



RMI ME2

# Mutual Evaluation Report

Anti-Money Laundering and Combating the  
Financing of Terrorism

# Republic of the Marshall Islands

July 2011

The Republic of the Marshall Islands (RMI) is a member of the Asia Pacific Group on Money Laundering (APG). This evaluation was conducted by the APG and was adopted as a 2nd mutual evaluation by its Plenary on 20 July 2011.

2011 ASIA/PACIFIC GROUP ON MONEY LAUNDERING. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission. Requests for permission to further disseminate, reproduce or translate all or part of this publication should be obtained from the APG Secretariat, Locked Bag A3000, Sydney South, NSW 1232, Australia.  
(Telephone: +612 9277 0600 Fax: +612 9277 0606 Email: [mail@apgml.org](mailto:mail@apgml.org))

Contents	Page
Acronyms .....	5
Executive Summary .....	7
1. GENERAL .....	17
1.1. General Information on Republic of the Marshall Islands .....	17
1.2. General Situation of Money Laundering and Financing of Terrorism .....	19
1.3. Overview of the Financial Sector and DNFBP .....	20
1.4. Overview of the DNFBP Sector .....	24
1.5. Overview of commercial laws and mechanisms governing legal persons and arrangements .....	25
1.6. Overview of strategy to prevent money laundering and terrorist financing .....	26
2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES .....	30
2.1 Criminalization of Money Laundering (R.1 & 2) .....	30
2.2. Criminalization of Terrorist Financing (SR.II) .....	37
2.3. Confiscation, freezing and seizing of proceeds of crime (R.3) .....	42
2.4. Freezing of funds used for terrorist financing (SR.III) .....	48
2.5. The Financial Intelligence Unit and its Functions (R.26) .....	52
2.6. Law enforcement, prosecution and other competent authorities—the framework for the investigation and prosecution of offences, and for confiscation and freezing (R.27, & 28) .....	61
2.7. Cross Border Declaration or Disclosure (SR.IX) .....	67
3. PREVENTIVE MEASURES —FINANCIAL INSTITUTIONS .....	75
3.1. Risk of money laundering or terrorist financing .....	75
3.2. Customer due diligence, including enhanced or reduced measures (R.5 to 8) .....	77
3.3. Third Parties and Introduced Business (R.9) .....	89
3.4. Financial Institution Secrecy or Confidentiality (R.4) .....	90
3.5. Record keeping and wire transfer rules (R.10 & SR.VII) .....	91
3.6. Monitoring of Transactions and Relationships (R.11 & 21) .....	96
3.7. Suspicious Transaction Reports and Other Reporting (R.13-14, 19, 25 & SR.IV) .....	98
3.8. Internal Controls, Compliance, Audit and Foreign Branches (R.15 & 22) .....	103
3.9. Shell Banks (R.18) .....	105
3.10. The Supervisory and Oversight System - Competent Authorities and SROs: Role, Functions, Duties and Powers (Including Sanctions) (R.23, 30, 29, 17, 32 & 25) ..	106
3.11. Money or Value Transfer Services (SR.VI) .....	116
4. PREVENTIVE MEASURES—DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS .....	119
4.1. Customer Due Diligence and Record-keeping (R.12) .....	119
4.2. Monitoring Transactions and other Issues (R.16) .....	119
4.3. Regulation, Supervision, and Monitoring (R.24-25) .....	120
4.4. Other Non-Financial Businesses and Professions—Modern-Secure Transaction Techniques (R.20) .....	121
5. LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANIZATIONS .....	123
5.1 Legal Persons – Access to beneficial ownership and control information (R. 33) ..	123
5.2. Legal Arrangements—Access to Beneficial Ownership and Control Information (R.34) .....	128

5.3.	Non-Profit Organizations (SR.VIII).....	129
6.	NATIONAL AND INTERNATIONAL CO-OPERATION .....	134
6.3.	Mutual Legal Assistance (R.36-38, SR.V) .....	136
6.4.	Extradition (R.37, 39, SR.V) .....	144
6.5.	Other Forms of International Co-Operation (R.40 & SR.V) .....	146
7.	OTHER ISSUES.....	150
7.1.	Resources and Statistics .....	150
7.2.	Other relevant AML/CFT Measures or Issues.....	150

## **TABLES**

1.	Ratings of Compliance with FATF Recommendations.....	152
2.	Recommended Action Plan to Improve the AML/CFT System .....	158

## **ANNEXES**

Annex 1.	Authorities' Response to the Assessment.....	168
Annex 2.	Details of All Bodies Met During the On-Site Visit .....	170
Annex 3.	List of All Laws, Regulations, and Other Material Received .....	171
Annex 4.	Copies of Key Laws, Regulations, and Other Measures .....	172

## Acronyms

AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
BA	Banking Act
BCA	Business Corporation Act
BC	Banking Commission
BOMI	Bank of Marshall Islands
BOG	Bank of Guam
CDA	Currency Declaration Act
CDD	Customer Due Diligence
CP	Commissioner of Police
CPC	Criminal Procedure Code
CSP	Company Service Provider
CTA	Counter Terrorism Act 2002
DFIU	Domestic Financial Intelligence Unit
DNFBP	Designated Non-Financial Businesses and Professions
DPS	Department of Public Safety
FATF	Financial Action Task Force
FI	Financial institution
FIU	Financial Intelligence Unit
FSAP	Financial Sector Assessment Program
FSRB	FATF-style Regional Body
FT	Financing of terrorism
IAIS	International Association of Insurance Supervisors
IRI	International Registries Incorporated
KYC	Know your customer/client
MIDB	Marshall Island Development Bank
MOFA	Ministry of Foreign Affairs
MOF	Ministry of Finance
MOU	Memorandum of Understanding
MICNGOS	Marshall Islands Council of NGOs
ML	Money laundering
MLA	Mutual legal assistance
NPO	Nonprofit organization
OAG	Office of Attorney General
PEP	Politically-exposed person
POCA	Proceeds of Crime Act
RMI	Republic of Marshall Island
ROC	Registrar of Corporations
SRO	Self-regulatory organization
STR	Suspicious Transaction Report
TCMI	Trust Company of the Marshall Island
UNSCR	United Nations Security Council Resolution

## **PREFACE - Information and methodology used for the evaluation of the Republic of the Marshall Islands (RMI)**

1. The evaluation of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of the Republic of the Marshall Islands (hereinafter “RMI”) was based on the Forty Recommendations 2003 and the Nine Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), and was prepared using the AML/CFT Methodology 2004. The evaluation was based on the laws, regulations and other materials supplied by the RMI and information obtained by the assessment team during its on-site visit to the RMI from 6 to 17 September 2010, and subsequently. During the on-site visit the assessment team met with officials and representatives of all relevant RMI government agencies and the private sector. A list of the bodies met is set out in Annex 2 to the mutual evaluation report.

2. The evaluation was conducted by a team of assessors composed of APG experts in criminal law, law enforcement and regulatory issues. The assessment team consisted of:

### **Legal expert**

- Arnold Frane, Bank Officer V of the Anti-Money Laundering Council (AMLC) Secretariat of the Philippines

### **Financial experts**

- Peter Dench, Advisor, Prudential Supervision Department, Reserve Bank of New Zealand
- Gunagand Semdiu Decherong, Executive Commissioner, Republic of Palau Financial Institutions Commission

### **Law enforcement expert**

- Gai Lambourne, Technical Advisor, Australian Transaction Reports and Analysis Centre (AUSTRAC)

### **APG Secretariat**

- Lindsay Chan, Principal Executive Officer

3. The experts reviewed the institutional framework, the relevant AML/CFT laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter money laundering (ML) and the financing of terrorism (FT) through financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs), as well as examining the capacity, the implementation and the effectiveness of all these systems.

4. This report provides a summary of the AML/CFT measures in place in the RMI as at the date of the on-site visit or immediately thereafter. It describes and analyses those measures, sets out RMI’s levels of compliance with the FATF 40+9 Recommendations (see Table 1), and provides recommendations on how certain aspects of the system could be strengthened (see Table 2).

## Executive Summary

### Key Findings

1. **The RMI has a very limited financial sector with total banking sector assets estimated at US\$133 million in May 2010.** There are two AML/CFT supervised commercial banks that dominate the financial sector in the RMI. Financial institutions and cash dealers are regulated for AML/CFT except for a few informal providers.
2. **Money laundering (ML) and financing of terrorism (FT) vulnerabilities in the RMI derive mainly from its offshore company registration sector.** The corporate anonymity afforded by companies registered in the RMI represents significant ML/FT vulnerabilities. There is no mandatory requirement for legal persons to provide information either on the legal or beneficial ownership of shareholders, and there is no supervision of company formation service providers based offshore.
3. **The Banking Commission is the lead agency for AML/CFT in the RMI.** The *Banking Act* provides a range of statutory powers to the Banking Commissioner, including those of a financial intelligence unit (FIU), as a prudential regulator of licensed banks, and as an AML/CFT supervisor of financial institutions and cash dealers.
4. **Overall, the RMI has implemented reasonably sound measures concerning ML/FT criminalization, confiscation and international co-operation, and the preventive measures for the financial sectors, but technical and implementation deficiencies remain.** There are deficiencies in the following: elements of the ML and FT offences; mechanisms for freezing FT funds without delay and domestic designation; controls on movement of cash across borders; supervision of non-bank financial institutions and cash dealers; and implementation of the FATF standards amongst the designated non-financial businesses and professions (DNFBPs), in particular company service providers.
5. **There has been no prosecution or conviction for ML and FT.** Opportunities for possible ML prosecution were not pursued either due to lack of resources or expertise, and the view (by some authorities) that ML is more of an international rather than a domestic concern. The authorities consider terrorism and FT as very low risk, and there has never been a case of either event.
6. **The main DNFBP sector is the offshore company formation services sector which is not yet included in the AML/CFT regime.** Accountants, lawyers and other company service providers based in foreign jurisdictions submit applications for company formations to the RMI's offshore company registry.
7. **Key recommendations made to the RMI include:**
  - address remaining legal deficiencies in the ML and FT offences;
  - use available powers to investigate and prosecute the ML offence;
  - provide mechanisms/procedures for freezing terrorist property without delay and for domestic designation;
  - undertake further enhancements to DFIU functions;
  - rectify deficiencies in the *Currency Declaration Act 2009*;
  - take further steps to ensure all entities are aware of their obligations under the revised *AML/CFT Regulations*;

- undertake supervision (on and off-site) to confirm implementation;
- rectify technical deficiencies in the revised *AML/CFT Regulations*;
- introduce AML/CFT requirements for DNFBPs with a focus on enhancing supervision of company formation service providers based offshore;
- amend relevant statutes to include mandatory information on beneficial ownership and to prevent the misuse of bearer shares; and
- address remaining deficiencies in the MLA framework.

### Legal Systems and Related Institutional Measures

8. ML is criminalized under the *Banking Act* of 1987, although the latter has yet to be used for any criminal prosecution or criminal charges. Two ML investigations were undertaken, but no ML charges resulted from these cases. Statistics show that certain serious (predicate) offenses were investigated and prosecuted by law enforcement authorities that could have led to ML investigations and possible prosecution. The assessment team has observed that related ML investigations of these predicate offences often stop once the conviction for the predicate offence has been secured. Moreover, the agency charged with prosecution of offences, the Office of the Attorney General (OAG), has a limited number of personnel and most are fairly new. This may account for the lack of ML prosecutions. Another factor may stem from the view by some authorities that ML is a transnational crime rather than a domestic concern.

9. The definition of ML under the *Banking Act* is not fully in accord with the Vienna and Palermo Conventions. Not all of the 20 designated categories of predicate offences are currently covered by the term “serious offence” and included as predicate offences to ML. There are no provisions criminalizing piracy of products, human trafficking and migrant smuggling, insider trading and market manipulation. Some of the offences considered as environmental crimes are limited in scope and would not qualify as a serious offence because of the penalties imposed are either civil in nature or involve imprisonment of less than a year.

10. FT is criminalized under section 120 of the *Counter-Terrorism Act*, 2002 (“CTA”). The CTA’s definition of FT substantially follows Article 2 of the FT Convention. The CTA does not cover “attempts” to commit FT as required under the standard. The RMI has neither conducted an investigation nor prosecution relating to FT. FT offences are predicate offences for ML since they fall under the definition of “serious offence” under the *Banking Act*.

