai 2: Ashiani	7th DEFENDANT
AND	1: Abbas Rezaee 2: Ashtiani	8th DEFENDANT
AND	1: Bahmanyar Morteza 2: Bahmanyar	9th DEFENDANT
AND	1: Haleh 2: Bakhtiar	10th DEFENDANT
AND	1: Morteza 2: Behzad	11th DEFENDANT
AND	1: Ahmad Vahid 2: Dastjerdi	12th DEFENDANT
AND	1: Ahmad 2: Derakshandeh	13th DEFENDANT
AND	1: Mohammad 2: Eslami	14th DEFENDANT
AND	1: Reza-Gholi 2: Esmaeli	15th DEFENDANT
AND	1: Mohsen 2: Fakhrizadeh-Mahabadi	16th DEFENDANT
AND	1: Mohammad 2: Hejazi	17th DEFENDANT
AND	1: Mohsen 2: Hojati	18th DEFENDANT
AND	1: Seyyed Hussein 2: Hosseini	19th DEFENDANT
AND	1: Mehrdada Akhlaghi 2: Kitabachi	20th DEFENDANT
AND	1: Ali Hajinia 2: Leilabadi	21st DEFENDANT
AND	1: Naser 2: Maleki	22nd DEFENDANT
AND	1: Hamid-Reza 2: Mohajerani	23rd DEFENDANT
AND	1: Jafar 2: Mohammadi	24th DEFENDANT
AND	1: Ehsan 2: Monajemi	25th DEFENDANT
AND	1: Mohammad Reza 2: Naqdi	26th DEFENDANT
AND	1: Mohammad Mehdi 2: Nejad Nouri	27th DEFENDANT
AND	1: Houshang 2; Nobari	28th DEFENDANT
AND	1: Mohammad 2: Qannadi	29th DEFENDANT
AND	1: Amir 2: Rahimi	30th DEFENDANT
AND	1: Javad 2: Rahiqi	31st DEFENDANT
AND	1: Abbas 2:Rashidi	32nd DEFENDANT
AND	1: Morteza 2: Rezaie	33rd DEFENDANT
AND	1: Javad 2: Karimi Sabet	34th DEFENDANT
AND	1: Morteza 2: Safari	35th DEFENDANT
AND	1: Yahya Rahim 2: Safavi	36th DEFENDANT
AND	1: Seyed Jaber 2: Safdari	37th DEFENDANT
AND	1: Hosein 2: Salimi	38th DEFENDANT
AND	1: Qasem 2: Soleimani	39th DEFENDANT
AND	1: Ghasem 2: Soleymani	40th DEFENDANT
AND	1: Ali Akbar 2: Tabatabaei	41st DEFENDANT
AND	1: Mohammad 2: Reza Zahedi	42nd DEFENDANT
AND	1: Mohammad 2: Baqer Zolqadr	43rd DEFENDANT
AND	7 Th of Tir	44th DEFENDANT
AND	Abzar Boresh Kaveh Co. (Bk Co.)	45th DEFENDANT
AND	Amin Industrial Complex A.k.a.: a) Amin Industrial Compound b) Amin Industrial Company	46th DEFENDANT

AND	Ammunition and Metallurgy Industries Group (AMIG) A.k.a.: Ammunition Industries Group	47th DEFENDANT
AND	Armament Industries Group (AIG)	48th DEFENDANT
AND	Atomic Energy Organisation of Iran (AEOI)	49th DEFENDANT
AND	Bank Sepah and Bank Sepah l International	50th DEFENDANT
AND	Barzagani Tejarart Tavanmad Saccal Comapnies	51st DEFENDANT
AND	Behineh Trading Co.	52nd DEFENDANT
AND	Cruise Missile Industry Group A.KA. Navel Defence Missile industry Group	53rd DEFENDANT
AND	Defence Industries Organisation (DIO)	54th DEFENDANT
AND	Defense Technology and Science Research Center (DTSRC)	55th DEFENDANT
AND	Doostan International Company (DICO)	56th DEFENDANT
AND	Electro Sanam Company	57th DEFENDANT
AND	Esfahan Nuclear Fuel Research and Production Centre (NFRPC) and Esfahan Nuclear Technology Centre (ENTC)	58th DEFENDANT
AND	Ettehad Technical Group	59th DEFENDANT
AND	Fajr Industrial Group	60th DEFENDANT
AND	Farasakht Industries	61st DEFENDANT
AND	Faray and Technique	62nd DEFENDANT
AND	Fater Institute A.K.A. Faater Institute	63rd DEFENDANT
AND	First East Export Bank, P.L.C.	64th DEFENDANT
AND	Gharagahe Sazandegi Ghaem	65th DEFENDANT
AND	Ghorb Karbala	66th DEFENDANT
AND	Ghorb Nooh	67th DEFENDANT
AND	Hara Company	68th DEFENDANT
AND	Imensazan Consultant Engineers Institute	69th DEFENDANT
AND	Industrial Factories of Precision (IFP) Machinery A.K.A. Instrumentation Factories Plant	70th DEFENDANT
AND	Irano Hind Shipping Company	71st DEFENDANT
AND	Irisl Benelux NV	72nd DEFENDANT
AND	Jabber Ibn Hayan	73rd DEFENDANT
AND	Joza Industrial Co.	74th DEFENDANT
AND	Kala-Electric A.K.A. Kalaye Electric	75th DEFENDANT
AND	Karaj Nuclear Research Centre	76th DEFENDANT
AND	Kaveh Cutting Tools Company	77th DEFENDANT
AND	Kavoshyar Company	78th DEFENDANT
AND	Khatam Al-Anbiya Construction Headquarters (KAA)	79th DEFENDANT
AND	Khorasan Metallurgy Industries	80th DEFENDANT
AND	M. Babaie Industries	81st DEFENDANT

AND	Makin	82nd DEFENDANT
AND	Malek Ashtar University	83rd DEFENDANT
AND	Mesbah Energy Company	84th DEFENDANT
AND	Ministry of Defense Logistics Export A.K.A. Modlex	85th DEFENDANT
AND	Mizan Machinery Manufacturing A.K.A.	86th DEFENDANT
AND	Modern Industries Technique Company (MITEC) A.K.A. a) MITEC b) Rahkar Company c) Rahkar Industries d) Rahkar Sanaye Company e) Rahkar Sanaye Novin	87th DEFENDANT
AND	Niru Battery Manufacturing Company	88th DEFENDANT
AND	Novin Energy Company	89th DEFENDANT
AND	Nuclear Research Center for Agriculture and Medicine (NFRPC) A.K.A. a) Center for Agriculture Research and Nuclear Medicine b) Karaji Agricultural and Medical Research Center	90th DEFENDANT
AND	Omran Sahel	91st DEFENDANT
AND	Oriental Oil Kish	92nd DEFENDANT
AND	Parchin Chemical Industries	93rd DEFENDANT
AND	Pars Aviation Services Company	94th DEFENDANT
AND	Pars Trash Company	95th DEFENDANT
AND	Pejman Industrial Services Corporation	96th DEFENDANT
AND	Pishgam Energy Industries A.K.A. Pioneer Energy Industry	97th DEFENDANT
AND	Qods Areonautics Industries	98th DEFENDANT
AND	Rah Sahel	99th DEFENDANT
AND	Rahab Engineering Institute	100th DEFENDANT
AND	Sabalan Company	101st DEFENDANT
AND	Sad Import Export Company	102nd DEFENDANT
AND	Safety Equipment Procurement (SEP)	103rd DEFENDANT
AND	Sahand Aluminum Parts Industrial Company (SAPICO)	104th DEFENDANT
AND	Sahel Consultant Engineers	105th DEFENDANT
AND	Sanam Industrial Group	106th DEFENDANT
AND	Sepanir	107th DEFENDANT
AND	Sepasad Engineering Company	108th DEFENDANT
AND	Shahid Bagheri Industrial Group (SBIG)	109th DEFENDANT
AND	Shahid Hemmat Industrial Group (SHIG)	110th DEFENDANT
AND	Shahid Karrazi Industries	111th DEFENDANT
AND	Shahid Sattari Industries A.K.A. Shahid Sattari Group Equipment Industries	112th DEFENDANT
AND	Shahid Sayyade Shirazi Industries (SSSI)	113th DEFENDANT
AND	Sho ‘A’ Aviation	114th DEFENDANT
AND	South Shipping Line Iran (SSL)	115th DEFENDANT
AND	Special Industries Group (SIG)	116th DEFENDANT
AND	Tamas Company	117th DEFENDANT