11. RMI has a conviction based forfeiture regime under the *Banking Act*, CTA, and POCA. There are no provisions for the confiscation of assets of organized criminal groups. Moreover, it is uncertain whether the term “tainted property”, as defined under the *Banking Act* and POCA, covers instrumentalities intended for use in the commission of any ML, FT or other predicate offences, and property of corresponding value.

12. The CTA provides ample authority to freeze, seize and detain terrorist related funds, but is lacking a specific procedure to achieve freezing without delay. Further, the authority to freeze, seize and detain under section 122 (2) is limited to designated terrorist organizations. It is not clear that funds can be kept frozen beyond two years. There are no procedures for domestic designation, delisting and un-freezing pursuant to UNSCR 1373. There has been no instance where sections 122 and 108(3) have been utilized, as there has been no terrorism or FT-related investigation made as of the time of the on-site.

13. The powers of the Domestic Financial Intelligence Unit (DFIU) of the RMI are provided specifically in section 167, and more broadly in sections 170 and 180 of the Banking Commission Act. Cabinet Minute 236 by the Nitijela (Parliament), dated 21 November 2000, established the DFIU, comprising the Banking Commissioner as Head, the Commissioner of Police, the Chief of Revenue and Taxation Division and a representative from the OAG in a supportive role. The DFIU is an administrative FIU with no formal investigative role.
14. The DFIU is housed within the Banking Commission. Three Banking Commission staff perform DFIU functions together with AML/CFT and prudential supervision roles. All DFIU roles are conducted on a part-time basis, and as a result, the current staffing and technical resources of the DFIU are inadequate.
15. The DFIU has implemented standing operation procedures (SOPs) for overall DFIU operations, including for STR and CTR analysis. The STR SOP does not include referral to the UNSCR 1267 and other lists to assist in the prioritisation and analysis process.
16. In the period from 2005-2010, 19 STRs were disseminated to law enforcement out of a total of 211 STRs received. However, the sharing of information between the DFIU, law enforcement and Customs is carried out on an informal basis, where minimal or no records are maintained for statistical purposes.
17. The DFIU budget is part of the Banking Commission's budget; they are managed, however, independently from each other. At the time of the on-site visit, there was an indication the DFIU might acquire an independent budget in the future. A proposal for one dedicated staff member with the DFIU has been submitted. This is an outstanding issue from the previous MER.
18. The DFIU's effectiveness would be enhanced if it had dedicated staffing resources, a review of current SOPs to overcome some deficiencies in the processing of STRs, and the introduction of new SOPs to include a register to record accurately information requests for both audit and statistical purposes.
19. The Criminal Investigations Department (CID) of the Department of Public Safety (DPS) has been tasked with investigating ML, TF and predicate offences, and taking the lead investigation role in consultation with the Attorney General and the DFIU.
20. The Attorney General is the primary authority relating to the CTA, including the authority to prosecute under Section 104(4), and the authority to investigate, under Part III Section 113, and to direct the CID to investigate terrorist activities.
21. The CID has the authority to use special investigative techniques and undertake financial investigations for ML and FT. A lack of training and investigative skills has contributed to preventing these powers from being used.
22. The RMI has introduced *Proceeds of Crime* legislation. The legislation is silent on the search or production of warrant powers.
23. The CID's effectiveness would be enhanced with appropriate financial investigative techniques training to increase the level of understanding and knowledge of ML. This will provide the CID with the skills to investigate ML, proceeds of crime and taxation related matters.

24. The cross border declaration system was introduced by the Nitijela with the *Currency Declaration Act 2009* (CDA). The CDA was passed in May 2009 and came into effect in August 2009. The CDA contains a definition of “currency” that includes bearer negotiable instruments, precious metals and stones.

25. The declaration requirement of US\$10,000 or more under the CDA is applicable to inwards passengers only, and neither the definition of currency nor penalties for false declaration is included in the actual Customs Declaration Form. Further, the CDA does not specifically extend the declaration requirement to include the movement of currency through mail or containerized cargo.

26. The CDA provides Customs with the powers to request information on the origin and use of currency, and to seize and restrain currency, if there are reasonable grounds for suspecting the currency is intended for use in unlawful conduct.

27. Customs has a manual filing system for the cross border movement of currency and other customs related offences. However, there is no formal system for recording currency declaration in excess of US\$10,000, and there is no formal process for the sharing or transferring of information from the Customs to the DFIU. Information is on a case-by- case basis and in an informal manner, where minimal or no records are maintained for statistical or audit purposes.

28. At the time of the MER, consideration was being given to the creation and implementation of a Memorandum of Understanding (MOU) between Customs, the DFIU and law enforcement agencies on matters relating to ML and FT.

29. The RMI has introduced legislation and an inwards passenger declaration requirement since August 2009. Customs needs to undertake more work before the requirements set down in the CDA are met. The current declaration requirements should include outward declaration and currency sent through mail and containerized cargo, and an improved declaration form should be introduced to include the definition of currency and sanctions for false declaration.

### **Legal Persons and Arrangements & Non-Profit Organizations**

30. Regulations for legal persons are provided under the *Business Corporations Act (BCA)*, *Revised Partnership Act*, *Limited Partnership Act*, and *Limited Liability Company Act*. These statutes, collectively known as the *Associations Law*, provide the legal framework for the establishment and operation of domestic and non-resident domestic corporations, partnerships, limited partnerships, limited liability companies, foreign maritime entities, and foreign corporations authorized to do business in the RMI.

31. There are two Registrars: the Attorney General, for resident entities as described; and the Trust Company of the Marshall Islands (TCMI) for non-resident entities. There is an additional requirement if a foreign entity, natural or legal person, wants to register as a resident entity in the RMI. They must meet the requirements of the Foreign Investment Business License (FIBL) Act, and be registered under the Minister of Finance’s designated Register of Foreign Investments. There is a requirement in the FIBL Regulation to declare beneficial share ownership and the natural person owners, but the former is not defined and there is no sanction for false declaration.

32. The statutes do not include mandatory disclosure of beneficial ownership (except under the FIBL) and there are no measures to prevent misuse of bearer shares. The statutes permit nominee and non-resident directors, and directors can be a non-resident legal entity, thereby further obscuring beneficial ownership information. Timely access to accurate and current ownership information may

not be possible because of these reasons and because non-resident companies/entities are not required to keep a copy of their share register in the RMI; access by RMI authorities may only be available through the mutual legal assistance process. However, the two Registrars do make available the information they have to other competent authorities, including foreign competent authorities, and to the public, upon request.

33. The formation of trusts in RMI is governed by the *Trust Act of 1994* and the *Trust Companies Act of 1994*. Formation of trusts can only be performed by and is solely at the discretion of the Marshall Islands Trust Company (“MITC”), which has authority to accept or deny any application. However, the RMI stated the MITC is an inactive company. Additionally, since its formation, the policy of MITC has been not to accept any applications for trusts, nor has it ever accepted any applications for trusts. While there may be, in fact, no existing trust in the RMI formed by the MITC as of the on-site, trusts are nonetheless recognized in the RMI. The law on trusts is still valid and existing albeit unutilized.

34. The non-profit organisation (NPO) sector is governed primarily by the *Non-Profit Corporations Act*, *Cooperatives Act* and *Counter Terrorism Act*. Relevant provisions of the *Association Law* also apply. The Registrar of Corporations is responsible for the registration and filing of NPOs in the RMI, and is the designated contact point for any information request on NPOs. Due to staffing constraints, there is minimum supervision of the sector’s 100 registered NPOs.

35. In 2006, the RMI conducted a sectoral review of its NPO. As part of this review process, two bills to enhance NPO regulation and supervision were submitted to the Nitijela (Parliament) for approval. The bills did not necessarily cover all the requirements of SR.VIII. In any event, the Nitijela did not ratify the bills. Overall, the requirements of SR.VIII have not been implemented.

#### **Preventive Measures—Financial Institutions**

36. RMI sets out in legislation comprehensive AML/CFT preventative measures for the financial sector primarily through Part XIII of the *Banking Act* of 1987 (the *Banking Act*) and the AML Regulations 2002, as substantially revised in May 2010 (the revised *AML/CFT Regulations*). Formal advisory notices under the Act are occasionally issued by the Banking Commissioner, and non-binding guidance is also issued from time to time. Certain advisory notices issued pursuant to the Banking Commissioner’s regulatory powers under the *Banking Act* or revised *AML/CFT Regulations* have the effect of “Other Enforceable Means”. These preventative measures apply across all types of entities in the RMI’s relatively small financial sector, designated either as “financial institutions” (including banks, other lenders, and money transmission service providers) or “cash dealers” (including insurance intermediaries and currency exchangers). RMI has a relatively uncomplicated financial system, and apart from the two banks, there are no securities dealers, fund managers or money changers. The *Banking Act* provides for the licensing of offshore banks but no such licenses are on issue and the Banking Commissioner has advised that there is no intention to issue offshore banking licenses.

37. Most of the essential elements required for compliance with the FATF standards relating to customer due diligence (CDD) are covered by the *Banking Act* and associated legislation, primarily through the May 2010 revision to the *AML/CFT Regulations*. RMI has not generally adopted a risk-based approach to CDD requirements. Implementation of a significant proportion of the revised requirements by subject entities had only commenced in the second half of 2010 and was still underway at the time of the on-site visit. Effectiveness of arrangements to comply with obligations under the revised *AML/CFT Regulations* has not yet been verified through compliance monitoring. Financial institutions and cash dealers do not have adequate policies and procedures to determine the

natural persons who ultimately control customers who are legal persons, and the definition of beneficial owner in the applicable laws is not consistent with FATF standards.

38. Adequate measures with respect to foreign PEPs have been established by regulation and implemented by the two banks, the finance company and the money remitter that are currently most active in their respective sub-sectors. It is not yet possible to evaluate the effectiveness of PEP measures being established by other financial institutions and cash dealers.

39. Correspondent banking relationships are not currently provided by banks in RMI, but the banks' policies conform to international best practices. However, the legal requirements with respect to certain correspondent banking obligations are inadequate. There are no requirements for senior management authorization of correspondent bank accounts or for both parties to correspondent banking relationships to document their respective AML/CFT responsibilities.

40. Third party introducers are not present in RMI or used by the financial institutions for overseas-based customers. There is no domestic electronic funds transfer system between institutions and each bank only provides ATM access to its own accounts. Use of new payment technologies is relatively limited with one bank allowing customers to access their accounts through mobile phone banking using dedicated chip card protection. Business relationships with banks and other financial institutions are only established face-to-face. Banks are alert to the requirements for adequate policies and controls to reduce the risk of misuse of new payments technologies and non-face to face business.

41. There are no issues with respect to bank secrecy laws preventing effective implementation of AML/CFT requirements.

42. Record keeping requirements consistent with FATF standards have been in place for a number of years and are well entrenched in the financial sector. Some originator-information aspects of wire transfer obligations have been in place since the CTA commenced in 2003, but the full range of FATF requirements were only recently formalised under the revised *AML/CFT Regulations*, in 2010. Banks and the main money-remitter appear to be applying policies and procedures consistent with SRVII; however, the Banking Commissioner's powers to authorize a de-minimis threshold of US\$3,000 below which CDD is not required are not consistent with the FATF maximum of US\$1,000.

43. Although there is no explicit obligation to monitor transactions and relationships set forth in the Banking Act, the Banking Commission has incorporated new language in the revised *AML/CFT Regulations* that require financial institutions to conduct enhanced monitoring, specifically on complex or unusually large transactions, and to examine such transactions and set forth and record findings in writing.

44. Financial institutions are not yet required to examine, document and better understand transactions originating from high risk countries that appear to have no apparent economic or lawful purpose; and the Banking Commission has not issued advisories to institutions under its supervision on the weaknesses of AML/CFT regimes of other jurisdictions. As a result of the lack of regulations, the Banking Commission has not been able to apply countermeasures to non-compliant countries.

45. Suspicious transactions and reporting requirements are established in the RMI's *Banking Act* and accompanying revised *AML/CFT Regulations*. The latter, under section 5 (2) (c), further establishes that an STR is required when a financial institution or cash dealer knows, suspects or has reason to suspect that funds or other assets are derived from illegal activities. The former (i.e.

*Banking Act*) includes specific requirements to report when there is suspicion of FT or terrorism under section 170A. Attempted transactions are mandatory in relation to ML and FT under sections 170 (1) and 170A (2) respectively of the *Banking Act*. The language in the *AML/CFT Regulations*, as it is written, may allow for non-reporting of tax matters and there is no explicit requirement for reporting of all criminal activities.

46. A key deficiency is with effective implementation of STR reporting by non-bank financial institutions. Further, at the time of the mutual evaluation, the effectiveness of STR reporting on FT could not be determined due to recent implementation of reporting requirements.

47. The only gap identified in respect of tipping off is that there is no explicit provision in section 170 (4) of the *Banking Act* to prohibit tipping off in the period after a suspicion has been formed and before a STR is made.

48. RMI has CTR reporting requirements under the *Banking Act* and revised *AML/CFT Regulations*. Electronic filing is being done for CTRs.

49. The RMI Banking Commission has not been active in providing feedback to reporting institutions on filed STRs and there are no formalized procedures for communicating the results of financial institutions' reporting of STRs. Out-dated guidelines issued by the Banking Commission, which are roughly six years old, may no longer be relevant and applicable.

50. The requirements for internal controls are covered fully in the *Banking Act* and revised *AML/CFT Regulations*. The deficiency is with effective implementation of this requirement by non-bank financial institutions and cash dealers.

51. The revised *AML/CFT Regulations* extend AML/CFT measures to foreign branches and subsidiaries. However, there were no foreign branches or subsidiaries of financial institutions or cash dealers incorporated in the RMI at the time of the on-site.

52. Shell banks are not permitted to be licensed in RMI, and the banks do not have any dealings with shell banks. The legal requirements on financial institutions are set out in the revised *AML/CFT Regulations* and banks have already put in place policies and procedures consistent with the FATF standards.

53. The Banking Commissioner is provided with powers under the *Banking Act* to monitor and enforce the AML/CFT requirements imposed on these institutions, effected through a mix of on-site and off-site supervision. However, the RMI has material gaps in coverage of subject entities. Several entities that the AML/CFT regulatory requirements apply to (including a government-owned development finance institution) are not currently subject to the Banking Commissioner's supervision regime and do not appear to be complying with AML/CFT requirements. The RMI has not yet carried out a national AML/CFT risk assessment.

54. The Banking Commissioner is the responsible authority and has adequate powers to regulate and supervise compliance by financial institutions and cash dealers with the AML/CFT requirements; however, the implementation of supervision and enforcement of obligations has been limited to date. Both on-site and off-site supervision are carried out to some degree. Only one entity has been subject to on-site examination since 2007 and no assessments have yet been carried out of the financial sector's compliance with the full range of AML/CFT requirements as introduced in 2010. The Banking Commissioner has powers to collect information to assist in off-site monitoring, but there does not appear to be any ongoing compliance monitoring apart from the annual relicensing of banks

and access to annual internal audit reports for banks only. Guidance to subject entities on compliance with AML/CFT requirements is outdated and should be significantly revised to cover the new standards as set out in the revised *AML/CFT Regulations*. Bank examination manuals and supervision procedures also need to be significantly revised.

55. The Banking Commissioner licenses banks, with the approval of Cabinet, after due inquiry and investigation including fit and proper criteria applying to directors, senior managers and owners of more than 10% of the issued stock of the bank. Conditions may be attached to the licence. Banking licences are required to be renewed annually and updated information is obtained as part of the consideration of licence renewal. There are no provisions prohibiting criminals or their associates from holding a controlling interest in, or being a senior manager or director of a non-bank financial institution or cash dealer.

56. The Banking Commissioner has not yet substantively engaged with a number of entities that appear to fall within the scope of the AML/CFT requirements under the *Banking Act* and revised *AML/CFT Regulations*, giving rise to concerns about scope of coverage of the AML/CFT framework as a whole. The Commissioner has indicated that a program of engagement is planned to address these gaps in coverage. There is a need for additional staff resources and external technical assistance to: develop, provide training on, and implement effective monitoring and supervision of entities' compliance with the new requirements; conduct more frequent onsite examinations prioritised according to the perceived level of risk; revise supervision manuals, policies and procedures; and establish comprehensive guidance for subject entities.

57. A limited range of sanctions are provided for non-compliance with the *Banking Act* and *AML/CFT Regulations*, including fines or imprisonment for certain offences under the *Banking Act* and civil money penalties for the majority of offences, including those under the revised *AML/CFT Regulations*. Sanctions can be applied to employees, senior managers and directors of subject entities, as well as to the entity itself. There are no specific powers for the Banking Commissioner to issue administrative fines or compliance orders for breaches of AML/CFT requirements. For licensed banks, there are powers to suspend, revoke or vary a licence under the *Banking Act*, with the approval of the Cabinet, for failure to comply with requirements under the Act or Regulations or where the Commissioner has reasonable grounds to believe that ML activity is taking place. There have been no cases where sanctions have been exercised against subject entities to date. Where compliance failures have been identified by the Commissioner, the entity is advised in writing and rectification requested. The Commissioner will generally review rectification in subsequent on-site examinations. The minimal on and off site compliance monitoring in recent years and limited follow-up of remedial actions taken contributes to a lack of effectiveness of supervisory powers and sanctions.

58. Money value transfer (MVT) service providers are designated as financial institutions under the *Banking Act* and are subject to AML/CFT requirements. There is, however, no licensing or registration requirement for non-bank financial institutions, including MVT providers, or cash dealers. The CTA provides for the establishment of a register for MVT service providers but it has been established. The Banking Commissioner is seeking technical assistance for the establishment of a central registry for such businesses.

### **Preventive Measures—Designated Non-Financial Businesses and Professions**

59. The AML/CFT regulatory requirements in the *Banking Act* and revised *AML/CFT Regulations* apply to the operator of any gambling house, casino or lottery, and a person who carries on a business dealing in bullion. No other categories of DNFBP are covered by these requirements (or as required under FATF Recommendations 12 and 16), nor are there any requirements for any person

providing such services. Given the lack of legal requirements, the RMI currently does not license, supervise or regulate DNFBP for AML/CFT. Furthermore, there are no self regulatory bodies based in the RMI for DNFBP.

60. With the exception of company service formation providers, other designated DNFBP sectors are either non-existent or miniscule. No casinos, gambling businesses or lotteries are permitted in RMI under the provision of the *Gambling and Recreation Prohibition Act 1998*, with the exception of fund raising activities by non-profit organizations. There do not appear to be any real estate agents operating in RMI, nor are there any businesses dealing in precious stones and metals over the threshold amount. While trust is legally recognized, there is no trust formation business based in the RMI. There is a legal profession and a handful of accountants providing services to the private sector.

61. The main DNFBP sector is the offshore company formation services sector. These are accountants, lawyers and other company service providers based in foreign jurisdictions providing services for the RMI's offshore company registry. However, there is no direct supervision of such company formation service providers. The Registrar performs some due diligence prior to accrediting company formation service providers as "qualified intermediaries", including screening their names through commercially available databases and verifying that they are a licensed attorney, banker, accountant, or corporate formation specialist. There is no ongoing annual requirement to maintain the accredited status, although on each occasion a qualified intermediary submits an application of incorporation on behalf of a client, the details of the qualified intermediary are checked again through the data base used.

62. The RMI should introduce an appropriate legal and supervisory framework for AML/CFT requirements on DNFBP with a prioritised and phased implementation based on a risk assessment, with a focus on enhancing supervision of offshore company formation service providers.

63. Due to the relatively high reliance on the use of cash as the primary means of conducting transactions, there has been little done to promote and encourage more modern and secure methods of conducting financial transactions.

### **National and International Co-operation**

64. The national AML/CFT Committee is chaired by the Banking Commissioner, and consists of the Police Commissioner, the Assistant Secretary for Customs and a representative from the OAG. The Committee serves to act as a forum on AML/CFT and as the FIU Committee. Given the size of the RMI, coordination has been relatively informal but regular.

65. RMI acceded to the Vienna and Palermo Conventions on 10 November 2010. RMI. Many of the Palermo Convention's requirements are provided under the *Banking Act*, albeit with noted deficiencies as aforementioned. RMI acceded to the UN Convention for the Suppression of the Financing of Terrorism (1999) in 2003. RMI enacted the Counter Terrorism Act of 2002 to criminalise FT. There are some deficiencies with implementing the United Nations Security Council Resolutions.

66. RMI has a comprehensive MLA regime primarily governed by the *Mutual Legal Assistance in Criminal Matters Act* (MACMA) and the POCA. Deficiencies in the ML offence, particularly in relation to coverage of predicate offences, may undermine the operation of MLA in practice. FT-related requests for legal assistance made under the CTA are carried out utilizing the provisions of the MACMA. All requests for international assistance are made by, and through the Attorney General, who may grant, refuse or postpone any action on the request under the conditions provided under the

MACMA. The MACMA, however, is restrictive as it applies only where a foreign State has made an arrangement with, or enters into a reciprocal agreement or assistance in criminal matters with the RMI. At present, this formal arrangement is limited to an agreement with the US and RMI's tri-lateral extradition treaty with Palau and the Federated States of Micronesia. It was noted that there are no clear and efficient processes in place for the execution of mutual legal assistance requests in a timely way and without undue delay. Moreover, the deficiencies in the ML legislation, e.g. scope of predicate offences, has a limiting effect on RMI's ability to provide legal assistance.

67. Dual criminality, whether for ML or FT, is observed in the grant of mutual assistance under the MACMA. Section 405 (q), (ii) is comprehensive enough that would allow RMI authorities to provide assistance using the "same conduct" approach to MLA.

68. The *Criminal Extradition Act (CEA)* sets out the procedures for extradition. Given the broad wording of the *CEA*, it only requires that the person to be extradited has been charged with a crime, ML is deemed extraditable under the *CEA*. The CTA specifically provides that terrorism offences are extraditable offences. There are no procedures that provide clear timeframes for processing extradition requests. According to authorities, RMI does not extradite its nationals.

69. The RMI has legal and institutional gateways to facilitate international co-operation by law enforcement, the Banking Commission and the DFIU in situations other than the formal MLA process and generally provides such co-operation. There have only been limited cases of the use of such mechanisms.

## **1. GENERAL**

### **1.1. General Information on Republic of the Marshall Islands**

70. The RMI is comprised of 29 atolls and five single islands, which form two parallel groups, the "Ratak" (sunrise) chain and the "Ralik" (sunset) chain. The population in 2009 was 63,100. Two-thirds of the population lives on the islands of Majuro and Ebeye. The outer islands are sparsely populated due to lack of employment opportunities and economic development. There are also Marshallese resident in the US, primarily in Hawaii, Oregon, California, and Arkansas.

71. The Marshallese are of Micronesian origin, which is traced to Southeast Asia in the remote past. The matrilineal Marshallese culture revolves around a complex system of clans and lineages tied to land ownership.

72. Marshallese is the official language. English is spoken to some extent by most of the adult urban population. However, both the Nitijela (Parliament) and national radio use Marshallese.

73. The Revised Compact of Free Association, dated 30 April 2003, between the RMI and the United States (US) broadly defines the nature of the political, economic, and military relationships between the RMI and the US. Under the Compact, the RMI is empowered to operate under its own Constitution and conduct its own domestic and foreign affairs. There are special provisions governing mutual assistance and cooperation in law enforcement matters.

#### **Economy**

74. The RMI's total GDP in 2008 was estimated at US\$161.7 million. The RMI uses the US currency.

75. The government is the largest employer, employing 46% of the salaried work force. GDP is derived mainly from payments made by the US under the terms of the Compact of Free Association.

76. Since 1990, the RMI has offered ship registrations under the RMI flag. It now maintains a fleet of about 2400 vessels, the third-largest open registry fleet in the world.

77. The economy combines a small subsistence sector and a modern, service-oriented urban sector located in Majuro and Ebeye. It is sustained by government expenditures and the US Army installation at Kwajalein Atoll. The US airfield on Kwajalein serves as a second hub for international flights.

78. The modern sector consists of wholesale and retail trade; restaurants; banking and insurance; construction, repair, and professional services; and copra processing. Copra cake and oil are by far the nation's largest exports. A tuna loining plant that employs 600 workers reopened in early 2008. Copra production, the most important single commercial activity for the past 100 years, now depends on government subsidies. The subsidies are intended to help reduce migration from outer atolls to densely populated Majuro and Ebeye. Migration from the outer islands is estimated at 8% annually.

79. Marine resources (including fishing), aquaculture, tourism development, and agriculture, are top government development priorities. The Marshall Islands sells fishing rights to other nations as a source of income. The Marshall Islands must import a wide variety of goods, including foodstuffs, consumer goods, machinery, and petroleum products.