AND	Tiz Pars	118th DEFENDANT
AND	Ya Mahdi Industries Group	119th DEFENDANT
AND	Yas Air	120th DEFENDANT
AND	Yazd Metallurgy Industries (YMI) A.K.A. a) Yazd Ammunition Manufacturing and Metallurgy Industries b) Directorate of Yazd Ammunition and Metallurgy Industries	121st DEFENDANT

In Chambers 10

Before the Honourable Mrs. Justice Simone Wolfe-Reece.

This 12th day of March, 2026.

Upon the hearing of the fixed date claim form filed by the Director of Public Prosecutions and dated 12th March, 2026 and coming up for the hearing this day and upon hearing Counsel for the Applicant, Miss Ashtelle Steele, as instructed by the Office of the Director of Prosecutions.

It is hereby ordered that:

1. In accordance with section 3A (4) of the United Nations Security Council Resolutions Implementation Act, all individuals, entities and other groups designated pursuant to United Nations Security Council resolutions 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2009) and 1929 (2010), being all the Defendants herein and as specified in Sections A and B of United Nations document with reference number DPPA/SCAD/SCA/4/25(1) dated 27 September, 2025, attached hereto, are hereby declared as prescribed persons or proscribed entities as the case may be, for the purposes of the United Nations Security Council Resolutions Implementation Act.
2. In accordance with section 8A(1) of the United Nations Security Council Resolutions Implementation Act, no person in Jamaica or no Jamaican in or outside of Jamaica shall, in relation to any person or entity proscribed by this Order, knowingly:
 - (a) deal directly with any assets that are owned or controlled by or on behalf of, or at the direction of a person or entity that is herein proscribed, including funds derived or generated fro property owned or controlled directly or indirectly by that proscribed person or entity;
 - (b) enter onto or facilitate, directly or indirectly, any transaction in respect of assets referred to in paragraph (a) above;
 - (c) provide any financial or other related services in respect of any assets referred to in paragraph (a) to, for the benefit of, or at the direction of, a proscribed person or entity; or
 - (d) make any property or any financial or other related service available, directly or indirectly, for the benefit of a proscribed person or entity, or convert any such property or take steps to convert or disguise that the property is owned or controlled by or on behalf of a proscribed person or entity.
3. The Applicant’s attorney is to prepare, file and serve a copy of this Order along with a copy of United Nations document with reference number DPPA/SCAD/SCA/4/25(1) dated 27th September, 2025 on all relevant authorities and financial institutions in Jamaica.

By the Court:

HONOURABLE MRS. JUSTICE SIMONE WOLFE-REECE

Judge of the Supreme Court.

Filed by Director of Public Prosecutions whose address for service is Public Building West King Street, in the city and parish of Kingston, telephone number (876) 922-6321-5 fax (876) 922-4318.



HEADQUARTERS SIEGE NEW YORK, NY 10017

REFERENCE: DPPA/SCAD/SCA/425(1)

The Secretariat of the United Nations presents its compliments to the Permanent Representatives of Member States and Permanent Observers of non-member States to the United Nations and wishes to convey the following:

Pursuant to the process set forth in paragraphs 11 and 12 of Security Council resolution 2231 (2015), effective 27th September at 8 p.m. Eastern Daylight Time, all provisions of resolutions 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1835 (2008) and 1929 (2010) have been re-applied in the same manner as they applied before the adoption of resolution 2231 (2015) on 20th July, 2015.

Accordingly, the sanctions list maintained by the Security Council Committee established pursuant to resolution 1737 (2006) has been re-established and includes 43 individuals and 78 entities that were listed before the adoption of resolution 2231 (2015) on 20th July, 2015 (2015).

The following individuals and entities have been added back to the Committee’s Sanctions List:

A. Individuals

IRL001 Name: 1 FEREIDOUN 2: ABBASI-DAVANI 3: na 4: na
Title: na Designation: Senior Ministry of Defence and Armed Forces Logistics (MODAFL) Scientist DOB: a) 1958 b) 1959 POB: Abadan, Iran Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: na National Identification no: na Address: na Listed on : 24 Mar. 2007 (amended on 17th Dec., 2014) Other information: Has “links to the Institute of Applied Physics, working closely with Mohsen Fakhrizadeh-Mahabadi” (designated under IRL016) [Old Reference # 1.47.C.1].

IRL002 Name: 1 DAWOOD 2: Agha-jani 3: na 4: na
Title: na Designation: Head of Pilot Fuel Enrichment Plant (PFEP) (Natanz) DOB: 23rd April, 1957 POB: Ardebil, Iran Good quality a.k.a.: Nationality: na Passport no: 15824769, issued in Iran National Identification no: na Address: na Listed on: 23rd December, 2006 (amended on 17th December, 2014) other information: [Old Reference # 1.37.C3]

IRL003 Name: 1 AZIM 2: AGHAJANI 3: na 4: na
Title: na Designation: Member of the IRGC-Qods Force operating under the direction of Qods Force Commander, Major General Qasem Soleimani, who was designated by the UN Security Council in resolution, 1747 (2007) DOB: na POB: na Good quality a.k.a. Azim Adhajani; Azim Agha-Jani Low quality a.k.a.: na Nationality: Iran Passport no: a) 6620505, issued in Iran b) 9003213, issued in Iran National Identification no: na Address: na Listed on: 18th April, 2012 (amended on 17th December, 2014) Other information: Facilitated a breach of paragraph 5 of resolution 1747 (2007) prohibiting the export of arms and related material from Iran. [Old reference # LAC50.18..04.12(1)]

IRL004 Name: 1 ALI AKBAR 2: AHMADIAN 3: na 4: na
Title: na Designation: Vice Admiral; Chief of IRGC Joint Staff DOB: 1961 POB: Kerman Iran Good quality a.k.a.: Ali Akbar Ahmadian Low quality a.k.a.: na Nationality: na Passport no.: na National Identification no: na Address: na Listed on 24th March, 2007 (amended on 17th December, 2014) Other information: Position changed. [Old Reference # L47.D.2]

IRL005 Name: 1: AMIR MOAYYED 2: ALAI 3: na 4: na
Title: na Designation: Designated for involvement in managing the assembly and engineering of centrifuges. DOB: na POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 3 Mar. 2008 (amended on 17 Dec. 2014) Other information: [Old Reference # L03.1.1]

IRL006 Name: 1: BEHMAN 2: ASGARPOUR 3: na 4: na
Title: na Designation: Operational Manager (Arak) DOB: na POB: na Good quality a.k.a.: Behman Asgharpour; Behman Asgharpur Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 23 Dec. 2006 (amended on 17 Dec. 2014) Other information: [Old Reference # L37.C.2]

IRL007 Name: 1: MOHAMMAD FEDAI 2: ASHIANI 3: na 4: na
Title: na Designation: Designated for involvement in the production of ammonium uranyl carbonate and management of the Natanz enrichment complex. DOB: na POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 3 Mar. 2008 (amended on 17 Dec. 2014) Other information: [Old Reference # L3.1.2]

IRL008 Name: 1: ABBAS REZAEI 2: ASHTIANI 3: na 4: na
Title: na Designation: Senior official at the AEOI Office of Exploration and Mining Affairs DOB: na POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 3 Mar. 2008 (amended on 17 Dec. 2014) Other information: [Old Reference # L03.1.3]

IRL009 Name: 1: BAHMANYAR MORTEZA 2: BAHMANYAR 3: na 4: na
Title: na Designation: Head of Finance and Budget Department of the Aerospace Industries Organization (AIO).