#### **System of Government**

80. The 1979 constitution established a parliamentary government, with a President as Chief Executive and Head of State. The President is elected by the Nitijela (Parliament) from among its members. The Council of Iroij is the upper house of the RMI bicameral parliament, while the Nitijela is the elected lower house. The Council is comprised of 12 tribal chiefs who advise the Presidential Cabinet and review legislation affecting customary law or any traditional practice, including land tenure. Legislative power resides in the Nitijela which comprises 33 senators elected by 24 electoral districts which correspond roughly to each atoll of the RMI.

### **Legal system and hierarchy of laws**

81. The legal system is based on the former Trust Territory laws, but has been modified by the legislature, municipal bodies, customary law, and common law.

82. There are four levels of judicial courts: the Supreme Court, the High Court, the District and Community Courts, and the Traditional Rights Court. Trial is by jury or judge. Jurisdiction of the traditional rights court is limited to cases involving titles or land rights or other disputes arising from customary law and traditional practice.

### **Transparency, good governance, ethics and measures against corruption**

#### ***Good Governance***

83. The RMI has a democratic and accountable system of government with an independent judicial system and a free media. There have been a number of local and national elections since the RMI was founded, and in general, democracy has functioned well, although traditional chiefs and major land owners dominate the political landscape.

84. Most recently this democratic process was exercised on 21 October 2009, when a motion of no confidence in the former President was passed in the Nitijela, and the RMI cabinet dissolved. On 26 October 2009, the Nitijela elected a new President and some new ministers were appointed.

85. Concerns have been voiced publicly concerning fiscal accountability in the RMI given its relatively poor fiscal management record, including issues associated with the ongoing administration of the Marshall Islands Social Security Fund and relatively poor taxation collection. Furthermore, the Auditor General's Office has often been left vacant and not all government ministries produce an annual report with audited financial statements made available to the public.

#### ***Corruption***

86. The RMI is not ranked in Transparency International's Corruption Perception Index.

87. The RMI has not signed the UN Convention Against Corruption but the RMI *Criminal Code* provides criminal penalties for official corruption including misconduct in public offices, bribery and private official gain of public officials. Public officials, however, are not subject to financial disclosure laws. The OAG is responsible for investigating cases of alleged corruption, but few cases have been prosecuted. No high-level elected official has ever been indicted for corruption. The only case of a government official charged and convicted of corruption was the former director of the Marshall Island's College in 2002.

88. Voters tend to look to elected representatives for financial assistance, which pressures elected officials to use government authority to provide patronage to extended family members and supporters. This has frequently led to allegations of nepotism in government hiring and in contracting.

## **1.2. General Situation of Money Laundering and Financing of Terrorism**

### **Sources of Illicit Funds**

89. Based on operational law enforcement experience and STRs submitted, offences generating illicit proceeds are tax evasion and smuggling, followed by embezzlement, counterfeit instruments, cheque fraud and selling of marijuana. Statistics show a total of 54 serious offences were prosecuted in the 5 year period from 2004-2009. In the period from January to August 2010, there were 22 serious offences prosecuted. While details on the nature of the serious offence are not available for the five year period, the available statistics indicate they relate mainly to physical harm and not proceeds related i.e. assaultive behaviour (sexual assaults), or drunk or reckless driving. There were property related prosecutions such as burglary or larceny and selling of marijuana.

90. The relatively large number of criminal cases filed in Ebeye in 2004 reflect a series of cocaine-related cases involving a bale of cocaine that washed ashore. During the on-site, the Chief Justice advised that the bale of cocaine was not a result of deliberate importation but accidentally washed ashore, it is assumed, from a vessel passing through the RMI chain of atolls. However, numerous charges and convictions resulted from possession and use of cocaine. There has not been another incident of cocaine washed ashore since 2004.

91. Authorities mentioned that proceeds from taxation and customs offences would likely to be the major sources of illegal proceeds. However, most enterprise crimes involved relatively small amounts of money i.e. under US\$1,000 except for two cases involving the illegal importation of cigarettes and a case of employees stealing about US\$80,000 worth of goods from a local store.

92. Statistics on police investigation of proceeds related predicate offences are consistent with this view, except on taxation evasion:

**Table: Predicate Offences 2007 to 2009**

<b>Category</b>	<b>No.</b>
Auto-Theft	5
Burglary	180
Counterfeiting	5
Embezzlement	8
Forgery	4
Grand Larceny	87
Robbery	6

93. According to authorities, the discrepancy on taxation can be attributed to a lack of financial investigative capacity.

### **Money laundering methods and trends**

94. RMI has neither conducted a formal AML/CFT threat/risk assessment nor typologies studies. Without any ML prosecutions, and limited open source information, it is challenging to derive a

comprehensive conclusion of methods and trends. There were two cases initially investigated for ML but one case ended up being prosecuted on prostitution charges<sup>1</sup>, and a second case resulted in tax payment settlements with the local tax authorities. However, given the features of the RMI, it is probable that illicit proceeds would involve self laundering and either held as cash or converted into tangible assets, and if needed, transferred offshore either physically or via the formal banking system.

### **Terrorism and Financing**

95. Authorities view terrorism and FT threat as very low in the RMI. There has never been a terrorist incident in the RMI. There has been no STR reported pertaining to FT, although the FT reporting obligation was only recently introduced in mid- 2010. There have been no instances or investigations related to financing of terrorism in the RMI.

### **Money Laundering and Terrorism Financing Vulnerabilities**

96. The RMI is located in an isolated area of the Pacific Ocean and has a limited financial sector. The RMI is unlikely to be considered an attractive end destination or transit point for illicit proceeds because of these and other factors. Nor could the RMI be considered a significant source of illicit funds, either regionally or globally.

97. ML and FT vulnerabilities in the RMI derive mainly from its offshore company registration sector. The corporate anonymity afforded by companies registered in the RMI represents significant ML vulnerabilities. The RMI is heavily marketed on the internet by third parties outside of the control of the RMI on the taxation and corporate opaqueness advantages of the RMI's non-resident domestic company registry. There is no mandatory requirement for entities to provide information either on the legal or beneficial ownership of shareholders.

98. The Trust Company of the Marshall Islands, Inc. (TCMI) is the Registrar of Corporations for non-resident domestic corporations, partnerships, limited partnerships, limited liability companies, and foreign maritime entities. The RMI retains jurisdiction over RMI non-resident domestic legal persons. No AML/CFT controls apply. The TCMI building in the RMI is the repository of all filed and recorded documents of non-resident domestic entities. Registration of non-resident domestic entities is administered in part through International Registries, Inc. (IRI), a private company, headquartered in Virginia, with 19 subsidiaries and branches globally in Baltimore, Dalian, Dubai, Ft. Lauderdale, Geneva, Hamburg, Hong Kong, Houston, Istanbul, London, Mumbai, New York, Piraeus, Roosendaal, Seoul, Shanghai, Singapore, Tokyo, and Zurich.

99. The RMI was previously on the OECD's list of non-cooperative jurisdictions for taxation transparency but was removed in 2007 after the RMI committed to improving its program. Since then, the RMI has been proactive in signing agreements on taxation information exchange.

### **1.3. Overview of the Financial Sector and DNFBP**

100. The RMI has a relatively small financial system.

---

<sup>1</sup> This is a case in 2010 and does not appear in the above table on crime offences for 2007-09.

**Table (a): Overview of Financial Sector, 2010**

<b>Financial Institutions</b>	<b>Number of Institutions (As identified)</b>
Banks (see table (b) below )	2(i)
Insurance Companies (intermediaries)	3
Foreign exchange providers	2 (ii)
Money transmitters	3 (iii)
Finance Companies	3
Retirement Fund	1

- (i) Excluding the government owned development bank  
(ii) The two commercial banks  
(iii) One bank provides these services as an agent of an international money remitter

**Table (b): Overview of RMI's Regulated Banking Sector**

<b>No. of Banks</b>	<b>No. of Branches</b>	<b>No. of Deposit Account Holders</b>	<b>Number of Employees</b>	<b>Number of ATMs</b>	<b>Annual Average Currency transactions Above \$10,000</b>	<b>Total Assets</b>
<b>2</b>	<b>4</b>	<b>15,500</b>	<b>132</b>	<b>2</b>	<b>2,475</b>	<b>\$133.0m</b>

**Table (c): Financial Activity by Type of Financial Institution**

<b>Type of financial activity (See glossary of the 40 Recommendations)</b>	<b>Type of financial institution that performs this activity</b>	<b>AML/CFT regulator &amp; supervisor</b>
1. Acceptance of deposits and other repayable funds from the public (including private banking)	Banks	Banking Commission
2. Lending (including consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting))	Banks Finance companies	Banking Commission
3. Financial leasing (other than financial leasing arrangements in relation to consumer products)	Non-Bank Credit Institutions	Banking Commission
4. The transfer of money or value (including financial activity in both the formal or informal sector (e.g. alternative remittance activity), but not including any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds)	Banks Money remitters	Banking Commission

Type of financial activity (See glossary of the 40 Recommendations)	Type of financial institution that performs this activity	AML/CFT regulator & supervisor
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money)	Bank	Banking Commission
6. Financial guarantees and commitments	Banks Finance companies	Banking Commission
7. Trading in: (a) money market instruments (b) foreign exchange; (c) transferable securities	Banks	Banking Commission
8. Participation in securities issues and the provision of financial services related to such issues	N/A	N/A
9. Individual and collective portfolio management	Marshall Islands Social Security Administration	N/A
10. Safekeeping and administration of cash or liquid securities on behalf of other persons	Banks	Banking Commission
11. Underwriting and placement of life insurance and other investment related insurance (including insurance undertakings and to insurance intermediaries (agents and brokers)	Life insurance agents	Banking Commission
12. Money and currency changing	Banks	Banking Commission

### ***Banking Sector***

101. The banking sector has only two commercial banks, the Bank of Guam (BOG) and the Bank of the Marshall Islands (BOMI). The banking sector had a total asset size of US\$133 million in May 2010. The two banks provide full commercial banking services, including savings and term deposit accounts, cheque account facilities, consumer and commercial lending activities, money market accounts, and credit card services (only BOG).

102. The BOG operates as a branch in the RMI and has its head office in Guam. The BOG is regulated under US law, including AML/CFT controls. All deposits held by the bank are insured with the Federal Deposit Insurance Corporation (FDIC) of the United States.

103. BOMI is a locally incorporated commercial bank that is majority owned by the Marshall Islands Social Security Administration. Other shareholders are the Marshall Islands Development Bank (MIDB) and individuals.

104. Another bank, the First Micronesian Bank has obtained a banking license from the Banking Commission to operate in the RMI. However, the bank has not commenced operation, and Banking Commission issued a notice to withdraw the banking license in 2009. The RMI authorities could not confirm that the license was actually withdrawn.

105. MIDB is also another important financial institution in the RMI, which was established in 1988 to promote the development and expansion of the economy of the RMI by providing loans for

enterprises and individuals. The MIDB is not supervised by the Banking Commission for prudential or AML/CFT purposes.

106. Although the *Banking Act* 1987 provides for the licensing and operation of offshore banks, there are currently no offshore banks licensed in the RMI. The Banking Commission indicated it has no intention to license offshore banks in the future.

### **Money Changers**

107. Only the two banks provide authorized foreign exchange services. There are no licensed NBFI money changers.

### **Money/Value Transmission Providers**

108. There are two international money remitters operating in RMI i.e. Western Union and Money Gram. Western Union's two agents are a subsidiary of a local conglomerate and the Majuro Payless Store. Western Union mainly serves Filipinos and Marshallese based in the US; Money Gram has an agency in Majuro and operates as a division of the BOMI.

109. Given the market for remittance services is small, and adequately covered by existing providers, RMI officials expressed the view that the alternative remittance sector is minimal or insignificant. There is another company, BINGO, which the Banking Commission has identified as providing remittance services and will be included in the Banking Commission supervisory program. Currently, BINGO can be considered an alternative remittance provider until it is formally registered by the Banking Commission.

### **Insurance**

110. There are three insurance providers: Marshalls Insurance Agency, Moylans Insurance Underwriters and Individual Assurance Company. Insurance providers are locally incorporated and are agents of foreign insurers. All insurance providers, except IAC, ceased accepting new life insurance policies.

111. The insurance products provided in RMI are not those that are typically more vulnerable to misuse for ML/FT.

### **Finance Companies**

112. Ajejdrikdrik is a locally owned non-deposit taking finance company that provides personal and small business loans to the community. Most personal loans are provided as a cash advance against salaries with repayments based on salary deductions. The average loan is about US\$2,000 per loan, although business loans can be up to US\$30,000. Ajejdrikdrik is regulated for AML/CFT.

113. In addition, there are two (2) companies that offer loan financing through car sellers that are not currently regulated for AML/CFT.

### **Fund Management**

114. The Marshall Island Social Security Administration is an RMI statutory agency that manages the retirement fund open to all employees working in the RMI, RMI citizens working outside the country, and self-employed persons in RMI. It is not subject to AML/CFT obligations.

### ***Savings and Loan***

115. The authorities advised that there are no savings and loans or employee cooperatives in existence. They indicated that there used to be a teachers' cooperative but this is no longer operational.

### ***Securities***

116. There is no securities market in the RMI.

## **1.4 Overview of the DNFBP Sector**

### **a. Casinos (which also includes internet casinos)**

117. There are no casinos operating in the RMI because it is prohibited by the *Gambling and Recreation Prohibition Act 1998*.

### **b. Real estate agents**

118. All land in the RMI is owned by Marshallese individuals. Foreigners cannot own land in the RMI. Land is held in perpetuity by members of clans and extended families, and certain lands and fishing waters are held by the entire community. Land inheritance is matrilineal.

119. The use of land is determined by all three social classes in the RMI, namely the Iroij (chief), the Alap (owner or elder) and Rijerbal (worker or commoner). Iroij have ultimate control of such things as land tenure, resource use and distribution, and dispute settlement. The Alap supervises the maintenance of lands and daily activities. The Rijerbal are responsible for all daily work on the land including cleaning, farming, and construction activities.

120. All three tiers of land users must agree to any transfer of land title. Any proposed transfer need to be registered with the Land Register. The Land Register then must go through a process of public consultation i.e. put a public notice in a newspaper for three to six months to ensure no other valid claimant. This is part of a new system introduced in 2004.

121. Since 2004, there have only been 10 new land registrations. People have objected to these land registrations claiming rights to the land. If someone contests, the application goes to the civil court to deliberate and also to the Traditional Rights Court. This has caused problems with using land as collateral for loans.

122. There are no real estate agents in the RMI as the market for land title transfer is very small and complex. There are informal referrals within the community network but they are negligible.

### **c. Dealers in precious metals/ Dealers in precious stones**

123. The team visited three major shops selling jewellery and precious stones. None of the stores contained items valued over US\$15,000. Only one store stocked one item of value i.e. a pearl for US\$2,000. This was a left over stock from a pearl farm which had closed down a few years ago. The general view is people would buy precious stones and metals in Guam, Hawaii or continental USA.

### **d. Lawyers, notaries, other independent legal professionals and accountants**

**(i) Lawyers**

124. Lawyers in the RMI include those in public practice and lawyers employed by the government. There are about 57 active attorneys in the RMI. Lawyers based in the RMI also provide company formation services for domestic corporations.

125. Law graduates, either local or foreign, are required to obtain a practice licence from the Chief Justice. The prerequisites include passing RMI's Bar Examination, which is administered by the Chief Justice's Office and based on the US Bar Exam. The bar examination is exempted for any applicant employed as a government attorney for at least 5 years.

126. All applicants must submit an application to practice. The application form includes the requirement to certify that:

*"no criminal charge nor any charge for violation of professional ethics or responsibility is currently pending against me and that I have never been convicted of any crime or found in violation of a rule of professional ethics or responsibility."*

**(ii) Accountants**

127. Accountants based in Guam do audits of major companies and national and local government agencies. There is a branch of a large international accountancy firm based in the RMI. However, it has only two staff and the office does not carry out external audits. There is neither a professional accountancy association nor any legal requirements governing the accountancy profession in RMI.

128. There is an annual single audit of all government agencies, which is conducted by a contracted accountancy firm based in Guam.

129. Except for the branch office of an international accountancy firm, the accountants in private practice provide book keeping and accountancy services to small family owned businesses. The local office of the international accountancy firm does not provide company formation service nor hold funds in trust for clients.

**(e) Company and trust service providers**

130. Accountants, lawyers and other company service providers based in foreign jurisdictions submit applications for company formations to the RMI's offshore company registry. The Registrar performs some due diligence prior to accrediting company formation service providers as "qualified intermediaries", including screening their names through commercially available databases and verifying that they are a licensed attorney, banker, accountant, or corporate formation specialist. There is no ongoing annual requirement to maintain the accredited status, although on each occasion a qualified intermediary submits an application of incorporation on behalf of a client, the details of the qualified intermediary are checked again through the database used.

131. There is no trust industry in the RMI as the government decided not to register trusts – a mandatory legal requirement for domestic trusts - although foreign trusts are legally recognised in the RMI.

**1.5. Overview of commercial laws and mechanisms governing legal persons and arrangements**

132. The RMI Associations Law, *Title 52 of the Marshall Islands Revised Code (MIRC)*, consists of the *Business Corporations Act (BCA)*, *the Revised Partnership Act*, *the Limited Partnership Act*, *the Limited Liability Company Act*, and *Other Forms of Associations*. These statutes provide the legal framework for the establishment and operation of resident and non-resident domestic corporations, partnerships, limited partnerships, limited liability companies, foreign maritime entities, and foreign corporations authorized to do business in the RMI.

133. The *Associations Law* covers both resident and non-resident entities, irrespective of the Registrar under which it is incorporated. The RMI has two Registrars of Corporations: a Registrar responsible for resident domestic and authorized foreign corporations, and a Registrar responsible for non-resident domestic corporations, partnerships, limited partnerships, limited liability companies, and foreign maritime entities. The Attorney General is the designated Registrar responsible for resident domestic and authorized foreign corporations; TCMI is the Registrar responsible for non-resident domestic corporations, partnerships, limited partnerships, limited liability companies, and foreign maritime entities.

The *Trust Act of 1994* and the *Trust Companies Act of 1994* govern the formation of trusts. Although, as noted, the Marshall Islands Trust Company (“MITC”), which has the authority to accept or deny any trust application, is an inactive company.

#### **(c) Non Profit Organizations**

134. The following statutes and regulations govern the operations of incorporated and non-incorporated NPOs in the RMI.

- *Non-Profit Corporations Act*
- *Associations Law (Business Corporations Act, Revised Partnership Act, Limited Partnership, Limited Liability Company Act, Other Forms of Associations)*
- *Cooperatives Act*
- *Counter Terrorism Act*

135. The Marshall Islands Council of NGOs (MICNGOS) is the umbrella organization for the NGO sector in the RMI. It does not have a formal role as a self-regulatory organization..

### **1.6. Overview of strategy to prevent money laundering and terrorist financing**

#### **a. AML/CFT Strategies and Priorities**

136. Since the last Mutual Evaluation in November 2004, the RMI’s AML/CFT focus has been two-fold: rectifying deficiencies in the AML/CFT legal framework, and enhancing the regulatory/supervisory net of the Banking Commission. RMI made amendments to *Banking Act (Public Law 2009-20)*, issued revised *AML/CFT Regulations* and passed the *Currency Declarations Act (Public Law 2009-29)*.

137. The RMI has focused on preparing and introducing bills in Parliament to further enhance the AML/CFT framework. These include the Proceeds of Crime Bill 2010, Mutual Assistance in Criminal Matters Bill, *Banking Act* Amendment Bill 2010 to formalize the FIU, and resolutions to ratify the Vienna and Palermo Conventions. The RMI acceded to the Vienna and Palermo Conventions on 10 November 2010.

138. The Banking Commission aims to licence and regulate a small number of micro financial service providers not currently under the Commission's regulation and supervision. The Banking Commission is also planning to enhance its on-site inspection program of non-bank financial institutions and cash dealers.

139. There are plans to create an outreach program to familiarize cash dealers and financial institutions about trends and developments regarding illegal activities, and to develop industry specific guidance notes (or general guidance notes applicable to all sectors) in relation to the AML/CFT requirements of RMI.

#### **b. The Institutional Framework for Combating Money Laundering and Terrorist Financing**

140. An AML/CFT committee meets quarterly and consists of the heads of the Banking Commission, Domestic Financial Intelligence Unit, Department of Public Safety, Division of Customs; Registrar of Non-Resident Corporations, and Office of the Attorney General. There is also the FIU Committee which consists of the Banking Commissioner, Police Commissioner, Revenue and Taxation Division Chief, and OAG which meets on a monthly basis.

##### ***Banking Commission***

141. The Banking Commission serves as the sole financial sector regulatory agency of the RMI. The Banking Commission is empowered to implement the preventative measures under the *Banking Act* and revised *AML/CFT Regulations* issued in May 2010. The Banking Commission also has investigative powers.

##### ***Financial Intelligence Unit***

142. The Domestic Financial Intelligence Unit (DFIU) comprises of the Banking Commissioner as Head, the Commissioner of Police, and Revenue and Taxation Division Chief and a representative from the Attorney Generals Department in a supportive role. The Attorney General currently fulfils that role.

143. The DFIU is operationally housed within the Banking Commission. The dual roles of Banking Commissioner and DFIU Head is performed by the same person i.e. Banking Commissioner, with two of her staff (there are only three staff in the Banking Commission) also performing dual DFIU and Banking Commission roles.

144. Section 167 of the *Banking Act* 2000 provides the Banking Commissioner with the powers of a financial intelligence unit. The amendment to section 167 of the *Banking Act* passed in June 2009 extended the role of the FIU to include receipt, analysis and dissemination of STRs in relation to FT.

##### ***Department of Public Safety***

145. The Department of Public Safety (DPS) is the consolidated law enforcement agency for the RMI. The DPS was established pursuant to the *Public Safety Act 1988*. Part II, Division 1 of the Act, and specifically sections 503 and 504 respectively, established the office of the DPS and the Head of the Department, the Commissioner of Public Safety. The functions, powers and duties are contained in Part 11, Division 3 (Powers and Duties) and Part V (General) and Part VI (Undercover Investigation Division).

146. The Criminal Investigative Division (CID) within the DPS is the primary police organization to carry out investigations into ML or FT and other predicate offences pursuant to the *Banking Amendment Act 2000*, *Criminal Code Revised 2005* and the *Counter Terrorism Act 2002*.

#### ***Division of Customs, Revenue, Taxation, & Treasury***

147. The Division of Customs, Treasury, Revenue & Taxation in the Ministry of Finance is responsible for implementing the *Currency Declaration Act of 2009* and the *Import Duties Act of 1989*.

#### ***Ministry of Finance***

148. The Ministry of Finance is responsible for issuing foreign investment business licences (FIBL). Any person who is not a citizen of RMI is not permitted to do business in the RMI, and is also not permitted to acquire an interest in any business previously owned entirely by citizens of the RMI without first obtaining a FIBL from the Ministry of Finance.

#### ***Ministry of Foreign Affairs***

149. The Ministry of Foreign Affairs is responsible for coordinating ratification of UN instruments and monitoring the RMI's implementation of UN Conventions. This includes UNSCRs 1267 and 1373.

#### ***Office of the Attorney General (OAG)***

150. The Office of the Attorney General (OAG) offers legal services to the Office of the President, the Cabinet, the ten line ministries and to the various statutory corporations and other government agencies. The OAG is also responsible for all criminal prosecution in the RMI and all civil litigation in which the RMI is a party. There are four attorneys in the Office and some in the legislative branch of the Nitijela. The six attorneys include the chief prosecutor.

#### ***Registrar of Corporations – Resident & Non-Resident***

##### ***a. Office of Attorney General – Registrar of Incorporation***

151. Under the Associations Law, the OAG acts as the Registrar of Corporations and is responsible for the incorporation of resident domestic legal persons in the RMI.

152. The Office of the Registrar of Corporations in the OAG is also responsible for the registration and ongoing regulation of non-profit organizations (NPOs) in the RMI, both incorporated and unincorporated.

##### ***b. The Trust Company of the Marshall Islands, Inc. (TCMI)***

153. TCMI is the Registrar responsible for non-resident domestic corporations, partnerships, limited partnerships, limited liability companies, and foreign maritime entities.

##### ***c. Approach Concerning Risk***

154. The RMI has not undertaken a national risk assessment or adopted a risk based approach to AML/CFT supervision. It has not identified lower risk financial or DNFBP sectors or decided to limit or exempt the application of certain FATF Recommendations.