DOB: 31 Dec. 1952 POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: Iran Passport no: a) 10005159, issued in Iran b) 10005159, issued in Iran National identification no: na Address: na Listed on: 23 Dec. 2006 (amended on 17 Dec. 2014) Other information: [Old Reference # L37.D.4]

IRL010 Name: 1: HALEH 2: BAKHTIAR 3: na 4: na
Title: na Designation: Designated for involvement in the production of magnesium at a concentration of 99.9%.
DOB: 1975 POB: na Good quality a.k.a.: Halen Bakhtiar; Haleh Bakhtiari; Haleh Bakhtiyar Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 3 Mar. 2008 (amended on 17 Dec. 2014) Other information: [Old Reference # L03.I.4]

IRL011 Name: 1: MORTEZA 2: BEHZAD 3: na 4: na
Title: na Designation: Designated for involvement in making centrifuge components. DOB: 7 Jun. 1959 POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 3 Mar. 2008 (amended on 17 Dec. 2014) Other information: [Old Reference # L03.I.5]

IRL012 Name: 1: AHMAD VAHID 2: DASTJERDI 3: na 4: na
Title: na Designation: Head of the AIO DOB: 15 Jan. 1954 POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: A0002987, issued in Iran National identification no: na Address: na Listed on: 23 Dec. 2006 (amended on 17 Dec. 2014) Other information: Served as Deputy Defense Minister 2009-10. [Old Reference # L37.D.2]

IRL013 Name: 1: AHMAD 2: DERAKHSHANDEH 3: na 4: na
Title: na Designation: Chairman and Managing Director of Bank Sepah, which provides support for the AIO and subordinates, including SHIG and SBIG, both of which were designated under resolution 1737 (2006). DOB: 11 Aug. 1956 POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: 33 Hormozan Building, Pirozan St., Sharak Ghods, Tehran, Iran Listed on: 24 Mar. 2007 (amended on 17 Dec. 2014) Other information: [Old Reference # L47.C.8]

IRL014 Name: 1: MOHAMMAD 2: ESLAMI 3: na 4: na
Title: Dr. Designation: Head of Iran's Defence Industries Training and Research Institute. DOB: na POB: na Good quality a.k.a.: Mohammad Islami; Mohamed Islami; Mohammed Islami Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 3 Mar. 2008 (amended on 17 Dec. 2014) Other information: Served as Deputy Defence Minister from 2012 to 2013. [Old Reference # L03.I.6]

IRL015 Name: 1: REZA-GHOLI 2: ESMAELI 3: na 4: na
Title: na Designation: Head of Trade and International Affairs Department of the AIO. DOB: 3 Apr. 1961 POB: na Good quality a.k.a.: Reza-Gholi Ismaili Low quality a.k.a.: na Nationality: na Passport no: A0002302, issued in Iran National identification no: na Address: na Listed on: 23 Dec. 2006 (amended on 17 Dec. 2014) Other information: [Old Reference # L37.D.3]

IRL016 Name: 1: MOHSEN 2: FAKHRIZADEH-MAHABADI 3: na 4: na
Title: na Designation: Senior MODAFL scientist; Former head of the Physics Research Centre (PHRC) DOB: na POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: a) A0009228, issued in Unconfirmed (likely Iran) b) 4229533, issued in Unconfirmed (likely Iran) National identification no: na Address: na Listed on: 24 Mar. 2007 (amended on 17 Dec. 2014) Other information: The IAEA have asked to interview him about the activities of the PHRC over the period he was head but Iran has refused. [Old Reference # L47.C.2]

IRL017 Name: 1: MOHAMMAD 2: HEJAZI 3: na 4: na
Title: na Designation: Brigadier General/Commander of Bassij resistance force DOB: 1959 POB: Isfahan, Iran Good quality a.k.a.: Mohammed Hijazi Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 24 Mar. 2007 (amended on 17 Dec. 2014) Other information: [Old Reference # L47.D.5]

IRL018 Name: 1: MOHSEN 2: HOJATI 3: na 4: na
Title: na Designation: Head of Fajr Industrial Group, which is designated under resolution 1737 (2006) for its role in the ballistic missile programme. DOB: 28 Sep. 1955 POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: G4506013, issued in Iran National identification no: na Address: na Listed on: 24 Mar. 2007 (amended on 17 Dec. 2014) Other information: [Old Reference # L47.C.5]

IRL019 Name: 1: SEYYED HUSSEIN 2: HOSSEINI 3: na 4: na
Title: na Designation: AEOI official involved in the heavy water research reactor project at Arak. DOB: 27 Jul. 1973 POB: na Good quality a.k.a.: Syed Husain Husaini; Syed Husein Huseini Low quality a.k.a.: na Nationality: na Passport no: K8196482 National identification no: na Address: na Listed on: 3 Mar. 2008 (amended on 17 Dec. 2014) Other information: [Old Reference # L03.I.7]

IRL020 Name: 1: MEHRDADA AKHLAGHI 2: KETABACHI 3: na 4: na
Title: na Designation: Head of the Shahid Bagheri Industrial Group (SBIG), which is designated under resolution 1737 (2006) for its role in the ballistic missile programme (designated under IRe.066). DOB: 10 Sep. 1958 POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: A0030940, issued in Iran National identification no: na Address: na Listed on: 24 Mar. 2007 (amended on 17 Dec. 2014) Other information: [Old Reference # L47.C.6]

IRL021 Name: 1: ALI HAJINIA 2: LEILABADI 3: na 4: na
Title: na Designation: Director General of Mesbah Energy Company DOB: 19 Feb. 1950 POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: E4710151, issued in Iran (Issued 15 October 2000; expired 15 October 2005) National identification no: na Address: na Listed on: 23 Dec. 2006 (amended on 17 Dec. 2014) Other information: [Old Reference # L37.C.6]

IRL022 Name: 1: NASER 2: MALEKI 3: na 4: na
Title: na Designation: a) Head of Shahid Hemmat Industrial Group (SHIG), which is designated under resolution 1737 (2006) for its role in Iran's ballistic missile programme (designated under IRe.067). b) MODAFL official overseeing work on the Shahab-3 ballistic missile programme, Iran's long range ballistic missile currently in service. DOB: 1960 POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: A0003039, issued in Iran National identification no: 0035011785, issued in Iran Address: na Listed on: 24 Mar. 2007 (amended on 17 Dec. 2014) Other information: [Old Reference # L47.C.7]

IRL023 Name: 1: HAMID-REZA 2: MOHAJERANI 3: na 4: na
Title: na Designation: Designated for involvement in production management at the Uranium Conversion Facility (UCF) at Esfahan. DOB: 9 Sep. 1977 POB: na Good quality a.k.a.: Hamid Reza Mohajerani Araghi Low quality a.k.a.: na Nationality: Iran Passport no: Diplomatic Passport: Z30321794 , issued in Iran (Issued on 12 June 2014, expires 12 June 2019) National identification no: na Address: na Listed on: 3 Mar. 2008 (amended on 17 Dec. 2014) Other information: [Old Reference # L03.I.9]

IRL024 Name: 1: JAFAR 2: MOHAMMADI 3: na 4: na
Title: na Designation: Technical Adviser to the AEOI in charge of managing the production of valves for centrifuges. DOB: na POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 23 Dec. 2006 Other information: [Old Reference # L37.C.5]

IRL025 Name: 1: EHSAN 2: MONAJEMI 3: na 4: na
Title: na Designation: Construction Project Manager, Natanz DOB: na POB: na Good quality a.k.a.: Ihsan Monajemi Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 23 Dec. 2006 (amended on 17 Dec. 2014) Other information: [Old Reference # L37.C.4]

IRL026 Name: 1: MOHAMMAD REZA 2: NAQDI 3: na 4: na
Title: na Designation: Brigadier-General/Former Deputy Chief of Armed Forces General Staff for Logistics and Industrial Research/Head of State Anti-Smuggling Headquarters DOB: a) 11 Feb. 1949 b) 11 Feb. 1952 c) 11 Feb. 1953 d) 11 Feb. 1961 POB: a) Najaf, Iraq b) Tehran, Iran Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 3 Mar. 2008 (amended on 17 Dec. 2014) Other information: Engaged in efforts to get round the sanctions imposed by resolutions 1737 (2006) and 1747 (2007). [Old Reference # L03.I.10]

IRL027 Name: 1: MOHAMMAD MEHDI 2: NEJAD NOURI 3: na 4: na
Title: na Designation: Lieutenant General/Rector of Malek Ashtar University of Defence Technology (chemistry department, affiliated to MODAFL, has conducted experiments on beryllium). DOB: na POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 23 Dec. 2006 (amended on 17 Dec. 2014) Other information: Deputy Minister of Science, Research and Technology. [Old Reference # L37.C.7]

IRL028 Name: 1: HOUSHANG 2: NOBARI 3: na 4: na
Title: na Designation: Designated for involvement in the management of the Natanz enrichment complex. DOB: na POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 3 Mar. 2008 (amended on 17 Dec. 2014) Other information: [Old Reference # L03.I.11]

IRL029 Name: 1: MOHAMMAD 2: QANNADI 3: na 4: na
Title: na Designation: Vice President for Research and Development of the AEOI DOB: 13 Oct. 1952 POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: Iran Passport no: a) 20694, issued in Iran b) A0003044, issued in Iran National identification no: na Address: na Listed on: 23 Dec. 2006 (amended on 17 Dec. 2014) Other information: [Old Reference # L37.C.1]

IRL030 Name: 1: AMIR 2: RAHIMI 3: na 4: na
Title: na Designation: Head of Esfahan Nuclear Fuel Research and Production Center DOB: na POB: na Good quality a.k.a.: na Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 24 Mar. 2007 (amended on 17 Dec. 2014) Other information: The Esfahan Nuclear Fuel Research and Production Center is part of the AEOI Nuclear Fuel Production and Procurement Company, which is involved in enrichment related activities. [Old Reference # L47.C.4]

IRL031 Name: 1: JAVAD 2: RAHIQI 3: na 4: na
Title: na Designation: Head of the AEOI Esfahan Nuclear Technology Center DOB: 24 Apr. 1954 POB: Marshad, Iran Good quality a.k.a.: Javad Rahigi; Jawad Rahigi; Jawad Rahiqi Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 18 Apr. 2012 (amended on 17 Dec. 2014) Other information: [Old Reference # I.29.A.23] IRI.032 Name: 1: ABBAS 2: RASHIDI 3: na 4: na Title: na Designation: Designated for involvement in enrichment work at Natanz. DOB: na POB: na Good quality a.k.a.: Abas Rashidi; Abbas Rashedi; Abas Rashedi Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 3 Mar. 2008 (amended on 17 Dec. 2014) Other information: [Old Reference # L03.I.12]

- IRL033 Name: 1: MORTEZA 2: REZAIE 3: na 4: na
Title: na Designation: Brigadier General/Deputy Commander of IRGC DOB: 1956 POB: na Good quality a.k.a.: Mortaza Rezaie; Mortaza Rezai; Morteza Rezai Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 24 Mar. 2007 (amended on 17 Dec. 2014) Other information: [Old Reference # L47.D.1]
- IRi.034 Name: 1: M. JAVAD 2: KARIMI SABET 3: na 4: na
Title: na Designation: Head of Novin Energy Company, which is designated under resolution 1747 (2007) (designated under IRe.046). DOB: 25 Jul. 1973 POB: na Good quality a.k.a.: Mohammed Sabet; Mohammad Sabet b) M. Javad Kareemi Sabet; M. Jawad Kareemi Sabet; M. Jawad Karimi Sabet Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 3 Mar. 2008 (amended on 17 Dec. 2014) Other information: [Old Reference # I.03.I.8]
- IRL035 Name: 1: MORTEZA 2: SAFARI 3: na 4: na
Title: na Designation: Rear Admiral/Commander of IRGC Navy DOB: na POB: na Good quality a.k.a.: Mortaza Safari; Morteza Saferi; Murtaza Saferi; Murtaza Safari Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 24 Mar. 2007 (amended on 17 Dec. 2014) Other information: [Old Reference #L47.D.4]
- IRL036 Name: 1: YAHYA RAHIM 2: SAFAVI 3: na 4: na
Title: na Designation: Major General/Commander, IRGC (Pasdaran) DOB: 1952 POB: Isfahan, Iran Good quality a.k.a.: Yahya Raheem Safavi Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 23 Dec. 2006 (amended on 17 Dec. 2014) Other information: [Old Refence # L37.E.1]
- IRL037 Name: 1: SEYED JABER 2: SAFDARI 3: na 4: na
Title: na Designation: Manager of the Natanz Enrichment Facilities DOB: na POB: na Good quality a.k.a.: Syed Jaber Safdari Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 24 Mar. 2007 (amended on 17 Dec. 2014) Other information: [Old Reference # I.47.C.3]
- IRL038 Name: 1: HOSEIN 2: SALIMI 3: na 4: na
Title: na Designation: General/Commander of the Air Force, IRGC (Pasdaran) DOB: na POB: na Good quality a.k.a.: Husain Salimi; Hosain Salimi; Hussain Salimi; Hosein Saleemi; Husain Saleemi; Hosain Saleemi; Hussain Saleemi; Hossein Salimi; Hossein Saleemi Low quality a.k.a.: na Nationality: na Passport no: D08531177 , issued in Iran National identification no: na Address: na Listed on: 23 Dec. 2006 (amended on 17 Dec. 2014) Other information: [Old Reference # L37.D.1]
- IRL039 Name: 1: QASEM 2: SOLEIMANI 3: na 4: na
Title: na Designation: Brigadier General/Commander of Qods force DOB: 11 Mar. 1957 POB: Qom, Iran Good quality a.k.a.: Qasim Soleimani; Qasem Sulaimani; Qasim Sulaimani; Qasim Sulaymani; Qasem Sulaymani; Kasim Soleimani; Kasim Sulaimani; Kasim Sulaymani Low quality a.k.a.: Haj Qasem; Haji Qassem; Sardar Soleimani Nationality: na Passport no: 008827 , issued in Iran National identification no: na Address: na Listed on: 24 Mar. 2007 (amended on 17 Dec. 2014) Other information: Promoted to Major General, retaining his position as Commander of Qods force. [Old Reference # L47.D.6]
- IRL040 Name: 1: GHASEM 2: SOLEYMANI 3: na 4: na
Title: na Designation: Director of Uranium Mining Operations at the Saghand Uranium Mine DOB: na POB: na Good quality a.k.a.: Ghasim Soleymani; Ghasem Sulaymani; Ghasem Solaymani Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 3 Mar. 2008 (amended on 17 Dec. 2014) Other information: [Old Reference # L03.I.13]
- IRL041 Name: 1: ALI AKBAR 2: TABATABAEI 3: na 4: na
Title: na Designation: Member of the IRGC Qods Force operating under the direction of Qods Force Commander, Major General Qasem Soleimani who was designated by the UN Security Council in resolution 1747 (2007) (designated under IRi.039). DOB: 1967 POB: na Good quality a.k.a.: a) Sayed Akbar Tahmaesebi; Syed Akber Tahmaesebi b) Ali Akber Tabatabaei; Ali Akber Tahmaesebi; Ali Akbar Tahmaesebi Low quality a.k.a.: na Nationality: Iran Passport no: a) 9003213, issued in Iran/unknown b) 6620505, issued in Iran / unknown National identification no: na Address: na Listed on: 18 Apr. 2012 (amended on 17 Dec. 2014) Other information: Facilitated a breach of paragraph 5 of resolution 1747 (2007) prohibiting the export of arms and related materiel from Iran. [Old Reference # LAC.50.18.04.12.(2)]
- IRL042 Name: 1: MOHAMMAD REZA 2: ZAHEDI 3: na 4: na
Title: na Designation: Brigadier General/Commander of IRGC Ground Forces DOB: 1944 POB: Isfahan, Iran Good quality a.k.a.: Mohammad Reza Zahidi; Mohammad Raza Zahedi Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 24 Mar. 2007 (amended on 17 Dec. 2014) Other information: [Old Reference # L47.D.3]
- IRL043 Name: 1: MOHAMMAD BAQER 2: ZOLQADR 3: na 4: na
Title: na Designation: a) General/IRGC officer b) Deputy Interior Minister for Security Affairs DOB: na POB: na Good quality a.k.a.: Mohammad Bakr Zolqadr; Mohammad Bakr Zolkadr; Mohammad Baqer Zolqadir; Mohammad Baqer Zolqader Low quality a.k.a.: na Nationality: na Passport no: na National identification no: na Address: na Listed on: 24 Mar. 2007 (amended on 17 Dec. 2014) Other information: [Old Reference # L47.D.7]