155. The RMI does permit its financial institutions and cash dealers to take risk into account when determining the extent of the customer due diligence (CDD) measures that the institution must take. Section 3 of the revised *AML/CFT Regulations* include a definition of risk-based customer due diligence (CDD) and the requirement that CDD must be applied on a risk basis, which must include enhanced CDD for higher risk customers and PEPs, and may include simplified CDD for lower risk customers.

**d. Progress since the Last Mutual Evaluation**

156. The RMI has undertaken a number of enhancements to its legal and institutional framework:

- An AML/CFT Committee has been established;
- Amendments to sections 167 and 170 of the *Banking Act* were passed in 2009 to cover the financing of terrorism and suspicious transactions reporting of the former, respectively;
- Amendments to the AML Regulations, 2002 were passed in May 2010 to include revised and enhanced CDD requirements for financial institutions and cash dealers;
- Enactment of the Currency Declarations Act (Public Law 2009-29) to provide for the seizure, detention or forfeiture of currency that is derived from, or intended to be used in criminal conduct;
- The DFIU has entered into additional exchange instruments with foreign FIUs and information has been exchanged;
- The DFIU has been provided with an IT system for CTR and STR analysis and intelligence work by the US Department of State through the US Embassy in Majuro; and
- The Banking Commission has commenced a program of on-site inspection of financial institutions and cash dealers.

157. However, other recommendations from the first MER have not been fully met. These are detailed further in this report. The main outstanding item is that the Banking Commission has not included the Marshall Islands Development Bank (MIDB) in the AML/CFT supervisory framework.

## 2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

### 2.1 Criminalization of Money Laundering (R.1 & 2)

#### 2.1.1. Description and Analysis

*Criminalization of Money Laundering (c. 1.1—Physical and Material Elements of the Offence):*

158. The *Banking Act* and the *RMI Criminal Code* are the relevant statutes for the criminalization of ML. Money laundering is criminalized under section 166, Part XIII of the *Banking Act* of 1987, which states:

**§166. Money laundering offenses and penalties.**

*(1) A person commits the offense of money laundering if the person:*

*(a) acquires, possesses or uses property, knowing or having reason to believe that the property is the proceeds of crime;*

*(b) knowing or having reason to believe that such property is the proceeds of crime, renders assistance to another person for:*

*(i) the conversion or transfer of property, with the aim of concealing or disguising the illicit origin of that property, or of aiding any person involved in the commission of the offense to evade the legal consequences thereof; and*

*(ii) concealing or disguising the true nature, origin, location, disposition movement or ownership of the property.*

*(2) Where a person is convicted of any of the offenses specified in Subsection (1), in the case of a natural person, such person shall be liable to imprisonment for a term of imprisonment not exceeding twenty (20) years or a fine not exceeding \$2,000,000, or both, and in the case of a body corporate five (5) times such a fine or double the amount of money involved in the offense scheme, which ever is greater.*

159. Section 166 (1) is not fully in accord with the Vienna and Palermo Conventions. Acts are criminalized where a person acquires, possesses or uses property, knowing or having reason to believe that the property is the proceeds of crime. However, as stated, it does not penalize a person who is involved in the conversion or transfer of property, or concealment or disguise, only a person who “renders assistance”. To “render assistance” is to “aid and abet” which is more of an ancillary offense to ML.

*The Laundered Property (c. 1.2):*

160. Section 102 of the *Banking Act* defines the **proceeds of crime** as “any property derived from or obtained, directly or indirectly through the commission of a serious offense.” **Property**, on the other hand, has been defined as “assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title or interest in such assets, (see section 102, *Banking Act* ). The *Banking Act*’s definition of **proceeds of crime** and

**property** is the same as that, respectively, under the Vienna (*Article 1, (p) and (q)*) and Palermo (*Article 2, (d) and (e)*) Conventions.

*Proving Property is a Proceed of Crime (c. 1.2.1):*

161. There is no express requirement when proving that property is a proceed of crime that a person be convicted of a predicate offence. Authorities point out that the law only requires that the person “**knows or had reason to believe that the property is the proceeds of crime**” (emphasis supplied). Authorities indicate that they believe a ML prosecution could proceed in the absence of a charge or conviction for a predicate offence. There is, however, no case law yet on this matter.

*The Scope of the Predicate Offences; Threshold approach (c. 1.3)*

162. RMI has adopted a threshold approach by designating all **serious offences** as predicate offences to ML. The *Banking Act* defines a *serious offense* as follows:

(dd) “*serious offense*” means an offense against a provision of

(i) Any other law in the Republic of the Marshall Islands, for which the maximum penalty is imprisonment or other deprivation of liberty for a period of not less than 12 months;

(ii) a law of a foreign State, in relation to acts or omissions, which had they occurred in the Republic of the Marshall Islands, would have constituted an offense for which the maximum penalty imprisonment or other deprivation of liberty for a period of not less than 12 months.  
(§102 (dd), Part I, *Banking Act*)

163. The *Criminal Code* contains a number of offences that meet the one-year threshold qualifying as “serious offences”. They are as follows:

- Aggravated Assault (section 114)
- Bribery (section 118)
- Burglary (section 119)
- Conspiracy (section 120)
- Counterfeiting (section 121)
- Forgery (section 130)
- Kidnapping (section 135)
- Grand Larceny (section 137)
- Cheating (section 138)
- Embezzlement (section 139)
- Receiving stolen goods (section 140)
- Unlawful issuance of bank checks or drafts (section 141)
- Obstructing justice (section 149)
- Robbery (section 150)
- Misconduct in public office (section 171)
- Bribery of public officials and government employees (section 172)
- Private financial gain by public officials or government employees (section 173)
- Receipt of unauthorized rewards gratuities and emoluments (section 174).

164. Other offences that would qualify as a *serious offence* include violations of: the *Narcotics Drugs (Prohibition and Control) Act*, the *Weapons Control Act*, the *Prostitution Act*, the *Treason and Sedition Act*.

165. Aside from the commission of terrorist acts and FT under section 107 and 120 of the *Counter Terrorism Act* of 2002 (CTA), the following offences under the CTA would also come under the definition of *serious offences*:

- Weapons of Mass Destruction Offenses (Sec.125)
- Internationally Protected Persons Offenses (Sec.126)
- Hostage Taking (Sec. 127)
- Terrorist Bombing (Sec.128)
- Plastic Explosives (Sec. 129)
- Safety of Civil Aviation Offenses(Sec.130)
- Maritime Offenses (Safety of Maritime Navigation and Fixed Platform) (Sec.135)
- Nuclear Material Offenses (Sec.136).

166. The predicate offences under the RMI laws do not cover the entire FATF designated categories of predicate offences. There are no provisions criminalizing piracy of products, human trafficking and migrant smuggling, insider trading and market manipulation. Some of the offences considered as environmental crimes are limited in scope and would not qualify as a serious offence because of the penalties imposed are either civil in nature or involve imprisonment of less than a year (e.g. the *Marine Mammal Protection of 1990*, the *Coast Conservation Act of 1988 and Fisheries Act*). The penalty for smuggling under the *Import Duties Act of 1989* is imprisonment of not more than one (1) year and would therefore not qualify as a serious offence under RMI law.

*Extraterritorially Committed Predicate Offences (c. 1.5):*

167. As stated above, ML predicate offences consist of all serious offences under RMI law and those of foreign States, which, had they occurred in the RMI, would constitute an offence penalized with a maximum penalty of imprisonment or deprivation of liberty for a period of not less than 12 months (section 102(dd), *Banking Act* ). In other words, a criminal offence committed overseas would also qualify as a predicate offence as long as it would constitute a serious offence in the RMI.

*Laundering One's Own Illicit Funds (c. 1.6):*

168. The AML provisions of the *Banking Act* do not specify whether the ML offence extends to persons who have committed both the ML and predicate offences. There is no fundamental principle of law in the RMI that would prevent the ML offence to include self laundering.

*Ancillary Offences (c. 1.7):*

169. Under section. 166 (b) of the *Banking Act*:

“any person who, knowing or having reason to believe that such property is the proceeds of crime, **renders assistance to another person** for (i) the conversion or transfer of property, with the aim of concealing or disguising the illicit origin of that property, or of aiding any person involved in the commission of the offense to evade the legal consequences thereof; and (ii) concealing or disguising the true nature, origin, location, disposition, movement or ownership of the property, can be charged with money laundering.”

170. There is neither a definition of “render assistance” in the *Banking Act* nor in the *Criminal Code*.

171. Section 104 of the *Criminal Code* defines *accessories* as

“every person who, knowing that an offense against the Republic has been committed, receives, relieves, comforts, or assists the offender in order to hinder or prevent his apprehension, trial, or punishment, is an accessory after the fact. An accessory after the fact shall be imprisoned not more than one half (½) the maximum term of imprisonment or fined not more than one-half (½) the maximum fine prescribed for punishment of the principal, or both; or if the principal is punishable by life imprisonment, the accessory shall be imprisoned not more than ten (10) years.”

172. Section 105 (5) of the RMI *Criminal Code* covers aiding the conduct of a crime. It provides that

“a person who engages in conduct designed to aid another to commit a crime, is guilty of an attempt to commit the crime, although the crime is not committed or attempted by such other person”. Moreover, section 105 (1) covers attempting to commit a crime, providing that, “where no separate provision is made by law for punishment upon conviction of such attempt, a person so convicted shall be punished with imprisonment for a term not exceeding one-half (1/2) of the maximum term of imprisonment which may lawfully be imposed upon conviction for commission of the offense attempted,... ”

173. Conspiracy, under section 120 of the *Criminal Code*, is a serious offence and thus qualifies as a predicate offence to ML. It exists

“If two or more persons conspire, either to commit any crime against the Republic, or to defraud the Republic in any manner or for any purpose, and one or more of such parties do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be guilty of conspiracy and shall upon conviction be liable to a fine not exceeding \$2,000 or to a term of imprisonment not exceeding five (5) years, or both. If, however, the offense, the commission of which is the object of conspiracy, is a misdemeanor only, the punishment for such conspiracy shall not exceed the maximum penalty provided for such misdemeanor”.

174. The *Banking Act* uses “offence” but the *Criminal Code*, as highlighted above, uses both “offence” and “crime”. Section 102 of the *Criminal Codes* provides detailed definitions with offence and crime being interchangeable with felonies, misdemeanours or petty misdemeanours, except an offence can also be subject to a fine, forfeiture or other civil penalty, either in the code or any other statute.

*Additional Element—If an act overseas which do not constitute an offence overseas, but would be a predicate offence if occurred domestically, lead to an offence of ML (c. 1.8):*

175. This additional element does not apply to the RMI because of the dual criminality being observed in regard to predicate or serious offences (Please see discussion under c.1.3 above)

*Liability of Natural Persons (c. 2.1):*

176. ML under the *Banking Act* may be committed either by a natural or legal person. In order to be convicted of ML under section 166 of the *Banking Act*, a perpetrator must have *knowledge* or *has reason to believe*, that the laundered property is proceeds of crime.

*The Mental Element of the ML Offence (c. 2.2):*

177. The ML offence at section 166 of the *Banking Act* appears to be constructed to allow the mental element to be inferred from objective circumstances. According to RMI authorities, it is a fundamental principle of the RMI criminal law that the intentional element of any crime may be inferred from objective factual circumstances. Being a common law jurisdiction, the assessment team was informed that case laws of other common law jurisdictions are applicable to RMI. However, this principle was not expressly provided under the law nor was there any case law presented showing that application of such a fundamental principle. The OAG confirms that there is no case law dealing with objective evidence rule for any offence in the *Criminal Code*.

*Liability of Legal Persons (c. 2.3 )*

178. Criminal liability for ML also extends to legal persons in the RMI. Section 103 (9) of the *Criminal Code* defines “person” to include “a corporation or an unincorporated association”.

179. Section 166(2) of the *Banking Act* states that “Where a person is convicted of any of the offenses specified in Subsection (1), in the case of a natural person, such person shall be liable to imprisonment for a term of imprisonment not exceeding twenty (20) years or a fine not exceeding \$2,000,000, or both, and in the case of a body corporate five (5) times such a fine or double the amount of money involved in the offense scheme, whichever is greater.”

180. However, neither the *Criminal Code*’s definition nor the *Banking Act*’s definition covers all categories of legal persons defined in the FATF methodology, namely, “bodies corporate, foundation, anstalt, partnerships, or associations, or similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property”.