B. Entities and other groups

- IRe.001 Name: 7TH OF TIR
A.k.a.: na F.k.a.: na Address: na Listed on: 23 Dec. 2006 (amended on 17 Dec. 2014) Other Information: Subordinate of Defence Industries Organisation (DIO), widely recognized as being directly involved in the nuclear programme. [Old Reference #E.37.A.7]
- IRe.002 Name: ABZAR BORESH KAVEH CO. (BK CO.)
A.k.a.: na F.k.a.: na Address: na Listed on: 3 Mar. 2008 (amended on 17 Dec. 2014) Other Information: Involved in the production of centrifuge components. [Old Reference # E.03.III.1]
- IRe.003 Name: AMIN INDUSTRIAL COMPLEX A.k.a.: a) Amin Industrial Compound b) AminIndustrial Company
F.k.a.: na Address: a) P.O. Box 91735-549, Mashad, Iran b) Amin Industrial Estate, Khalage Rd., Seyedi District, Mashad, Iran c) Kaveh Complex, Khalaj Rd., Seyedi St., Mashad, Iran Listed on: 9 Jun. 2010 (amended on 17 Dec. 2014) Other Information: Sought temperature controllers which may be used in nuclear research and operational/production facilities. Amin Industrial Complex is owned or controlled by, or acts on behalf of, DIO, which was designated in resolution 1737 (2006). [Old Reference # E.29.I.1]
- IRe.004 Name: AMMUNITION AND METALLURGY INDUSTRIES GROUP (AMIG)
A.k.a.: Ammunition Industries Group F.k.a.: na Address: na Listed on: 24 Mar. 2007 (amended on 17 Dec. 2014) Other Information: Controls 7th of Tir, which is designated under resolution 1737 (2006) for its role in Iran's centrifuge programme. AMIG is in turn owned and controlled by DIO, which is designated under resolution 1737 (2006). [Old Reference # E.47.A.1]
- IRe.005 Name: ARMAMENT INDUSTRIES GROUP (AIG)
A.k.a.: na F.k.a.: na Address: a) Sepah Islam Road, Karaj Special Road Km 10, Iran b) Pasdaran Ave., Tehran, Iran c) P.O. Box 19585/777 , Tehran, Iran Listed on: 9 Jun. 2010 (amended on 17 Dec. 2014) Other Information: Manufacturers and services a variety of small arms and light weapons, including large- and medium- calibre guns and related technology. AIG conducts the majority of its procurement activity through Hadid Industries Complex. [Old Reference # E.29.I.2]
- IRe.006 Name: ATOMIC ENERGY ORGANISATION OF IRAN (AEOI)
A.k.a.: na F.k.a.: na Address: na Listed on: 23 Dec. 2006 Other Information: [Old Reference # E.37.A.1]
- IRe.007 Name: BANK SEPAH AND BANK SEPAH INTERNATIONAL
A.k.a.: na F.k.a.: na Address: na Listed on: 24 Mar. 2007 Other Information: Bank Sepah provides support for the Aerospace Industries Organisation (AIO) and subordinates, including Shahid Hemmat Industrial Group (SHIG) and Shahid Bagheri Industrial Group (SBIG), both of which were designated under resolution 1737 (2006). [Old Reference # E.47.A.8]
- IRe.008 Name: BARZAGANI TEJARAT TAVANMAD SACCAL COMPANIES A.k.a.: na F.k.a.: na Address: na Listed on: 3 Mar. 2008 Other Information: A subsidiary of Saccal System companies, this company tried to purchase sensitive goods for an entity listed in resolution 1737 (2006). [Old Reference # E.03.III.2]
- IRe.009 Name: BEHINEH TRADING CO.
A.k.a.: na F.k.a.: na Address: Tavakoli Building, Opposite of 15th Alley, Emam-Jomeh Street, Tehran, Iran Listed on: 18 Apr. 2012 Other Information: An Iranian company that played a key role in Iran's illicit transfer of arms to West Africa and acted on behalf of the IRGC Qods Force, commanded by Major General Qasem Soleimani, designated by the UN Security Council in resolution 1747 (2007), as the shipper of the weapons consignment. (Additional Information: Telephone: 98-919-538-2305; Website: <http://www.behinehco.ir>) [Old Reference # E.AC.50.18.04.12]
- IRe.010 Name: CRUISE MISSILE INDUSTRY GROUP
A.k.a.: Naval Defence Missile Industry Group F.k.a.: na Address: na Listed on: 24 Mar. 2007 Other Information: Production and development of cruise missiles. Responsible for naval missiles including cruise missiles. [Old Reference # E.47.A.7]
- IRe.011 Name: DEFENCE INDUSTRIES ORGANISATION (DIO)
A.k.a.: na F.k.a.: na Address: na Listed on: 23 Dec. 2006 Other Information: Overarching MODAFLcontrolled entity, some of whose subordinates have been involved in the centrifuge programme making components, and in the missile programme. [Old Reference # E.37.A.6]
- IRe.012 Name: DEFENSE TECHNOLOGY AND SCIENCE RESEARCH CENTER (DTSRC)
A.k.a.: na F.k.a.: na Address: Pasdaran Av., PO Box 19585/777, Tehran, Iran Listed on: 9 Jun. 2010 (amended on 17 Dec. 2014) Other Information: Owned or controlled by, or acts on behalf of, MODAFL, which oversees Iran's defence research and development, production, maintenance, exports and procurement. [Old Reference # E.29.I.3]
- IRe.013 Name: DOOSTAN INTERNATIONAL COMPANY (DICO)
A.k.a.: na F.k.a.: na Address: na Listed on: 9 Jun. 2010 (amended on 17 Dec. 2014) Other Information: Supplies elements to Iran's ballistic missile programme. [Old Reference # E.29.I.4]
- IRe.014 Name: ELECTRO SANAM COMPANY
A.k.a.: a) E. S. Co. b) E. X. Co. F.k.a.: na Address: na Listed on: 3 Mar. 2008 Other Information: AIO front- company, involved in the ballistic missile programme. [Old Reference # E.03.III.3]

- IRe.015 Name: ESFAHAN NUCLEAR FUEL RESEARCH AND PRODUCTION CENTRE (NFRPC)
AND ESFAHAN NUCLEAR TECHNOLOGY CENTRE (ENTC) A.k.a.: na F.k.a.: na Address: na Listed on: 24 Mar. 2007 Other Information: Parts of the Atomic Energy Organisation of Iran's (AEOI) Nuclear Fuel Production and Procurement Company, which is involved in enrichment- related activities. AEOI is designated under resolution 1737 (2006). [Old Reference # E.47.A.2]
- IRe.016 Name: ETTEHAD TECHNICAL GROUP
A.k.a.: na F.k.a.: na Address: na Listed on: 3 Mar. 2008 Other Information: AIO front-company, involved in the ballistic missile programme. [Old Reference # E.03.III.4]
- IRe.017 Name: FAJR INDUSTRIAL GROUP
A.k.a.: na F.k.a.: Instrumentation Factory Plant Address: na Listed on: 23 Dec. 2006 Other Information: Subordinate entity of AIO. [Old Reference # E.37.B.3]
- IRe.018 Name: FARASAKHT INDUSTRIES
A.k.a.: na F.k.a.: na Address: P.O. Box 83145-311, Kilometer 28, Esfahan-Tehran Freeway, Shahin Shahr, Esfahan, Iran Listed on: 9 Jun. 2010 Other Information: Owned or controlled by, or acts on behalf of, the Iran Aircraft Manufacturing Company, which in turn is owned or controlled by MODAFL. [Old Reference # E.29.I.5]
- IRe.019 Name: FARAYAND TECHNIQUE
A.k.a.: na F.k.a.: na Address: na Listed on: 23 Dec. 2006 Other Information: Involved in centrifuge programme, identified in IAEA reports. [Old Reference # E.37.A.5]
- IRe.020 Name: FATER INSTITUTE
A.k.a.: Faater Institute F.k.a.: na Address: na Listed on: 9 Jun. 2010 Other Information: Khatam alAnbiya (KAA) subsidiary. Fater has worked with foreign suppliers, likely on behalf of other KAA companies on IRGC projects in Iran. [Old Reference # E.29.II.1]
- IRe.021 Name: FIRST EAST EXPORT BANK, P.L.C.
A.k.a.: na F.k.a.: na Address: Unit Level 10 (B1), Main Office Tower, Financial Park Labuan, Jalan Merdeka, 87000 WP, Labuan, Malaysia Listed on: 9 Jun. 2010 Other Information: Owned or controlled by, or acts on behalf of, Bank Mellat. Bank Mellat has facilitated hundreds of millions of dollars in transactions for Iranian nuclear, missile, and defense entities. (Additional information: Business Registration Number LL06889 (Malaysia)) [Old Reference # E.29.I.6]
- IRe.022 Name: GHARAGAHE SAZANDEGI GHAEM
A.k.a.: na F.k.a.: na Address: na Listed on: 9 Jun. 2010 Other Information: Owned or controlled by KAA. [Old Reference # E.29.II.2]
- IRe.023 Name: GHORB KARBALA
A.k.a.: na F.k.a.: na Address: na Listed on: 9 Jun. 2010 Other Information: Owned or controlled by KAA. [Old Reference # E.29.II.3]
- IRe.024 Name: GHORB NOOH
A.k.a.: na F.k.a.: na Address: na Listed on: 9 Jun. 2010 Other Information: Owned or controlled by KAA. [Old Reference # E.29.II.4]
- IRe.025 Name: HARA COMPANY
A.k.a.: na F.k.a.: na Address: na Listed on: 9 Jun. 2010 Other Information: Owned or controlled by Ghorb Nooh. [Old Reference # E.29.II.5]
- IRe.026 Name: IMENSAZAN CONSULTANT ENGINEERS INSTITUTE
A.k.a.: na F.k.a.: na Address: na Listed on: 9 Jun. 2010 Other Information: Owned or controlled by, or acts on behalf of, KAA. [Old Reference # E.29.II.6]
- IRe.027 Name: INDUSTRIAL FACTORIES OF PRECISION (IFP) MACHINERY
A.k.a.: Instrumentation Factories Plant F.k.a.: na Address: na Listed on: 3 Mar. 2008 Other Information: Used by AIO for some acquisition attempts. [Old Reference # E.03.III.5]
- IRe.028 Name: IRANO HIND SHIPPING COMPANY
A.k.a.: na F.k.a.: na Address: a) 18 Mehrshad Street, Sadaghat Street, Opposite of Park Mellat, ValieAsr Ave., Tehran, Iran b) 265, Next to Mehrshad, Sedaghat St., Opposite of Mellat Park, Vali Asr Ave., Tehran, 1A001, Iran Listed on: 9 Jun. 2010 Other Information: [Old Reference # E.29.III.1]
- IRe.029 Name: IRISL BENELUX NV
A.k.a.: na F.k.a.: na Address: Noorderlaan 139, B-2030, Antwerp, Belgium Listed on: 9 Jun. 2010 Other Information: Additional information: VAT Number BE480224531 [Old Reference # E.29.III.2]
- IRe.030 Name: JABBER IBN HAYAN
A.k.a.: na F.k.a.: na Address: na Listed on: 3 Mar. 2008 Other Information: AEOI laboratory involved in fuel- cycle activities. [Old Reference # E.03.III.6]
- IRe.031 Name: JOZA INDUSTRIAL CO.
A.k.a.: na F.k.a.: na Address: na Listed on: 3 Mar. 2008 Other Information: AIO front-company, involved in the ballistic missile programme. [Old Reference # E.03.III.7]
- IRe.032 Name: KALA-ELECTRIC
A.k.a.: Kalaye Electric F.k.a.: na Address: na Listed on: 23 Dec. 2006 Other Information: Provider for PFEP - Natanz. [Old Reference # E.37.A.3]