*Liability of Legal Persons should not preclude possible parallel criminal, civil or administrative proceedings & c. 2.4):*

181. There are no specific provisions that prohibit the possible parallel criminal, civil or administrative proceedings. Under section 113 (m) of the *Banking Act*, the Banking Commissioner is authorized to revoke the licence of a bank, whenever there are reasonable grounds to believe that ML activities are taking place. It would appear that this sanction is in addition to the criminal sanctions under section 166, *Banking Act*. Further, section 181 of the *Banking Act*, provides that

“in addition to any criminal penalties or fines authorized by Part XIII of the *Banking Act*, 1987, each financial institution and cash dealer, and any partner, director, officer, employee, or person participating in the conduct of the affairs of the financial institution or cash dealer who violates any provision of Part XIII, or any regulation promulgated by the Banking Commissioner implementing any provision of Part XIII shall be liable for a civil money penalty of not more than \$10,000 per violation.”

*Sanctions for ML (c. 2.5):*

182. Section 166(2) of the *Banking Act* states that, “Where a person is convicted of any of the offenses specified in Subsection (1), in the case of a natural person, such person shall be liable to imprisonment for a term of imprisonment not exceeding twenty (20) years or a fine not exceeding \$2,000,000, or both, and in the case of a body corporate five (5) times such a fine or double the amount of money involved in the offense scheme, whichever is greater.”

183. Additionally, pursuant to section 113 of the *Banking Act*, “(1) In the case of a licensed bank...(m) where the Commissioner is satisfied that there are reasonable grounds to believe that money laundering activity is taking place the Commissioner may, with the approval of the Cabinet, by notice given in writing, suspend the license and require the bank to show cause why the license should not be revoked or varied; or revoke the license”.

184. The *Banking Act* penalty (imprisonment for a term not exceeding 20 years) is more severe than the penalties for serious offences in the *Criminal Code* which range from 5 to 10 years maximum imprisonment. As regards legal persons, the amount of fine is US\$10 million or double the amount involved in the ML offence which is a considerable and significant amount. Unfortunately, the effectiveness and dissuasive effect of the existing ML laws could not be measured at the time of the on-site due to the lack of ML investigations, prosecutions, or convictions.

### ***Statistics and effectiveness***

185. While the RMI authorities maintain relevant statistics on criminal investigations, prosecutions and convictions, only two (2) ML investigations have been undertaken, but no prosecutions have been carried out notwithstanding the fact that ML laws have been introduced into the *Banking Act* since 2000 and 2002.

186. Based on its 2009 statistics, there were certain serious (predicate) offences that were investigated and prosecuted (e.g. grand larceny, burglary and forgery) that could have led to ML investigations and possible prosecution. The assessment team has observed that further investigation of these predicate offences for possible ML often stops once the conviction for the predicate offence has been secured. Moreover, the agency charged with prosecution of offences, the OAG, has a limited number of personnel and most are fairly new. This may account for absence or lack of ML statistics. The other factor may have stemmed from the view by some authorities that ML is a transnational crime rather than a domestic concern.

187. There have been no investigations or prosecutions of ML offences in the RMI which involved legal persons incorporated in the RMI’s offshore registry.

### **2.1.2. Recommendations and Comments**

188. While some of the provisions of the *Banking Act* comply with requirements under the FATF Recommendations, there are deficiencies and ambiguities which need to be remedied. They are the following:

#### **Recommendation 1**

- Amend the *Banking Act* to (a) remove the reference to “render assistance” in Section 166 (b); and (b) specifically cover “self-laundering”.
- Include comprehensive offences against each designated category of predicate offences, including by:

- Enacting legislation that would criminalize piracy of products, human trafficking, migrant smuggling, insider trading and market manipulation with penalties that would qualify them to be predicate offences to ML; and
  - Amending the existing customs and environmental law by providing for penalties that would qualify them to be serious offences and thus be predicate offences to ML.
- The authorities should develop a strategy to build expertise and undertake ML investigation and prosecution, with an initial focus on simpler cases of potential ML, proceeds of crime and taxation related violations (see related recommendation under R.27).

## Recommendation 2

- Amend the definition of legal persons to include the full range as defined in the methodology.

### 2.1.3. Compliance with Recommendations 1 & 2

	Rating	Summary of factors underlying rating
<b>R.1</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• The definition of ML is not fully in accord with the Vienna and Palermo Conventions.</li> <li>• The definition of “serious offence” does not cover the entire FATF designated list of offences.</li> <li>• Offences such as piracy of products, human trafficking and migrant smuggling, market manipulation and insider trading, smuggling and certain environmental crimes are not included.</li> <li>• Doubts exists as to whether self-laundering is allowed.</li> <li>• Lack of effective implementation.</li> </ul>
<b>R.2</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• The scope of criminal liability for legal persons is limited to bodies corporate and does not include the full range of legal persons as defined in the Methodology</li> <li>• Lack of effective implementation</li> </ul>

## 2.2. Criminalization of Terrorist Financing (SR.II)

### 2.2.1. Description and Analysis

#### *Legal Framework:*

189. The financing of terrorism is criminalized in section 120 of the Counter-Terrorism Act, 2002 (“CTA”). The RMI has signed and ratified the UN Convention for the Suppression of the Financing of Terrorism as well as all 12 international conventions and protocols relating to the fight against terrorism. Additionally, pursuant to section 104(5)

*“application of any provisions of (the CTA), relating or implementing the provisions of any international terrorism convention or protocol, shall conform to and meet the requirements of the particular convention or protocol, and shall be subject to the exclusions and jurisdictional requirements contained therein.”*

#### *Criminalization of Financing of Terrorism (c. II.1):*

190. Under section 105 of the CTA, the terms “terrorist” (37), “terrorism”(35), “terrorism offense”(36) and “terrorist act” (38) and “terrorist organization” (39) are defined as follows:

- *"terrorist"* means a person who engages in terrorism.
- *"terrorism"* means and includes terrorism offences and terrorist acts;
- *"terrorism offense"* means:
  - (a) *any crime established by this Act;*
  - (b) *any crime established by the laws of the Marshall Islands and declared to be a terrorism offense by the Nitijela;*
  - (c) *any crime established by an international terrorism convention;*
  - (d) *any crime recognized under international humanitarian law as a terrorism offense; and*
  - (e) *any crime established under the law of a foreign State, where such crime, if committed in the Marshall Islands, would constitute a terrorism offense under the laws of the Marshall Islands*
- *"terrorist act"* means and includes any act that is intended, or by its nature or context can be reasonably regarded as intended, to intimidate the public or any portion of the public, or to compel a government or an international or regional organization to do or refrain from doing any act, and:
  - (a) *involves the seizing or detaining, and threatening to kill, injure, harm, or continue to detain, another person;*
  - (b) *endangers the life of any person;*
  - (c) *creates a risk to the health or the safety of the public, or to any portion of the public;*
  - (d) *endangers the national security or national defense of any country;*
  - (e) *involves substantial damage to property;*
  - (f) *involves the hijacking, seizure or sabotage of any conveyance (including an aircraft, vessel, ship, or vehicle), or of any fixed platform attached to the continental shelf;*
  - (g) *involves any act that is designed to disrupt or destroy an electronic system, including, without limitation:*
    - (i) *an information system;*

- (ii) a telecommunications system;*
- (iii) a financial system;*
- (iv) a system used for the delivery of essential government services;*
- (v) a system used for, or by, an essential public utility;*
- (vi) a system used for, or by, a transport system;*

*(h) involves any act that is designed to disrupt the provision of essential emergency services such as the police, civil defense and medical services;*

- “terrorist organization” means a group composed of two or more persons, whether organized or not, that engages in terrorism.

191. Terrorism financing is criminalized under section 120 of the CTA which provides that:

*“(1) Any person who knowingly, by any means, directly or indirectly, solicits, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part:*

- (a) for terrorism;*
- (b) for the benefit of persons who engage in terrorism, or for the benefit of entities owned or controlled, directly or indirectly, by persons who engage in terrorism; or*
- (c) for the benefit of persons and entities acting on behalf of or at the direction of any person referred to in subsection 1(b); commits a crime punishable by the penalties established by section 107 (1) (a) of this Act.*

*(2) For an act to constitute an offense under this section it shall not be necessary that the funds were actually used to commit or carry out a terrorism offense, or terrorist act.*

*(3) Citizens and nationals of the Marshall Islands and any persons or entities within the Marshall Islands are prohibited from making any funds, financial assets or economic resources or financial or other related services available, directly, or indirectly, to any person referred to in subsection 1(b) or 1(c).”*

192. Section 120 (1) above is substantially similar to Article 2 (1) of the FT Convention. Instead of the phrase “unlawfully and willfully” found in the FT Convention, the CTA used the term “knowingly” which, RMI authorities stated, requires a much lower degree of proof.

193. Section 120 (2), on the other hand, is a modified version of Article 2 (3) of the FT Convention. However, the provision does not cover “attempts” as required under criteria.II.1.d of SR II.

194. The term “terrorism” has a wide coverage which includes terrorism offence and terrorist acts as defined in section 105(36) and 105(38) and substantially covers the requirements under Article 2 (a) and (b) of the FT Convention.

195. Section 105(13) of the CTA defines “funds” as “property or assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments

of any form, including electronic or digital, evidencing title to, or interest in, such property or assets, including, but not limited to, bank credits, travelers checks, bank checks, money orders, shares, securities, bonds, debt instruments, drafts, letters of credit, and currency.” The term “funds” under the CTA is a near verbatim copy of Article 1(1) of the FT Convention. Section 105 added property, debt instruments and currency to the CTA’s definition of the term “funds”.

196. Section 106 (CTA) provides that “any person who knowingly, directly or indirectly, engages in terrorist act is guilty of an offence against this Act, and shall unless otherwise punishable under any other section be punishable, under section 107 of this Act”. The criminal penalties provided under section 107 (1) include imprisonment of not less than 30 years and a fine of not more than \$100,000,000.00, or both”.

197. Under section 107 (3), a person commits a crime, punishable under subsection (1) of section 107(1), if that person knowingly:

- (a) attempts, conspires, or threatens to commit;
- (b) participates as an accomplice in;
- (c) organizes or directs others to commit;
- (d) contributes to the commission of; any crime established (under the CTA).

198. Section 107 (3) essentially follows Article 2 (5) of the FT Convention, although there is a deficiency in the definition of “attempts” as highlighted earlier.

*Predicate Offence for Money Laundering (c. II.2):*

199. Under the *Banking Act*, a “serious offense” is an offence that carries with it imprisonment of not less than 12 months. All serious offences are predicate offences to ML. Considering that the penalty for the financing of terrorism in RMI is imprisonment for not less than 30 years, FT is therefore a predicate offence to ML.

*Jurisdiction for Terrorist Financing Offence (c. II.3):*

200. The jurisdictional application of the provisions of the CTA are provided under section 104 (2) and (3), thus:

- (2) *This Act shall apply in respect of any crime established by this Act when the offense is committed:*
  - (a) *in the Marshall Islands;*
  - (b) *by a citizen of the Marshall Islands;*
  - (c) *on board an aircraft or ship:*
    - (i) *registered under the laws of the Marshall Islands at the time the offense was committed;*
    - (ii) *operating under or flying the Marshall Islands flag;*
    - (iii) *which lands in the territory of the Marshall Islands with the alleged offender on board;*
    - (iv) *leased or chartered without a crew to a lessee who has his principal place of business in the Marshall Islands, or who is a habitual resident of the Marshall Islands;*
  - (d) *against or on board a fixed platform while it is located on the Marshall Islands’ continental shelf;*

(3) *This Act shall apply in respect of any crime established by this Act when the offense:*

- (a) was directed toward or resulted in the carrying out of a crime against a citizen of the Marshall Islands, or during the commission of which a citizen of the Marshall Islands was threatened, injured or killed;*
- (b) was directed towards or resulted in the carrying out of a crime against the government of the Marshall Islands or a facility, diplomatic or consular premises of the government of the Marshall Islands abroad;*
- (c) was directed towards or resulted in a crime committed in an attempt to compel the Marshall Islands to do or abstain from doing any act;*
- (d) was committed by a stateless person who has his or her habitual residence in the Marshall Islands.*

201. The aforementioned provisions under section 104 would seem to suggest that RMI authorities, specifically the Attorney General (under section 104 (1)), can enforce the FT provisions and other violations of the CTA under section 104 (2) whenever the offence is: a) committed by its citizens; or b) committed within the territory of the RMI; and under section 104 (3), whenever the offence is directed against i) a citizen of RMI; and ii) its government, even if the offence is committed outside of territorial jurisdiction of RMI.