- IRe.033 Name: KARAJ NUCLEAR RESEARCH CENTRE
A.k.a.: na F.k.a.: na Address: na Listed on: 24 Mar. 2007 Other Information: Part of AEOI's research division. [Old Reference # E.47.A.5]
- IRe.034 Name: KAVEH CUTTING TOOLS COMPANY
A.k.a.: na F.k.a.: na Address: a) 3rd Km of Khalaj Road, Seyyedi Street, Mashad, 91638, Iran b) Km 4 of Khalaj Road, End of Seyyedi Street, Mashad, Iran c) P.O. Box 91735-549, Mashad, Iran d) Khalaj Rd., End of Seyyedi Alley, Mashad, Iran e) Moqan St., Pasdaran St., Pasdaran Cross Rd., Tehran, Iran Listed on: 9 Jun. 2010 Other Information: Owned or controlled by, or acts on behalf of, DIO. [Old Reference # E.29.I.7]
- IRe.035 Name: KAVOSHYAR COMPANY
A.k.a.: na F.k.a.: na Address: na Listed on: 24 Mar. 2007 Other Information: Subsidiary company of AEOI which has sought glass fibres, vacuum chamber furnaces and laboratory equipment for Iran's nuclear programme. [Old Reference # E.47.A.3]
- IRe.036 Name: KHATAMAL-ANBIYA CONSTRUCTION HEADQUARTERS (KAA)
A.k.a.: na F.k.a.: na Address: na Listed on: 9 Jun. 2010 (amended on 17 Dec. 2014) Other Information: KAA is an IRGC-owned company involved in large scale civil and military construction projects and other engineering activities. It undertakes a significant amount of work on Passive Defense Organization projects. In particular, KAA subsidiaries were heavily involved in the construction of the uranium enrichment site at Qom/Fordow. [Old Reference # E.29.II.7]
- IRe.037 Name: KHORASAN METALLURGY INDUSTRIES
A.k.a.: na F.k.a.: na Address: na Listed on: 3 Mar. 2008 Other Information: Subsidiary of AMIG which depends on DIO. Involved in the production of centrifuges components. [Old Reference # E.03.III.8]
- IRe.038 Name: M. BABAIE INDUSTRIES
A.k.a.: na F.k.a.: na Address: P.O. Box 16535-76, Tehran, 16548, Iran Listed on: 9 Jun. 2010 Other Information: Subordinate to Shahid Ahmad Kazemi Industries Group (formally the Air Defense Missile Industries Group) of Iran's Aerospace Industries Organization (AIO). AIO controls the missile organizations Shahid Hemmat Industrial Group (SHIG) and the Shahid Bakeri Industrial Group (SBIG), both of which were designated in resolution 1737 (2006). [Old Reference # E.29.I.8]
- IRe.039 Name: MAKIN
A.k.a.: na F.k.a.: na Address: na Listed on: 9 Jun. 2010 Other Information: Owned or controlled by or acting on behalf of KAA, and is a subsidiary of KAA. [Old Reference # E.29.II.8]
- IRe.040 Name: MALEK ASHTAR UNIVERSITY
A.k.a.: na F.k.a.: na Address: Corner of Imam Ali Highway and Babaei Highway, Tehran, Iran Listed on: 9 Jun. 2010 Other Information: Subordinate of the DTRSC within MODAFL. This includes research groups previously falling under the Physics Research Center (PHRC). IAEA inspectors have not been allowed to interview staff or see documents under the control of this organization to resolve the outstanding issue of the possible military dimension to Iran's nuclear programme. [Old Reference # E.29.I.9]
- IRe.041 Name: MESBAH ENERGY COMPANY
A.k.a.: na F.k.a.: na Address: na Listed on: 23 Dec. 2006 Other Information: Provider for A-40 research reactor, Arak. [Old Reference # E.37.A.2]
- IRe.042 Name: MINISTRY OF DEFENSE LOGISTICS EXPORT
A.k.a.: MODLEX F.k.a.: na Address: a) P.O. Box 16315-189, Tehran, Iran b) Located on the west side of Dabestan Street, Abbas Abad District, Tehran, Iran Listed on: 9 Jun. 2010 Other Information: MODLEX sells Iranian-produced arms to customers around the world in contravention of resolution 1747 (2007), which prohibits Iran from selling arms or related materiel. [Old Reference # E.29.I.10]
- IRe.043 Name: MIZAN MACHINERY MANUFACTURING
A.k.a.: 3MG F.k.a.: na Address: P.O. Box 16595-365, Tehran, Iran Listed on: 9 Jun. 2010 Other Information: Owned or controlled by, or acts on behalf of, SHIG. [Old Reference # E.29.I.11]
- IRe.044 Name: MODERN INDUSTRIES TECHNIQUE COMPANY (MITEC)
A.k.a.: a) MITEC b) Rahkar Company c) Rahkar Industries d) Rahkar Sanaye Company e) Rahkar Sanaye Novin F.k.a.: na Address: Arak, Iran Listed on: 9 Jun. 2010 (amended on 17 Dec. 2014) Other Information: MITEC is responsible for design and construction of the IR-40 heavy water reactor in Arak. MITEC has spearheaded procurement for the construction of the IR-40 heavy water reactor. [Old Reference # E.29.I.12]
- IRe.045 Name: NIRU BATTERY MANUFACTURING COMPANY
A.k.a.: na F.k.a.: na Address: na Listed on: 3 Mar. 2008 Other Information: Subsidiary of DIO. Its role is to manufacture power units for the Iranian military including missile systems. [Old Reference # E.03.III.9]
- IRe.046 Name: NOVIN ENERGY COMPANY
A.k.a.: Pars Novin F.k.a.: na Address: na Listed on: 24 Mar. 2007 Other Information: Operates within AEOI and has transferred funds on behalf of AEOI to entities associated with Iran's nuclear programme. [Old Reference # E.47.A.6]
- IRe.047 Name: NUCLEAR RESEARCH CENTER FOR AGRICULTURE AND MEDICINE (NFRPC)
A.k.a.: a) Center for Agricultural Research and Nuclear Medicine b) Karaji Agricultural and Medical Research Center F.k.a.: na Address: P.O. Box 31585-4395, Karaj, Iran Listed on: 9 Jun. 2010 (amended on 17 Dec. 2014) Other Information: NFRPC is a large research component of AEOI, which was designated in resolution 1737 (2006). The NFRPC is AEOI's center for the development of nuclear fuel and is involved in enrichment-related activities. [Old Reference # E.29.I.13]
- IRe. 048 Name: OMRAN SAHEL
A.k.a.: na F.k.a.: na Address: na Listed on: 9 Jun. 2010 Other Information: Owned or controlled by Ghorb Nooh. [Old Reference # E.29.II.9]

- IRe.049 Name: ORIENTAL OIL KISH
A.k.a.: na F.k.a.: na Address: na Listed on: 9 Jun. 2010 Other Information: Owned or controlled by, or acts on behalf of, KAA. [Old Reference # E.29.II.10]
- IRe.050 Name: PARCHIN CHEMICAL INDUSTRIES
A.k.a.: na F.k.a.: na Address: na Listed on: 24 Mar. 2007 Other Information: Branch of DIO, which produces ammunition, explosives, as well as solid propellants for rockets and missiles. [Old Reference # E.47.A.4]
- IRe.051 Name: PARS AVIATION SERVICES COMPANY
A.k.a.: na F.k.a.: na Address: na Listed on: 24 Mar. 2007 Other Information: Maintains various aircraft, including MI-171, used by IRGC Air Force. [Old Reference # E.47.B.2]
- IRe.052 Name: PARS TRASH COMPANY
A.k.a.: na F.k.a.: na Address: na Listed on: 23 Dec. 2006 Other Information: Involved in centrifuge programme, identified in IAEA reports. [Old Reference # E.37.A.4]
- IRe.053 Name: PEJMAN INDUSTRIAL SERVICES CORPORATION
A.k.a.: na F.k.a.: na Address: P.O. Box 16785-195, Tehran, Iran Listed on: 9 Jun. 2010 Other Information: Owned or controlled by, or acts on behalf of, SBIG [Old Reference # E.29.I.14]
- IRe.054 Name: PISHGAM ENERGY INDUSTRIES
A.k.a.: Pioneer Energy Industries F.k.a.: na Address: na Listed on: 3 Mar. 2008 Other Information: Participated in the construction of the Uranium Conversion Facility at Esfahan. [Old Reference #E.03.III.10]
- IRe.055 Name: QODS AERONAUTICS INDUSTRIES
A.k.a.: na F.k.a.: na Address: na Listed on: 24 Mar. 2007 Other Information: Produces unmanned aerial vehicles (UAVs), parachutes, para-gliders, para-motors, etc. IRGC has boasted of using these products as part of its asymmetric warfare doctrine. [Old Reference # E.47.B.1]
- IRe.056 Name: RAH SAHEL
A.k.a.: na F.k.a.: na Address: na Listed on: 9 Jun. 2010 Other Information: Owned or controlled by, or acting on behalf of, KAA. [Old Reference # E.29.II.11]
- IRe.057 Name: RAHAB ENGINEERING INSTITUTE
A.k.a.: na F.k.a.: na Address: na Listed on: 9 Jun. 2010 Other Information: Owned or controlled by, or acting on behalf of, KAA and is a subsidiary of KAA. [Old Reference # E.29.II.12]
- IRe.058 Name: SABALAN COMPANY
A.k.a.: na F.k.a.: na Address: Damavand Tehran Highway, Tehran, Iran Listed on: 9 Jun. 2010 Other Information: Sabalan is a cover name for SHIG. [Old Reference # E.29.I.15]
- IRe.059 Name: SAD IMPORT EXPORT COMPANY
A.k.a.: na F.k.a.: na Address: a) Haftom Tir Square, South Mofte Avenue, Tour Line No 3/1, Tehran, Iran b) P.O. Box 1584864813, Tehran, Iran Listed on: 20 Dec. 2012 (amended on 17 Dec. 2014) Other Information: Assisted Parchin Chemical Industries and 7th of Tir Industries, designated in resolutions 1747 (2007) and 1737 (2006), in violating paragraph 5 of resolution 1747 (2007). [Old Reference # I.AC.50.20.12.12.(2)]
- IRe.060 Name: SAFETY EQUIPMENT PROCUREMENT (SEP)
A.k.a.: na F.k.a.: na Address: na Listed on: 3 Mar. 2008 Other Information: AIO front-company, involved in the ballistic missile programme. [Old Reference # E.03.III.11]
- IRe.061 Name: SAHAND ALUMINUM PARTS INDUSTRIAL COMPANY (SAPICO)
A.k.a.: na F.k.a.: na Address: Damavand Tehran Highway, Tehran, Iran Listed on: 9 Jun. 2010 Other Information: SAPICO is a cover name for SHIG. [Old Reference # E.29.I.16]
- IRe.062 Name: SAHEL CONSULTANT ENGINEERS
A.k.a.: na F.k.a.: na Address: na Listed on: 9 Jun. 2010 Other Information: Owned or controlled by Ghorb Nooh. [Old Reference # E.29.II.13]
- IRe.063 Name: SANAM INDUSTRIAL GROUP
A.k.a.: na F.k.a.: na Address: na Listed on: 24 Mar. 2007 Other Information: Subordinate to AIO, which has purchased equipment on AIO's behalf for the missile programme. [Old Reference # E.47.A.9]
- IRe.064 Name: SEPANIR
A.k.a.: na F.k.a.: na Address: na Listed on: 9 Jun. 2010 Other Information: Owned or controlled by, or acting on behalf of, KAA. [Old Reference # E.29.II.14]
- IRe.065 Name: SEPASAD ENGINEERING COMPANY
A.k.a.: na F.k.a.: na Address: na Listed on: 9 Jun. 2010 Other Information: Owned or controlled by, or acting on behalf of, KAA. [Old Reference # E.29.II.15]
- IRe.066 Name: SHAHID BAGHERI INDUSTRIAL GROUP (SBIG)
A.k.a.: na F.k.a.: na Address: na Listed on: 23 Dec. 2006 Other Information: Subordinate entity of AIO. [Old Reference # E.37.B.2]
- IRe.067 Name: SHAHID HEMMAT INDUSTRIAL GROUP (SHIG)
A.k.a.: na F.k.a.: na Address: na Listed on: 23 Dec. 2006 Other Information: Subordinate entity of AIO. [Old Reference # E.37.B.1]
- IRe.068 Name: SHAHID KARRAZI INDUSTRIES
A.k.a.: na F.k.a.: na Address: Tehran, Iran Listed on: 9 Jun. 2010 Other Information: Owned or controlled by, or acts on behalf of, SBIG [Old Reference # E.29.I.17]

- IRe.069 Name: SHAHID SATTARI INDUSTRIES
A.k.a.: Shahid Sattari Group Equipment Industries F.k.a.: na Address: Southeast Tehran, Iran Listed on: 9 Jun. 2010 Other Information: Owned or controlled by, or acts on behalf of, SBIG. [Old Reference # E.29.I.18]
- IRe.070 Name: SHAHID SAYYADE SHIRAZI INDUSTRIES (SSSI)
A.k.a.: na F.k.a.: na Address: a) Next To Nirou Battery Mfg. Co, Shahid Babaii Expressway, Nobonyad Square, Tehran, Iran b) Pasdaran St., P.O. Box 16765, Tehran, 1835, Iran c) Babaei Highway - Next to Niru M.F.G, Tehran, Iran Listed on: 9 Jun. 2010 Other Information: SSSI is owned or controlled by, or acts on behalf of, DIO. [Old Reference # E.29.I.19]
- IRe.071 Name: SHO'A' AVIATION
A.k.a.: na F.k.a.: na Address: na Listed on: 24 Mar. 2007 Other Information: Produces micro-lights which IRGC has claimed it is using as part of its asymmetric warfare doctrine. [Old Reference # E.47.B.3]
- IRe.072 Name: SOUTH SHIPPING LINE IRAN (SSL)
A.k.a.: na F.k.a.: na Address: a) Qaem Magham Farahani St., Tehran, Iran b) Apt. No. 7, 3rd Floor, No. 2, 4th Alley, Gandhi Ave., Tehran, Iran Listed on: 9 Jun. 2010 Other Information: [Old Reference # E.29.III.3]
- IRe.073 Name: SPECIAL INDUSTRIES GROUP (SIG)
A.k.a.: na F.k.a.: na Address: Pasdaran Avenue, PO Box 19585/777, Tehran, Iran Listed on: 9 Jun. 2010 Other Information: Subordinate of DIO. [Old Reference # E.29.I.20]
- IRe.074 Name: TAMAS COMPANY
A.k.a.: na F.k.a.: na Address: na Listed on: 3 Mar. 2008 Other Information: Involved in enrichmentrelated activities. TAMAS is the overarching body, under which four subsidiaries have been established, including one for uranium extraction to concentration and another in charge of uranium processing, enrichment and waste. [Old Reference # E.03.III.12]
- IRe.075 Name: TIZ PARS
A.k.a.: na F.k.a.: na Address: Damavand Tehran Highway, Tehran, Iran Listed on: 9 Jun. 2010 Other Information: Tiz Pars is a cover name for SHIG. Between April and July 2007, Tiz Pars attempted to procure a five axis laser welding and cutting machine, which could make a material contribution to Iran's missile programme, on behalf of SHIG. [Old Reference # E.29.I.21]
- IRe.076 Name: YAMAHD I INDUSTRIES GROUP
A.k.a.: na F.k.a.: na Address: na Listed on: 24 Mar. 2007 Other Information: Subordinate to AIO, which is involved in international purchases of missile equipment. [Old Reference # E.47.A.10]
- IRe.077 Name: YAS AIR
A.k.a.: na F.k.a.: na Address: Mehrabad International Airport, Next to Terminal No. 6, Tehran, Iran Listed on: 20 Dec. 2012 Other Information: Yas Air is the new name for Pars Air, a company that was owned by Pars Aviation Services Company, which in turn was designated by the United Nations Security Council in resolution 1747 (2007). Yas Air has assisted Pars Aviation Services Company, a United Nations-designated entity, in violating paragraph 5 of resolution 1747 (2007). [Old Reference # I.AC.50.20.12.12.(1)]
- IRe.078 Name: YAZD METALLURGY INDUSTRIES (YMI)
A.k.a.: a) Yazd Ammunition Manufacturing and Metallurgy Industries b) Directorate of Yazd Ammunition and Metallurgy Industries F.k.a.: na Address: a) Pasdaran Avenue, next to Telecommunication Industry, Tehran, 16588, Iran b) Postal Box 89195/878, Yazd, Iran c) P.O. Box 89195-678, Yazd, Iran d) Km 5 of Taft Road, Yazd, Iran Listed on: 9 Jun. 2010 Other Information: YMI is a subordinate of DIO. [Old Reference #E.29.I.22].

The updated version of the Committee’s Sanctions List, available in HTML, PDF and XML format, may be found at the following URL:

<https://main.un.org/securitycouncil/en/sanctions/1737/materials>.

The United Nations Security Council Consolidated List is also updated following all changes made to the Committee’s Sanctions List and is accessible at the following URL:

<https://main.un.org/securitycouncil/content/un-sc-consolidated-list>.

The Secretariat of the United Nations avails itself of this opportunity to renew to the Permanent Representatives of Member States and Permanent Observers of non-Member States to the United Nations the assurances of its highest consideration.

Dated this 14th day of June, 2026.

DR. HORACE CHANG
Minister of National Security and Peace.

KAMINA JOHNSON SMITH
Minister of Foreign Affairs and Foreign Trade.