*The Mental Element of the FT Offence (applying c. 2.2 in R.2):*

202. As with ML, there is neither an express legal provision nor case law that would show that the intentional element of any crime may be inferred from objective factual circumstances. This is the same issue as highlighted under the analysis of ML offence above.

*Liability of Legal Persons (applying c. 2.3 & c. 2.4 in R.2):*

203. Section 105(23) of the CTA defines “person” to include both natural and legal persons and any foreign government or nation or any agency, instrumentality or political subdivision of any such government or nation, whether or not it is engaging in legal activities or is operating legally and in a lawful manner (section 105 [23]).

204. The provisions on the liability of corporations and other legal persons are found under section 109 which reads:

- (1) Legal persons, including any foreign government or nation or any agency, instrumentality or political subdivision of any such government or nation, shall be liable in the same manner and to the same extent as any natural person for any terrorism offense.*
- (2) The maximum assessable fine for legal persons shall be increased by ten times the amount assessable in the case of a natural person.*
- (3) Where in proceedings for a violation of this Act it is necessary to establish the state of mind of a corporation or other legal person, it is sufficient to show that a director, officer or agent who engaged in the conduct within the scope of his or her actual or apparent authority had that state of mind*
- (4) Any conduct engaged in by:*
  - (a) a director, officer or agent of a corporation or other legal person within the scope of his or her actual or apparent authority; or*

*(b) any other person at the direction or with the consent or agreement (whether express or implied) of a director, officer or agent of the corporation or legal person, where the giving of such direction, consent or agreement is within the scope of the actual or apparent authority of the director, officer or agent; shall be deemed, for the purposes of this Act, to have also been engaged in by the corporation or legal person.*

*Sanctions for FT (applying c. 2.5 in R.2):*

205. Criminal penalties for violations of the provisions of the CTA are generally found under section 107 (1), (2) and (6) which read:

*(1) Unless otherwise provided, any person convicted of an offence against this Act;*

*(a) shall, where no other punishment is prescribed in respect of that offense, be punishable by a term of not less than 30 years and not more than life imprisonment, or a fine of not more than \$100,000,000.00; or both.*

*(b) shall not be entitled to probation for an offense committed or have the term of imprisonment imposed on him run concurrently with any other term of imprisonment; and*

*(c) shall not be entitled to bail pending his trial or his appeal against conviction for the offense.*

*(2) In lieu of the amount of the fine otherwise authorized by this Act, and in addition to any term of imprisonment, a defendant who derived profits or other proceeds from a crime established by this Act may be liable to a fine of not more than twice the gross profits or other proceeds, where the profits or proceeds from the offense exceed the maximum assessable fine*

*x x x*

*(6) The court, in imposing sentence on any person convicted of a terrorism offense, shall order, in addition to any other sentence imposed, that the person forfeit to the Marshall Islands all property described in section 108.*

206. As stated in section 9 above, legal persons shall be liable in the same manner and to the same extent as a natural person for any terrorism offence. Moreover, the amount of accessible fine (maximum of US\$100 million) applicable to natural persons shall be increased ten fold whenever the offender happens to be a legal person.

## **Effectiveness**

207. RMI has a generally low risk for FT, and the RMI has conducted neither an investigation nor prosecution relating to FT. The absence or lack of FT-related investigation/prosecution made it difficult for the assessment team to assess the effectiveness of the law and the sanctions it imposes on would-be offenders.

### 2.2.2. Recommendations and Comments

208. According to RMI authorities, RMI has a very small and geographically isolated financial centre which, due to its restrictive nature, does not lend itself to FT. While there are sufficient provisions under the CTA which will enable RMI to respond to (and prevent) FT, it is recommended that the RMI conducts a FT risk assessment as part of a national AML/CFT assessment, and amend the definition of “attempts” to be consistent with the FT Convention.

### 2.2.3. Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II	LC	<ul style="list-style-type: none"> <li>The definition of “attempts” is not fully consistent with the FT Convention.</li> <li>While offences meet all the essential criteria of SR II, there is as yet no basis to evaluate the effectiveness of the implementation.</li> </ul>

## 2.3. Confiscation, freezing and seizing of proceeds of crime (R.3)

### 2.3.1. Description and Analysis

#### *Legal Framework:*

209. The confiscation regime of the RMI is covered by sections 167(l) and 171-175 of the *Banking Act*, sections 108, 113, 122 of the CTA and sections 216–226, 237-245, 251-252, 257, and 262 of the *Proceeds of Crime Act* (“POCA”). The confiscation measures under the *Banking Act*, CTA and POCA are all conviction based. The RMI has no civil forfeiture regime.

210. It was noted that the *Banking Act* and POCA have similar but not identical provisions on “property”, “tainted property” and “proceeds”. It would appear that insofar as confiscation is concerned, the POCA, being a law of general application, would apply to all serious offences except ML which is specifically covered by the *Banking Act*.

#### *Confiscation of Property (c. 3.1):*

211. For an order of confiscation to be issued under the *Banking Act* and POCA, the High Court of RMI must be satisfied that the property subject of the confiscation is “*tainted property*”. Moreover, an application for a confiscation order must be filed with the High Court: Under the *Banking Act*, within six (6) months after conviction; and, under the POCA, within one (1) year from date of conviction.

212. “Tainted property” is defined under section 102 (ff) of the *Banking Act* and under section 205 (1) (p) of the POCA. Under the *Banking Act* “tainted property” is defined as “*any property obtained in whole or in part from the proceeds of a criminal offense or from proceeds of money laundering.*”

213. On the other hand, the POCA defines “tainted property” as “(i) *property used in, in connection with, the commission of a serious offense; or (ii) proceeds of crime*”. “Property” under the POCA is defined as “*currency and all other real or personal property of every description, whether situated in the Republic of the Marshall Islands or elsewhere and whether tangible or intangible, and includes an interest in any such property (section 205 (1) (l), POCA).*”

214. Further, under section 205 (1), (k) of the POCA, “proceeds of crime” is defined as *“fruits of a crime, or any property derived or realized directly or indirectly from a serious offense and includes, on a proportional basis, property into which any property derived or realized directly from the offense was later successfully converted, transformed, intermingled, as well as income, capital or other economic gains derived or realized from such property at any time since the offense.”*

215. For the definition of “proceeds” and “property” under the *Banking Act*, please refer to the discussions under c.1.2.

216. As discussed under Recommendation 1, there are a number of categories of predicate offences which are not criminalised in the RMI. The application of proceeds of crime powers under the POCA would not be available to confiscate property for those categories of predicate offences.

217. “Tainted property” in the POCA and *Banking Act*, with one exception, does not include those instrumentalities intended for use in the commission of ML or other predicate offences. The exception, under section 171 of the *Banking Act*, it appears that with respect to currency exported out or imported into the RMI, the Commissioner or Attorney General may detain or seize such currency whenever there is a reasonable ground to suspect that such currency is (i) property derived from a serious offence; or (ii) **intended by any person for use in the commission of a serious offence** (emphasis supplied). Said currency, while detained, shall not be released where an application for a confiscation order has been filed (section 171 (5), (a), *Banking Act*).

218. The provisions of the *Banking Act* (section 176) and POCA (section 227) allow payment instead of a confiscation order whenever such a confiscation order cannot be made because the subject property or any interest therein:

- “(1) cannot, on the exercise of due diligence be located;*
  - (2) has been transferred to a third party in circumstances which do not give rise to a reasonable inference that the title or interest was transferred for the purpose of avoiding the confiscation of the property;*
  - (3) is located outside the Republic of the Marshall Islands;*
  - (4) has been substantially diminished in value or rendered worthless; or*
  - (5) has been commingled with other property that cannot be divided without difficulty;*
- the High Court may, instead of ordering the property or part thereof or interest therein to be confiscated, order the person to pay to the Republic of the Marshall Islands an amount equal to the value of the property, part or interest ...”*

*Provisional Measures to Prevent Dealing in Property subject to Confiscation (c. 3.2):*

219. Under sections 237 and 238 of the POCA, the Attorney General may *ex parte* apply to the High Court for a restraining order prohibiting a defendant or any person from disposing of, or otherwise dealing with, the property or such part thereof or interest therein as specified in the restraining order, except in such manner specified in said order (section 238 (1)(f) POCA).

220. A “defendant”, for purposes of sections 237 and 238 is a *“person charged or about to be charged with a serious offense, whether or not he or she has been convicted of the offense”*. Moreover, a restraining order will be issued by the High Court when it is satisfied that there is a reasonable ground to believe that: i) the defendant committed a serious offence (conviction is not a requisite); ii) the property is tainted; and iii) defendant benefited from the offence, directly or indirectly. When the restraining order is directed against property of a person other than the

defendant, the restraining order will, nonetheless, be issued based on reasonable grounds to believe that the subject property is tainted and subject to the defendant's effective control. A "person" may either be a natural or legal person (section 205 (1)(i), POCA).

221. Property, under the POCA, will be deemed "tainted property" if the same is i) used in, or in connection with, the commission of a serious offence; or ii) proceeds of crime (section 205 (1)(p), POCA). "Proceeds of crime", on the other hand, is defined as fruits of a crime, or any property derived or realized directly or indirectly from a serious offence and includes, on a proportional basis, property into which any property derived or realized directly from the offence was later successively converted, transformed or intermingled, as well as income, capital or other economic gains derived or realized from such property at any time since the offence (section 205 (1)(k), POCA).

222. Violation of a restraining order is penalized with imprisonment for a maximum period of five years or a maximum fine of US\$50,000.00, or both. In case the violator is a corporation or legal person the maximum fine is US\$250,000.00 (section 242, POCA).

223. A restraining order remains in force until; i) it is discharged, revoked or modified; ii) the period of six (6) months from the date on which it is made or such later time as the High Court may determine; or a confiscation order or a pecuniary penalty order, as the case may be, is made in respect of property, which is the subject of a restraining order (section 243, POCA).

224. Under section 167 (1) of the *Banking Act*, the Banking Commissioner may apply for a warrant authorizing, among others, the removal of any document, material or other things within the premises of a financial institution, cash dealer or officer or employee thereof for the purpose of preventing ML activities. Trust and company service providers are not included in the definition and records of offshore companies would not be subject to such a warrant. Moreover, the Commissioner or Attorney General, under section 171 of the *Banking Act*, may seize and detain any currency that is being imported into or exported from RMI if there are reasonable grounds to suspect that such currency is (i) property derived from a serious offence; or (ii) intended by any person for use in the commission of a serious offence.

225. Section 108 and 122 of the CTA set out provisional measures in relation to terrorism. Section 108 of the CTA reads, in part:

*"(3) For the purposes of forfeiture proceedings under this section, a temporary restraining order and seizure warrant may be entered upon application of the Attorney-General without notice or opportunity for a hearing when an information or complaint has not yet been filed with respect to the property, where there is probable cause to believe that the property with respect to which the order is sought would, in the event of conviction, be subject to forfeiture under this section and exigent circumstances exist that place the life or health of any person in danger...."*

226. Further, under section 122 of the CTA

*"(1) Any law enforcement officer or customs official of the Marshall Islands may seize and in accordance with this section detain, any funds, that the officer or official has probable cause to believe were derived from or intended for terrorism, including, without limitation, funds being imported into or exported from the Marshall Islands. (2) Funds of, or intended for, terrorist organizations shall be frozen, seized, and in accordance with this section, detained, where the organization has been designated as a terrorist organization by the United Nations Security Council, or by the Minister pursuant to regulations promulgated pursuant to this*

*Act, or where there is probable cause to believe that the entity involved is a terrorist organization....”*

*Ex Parte Application for Provisional Measures (c. 3.3):*

227. The Attorney General, under section 237 of the POCA may apply to the High Court for a restraining order against any covered property whether held by a defendant or held by a person other than a defendant. An application for a restraining order may be made *ex parte* and shall be in writing.

228. Although the application is made *ex parte*, the High Court, before entering a restraining order, may require notice to be given to, or may hear, any person who, in the opinion of the High Court, appears to have an interest in the property, unless the Court is of the opinion that giving such notice before making the order would result in the disappearance, dissipation or reduction in value of the property subject of the application (section 239, POCA).

229. Application for search warrants can be made under sections 251–257 of the POCA in respect of searching a person or premises for tainted property and seizing such property. Where there is reason for urgency, applications can be made by telephone, radio communication or facsimile under section 253. Section 254 authorizes the police officer to carry out a search and seize property without warrant in emergency situations i.e. that “*the circumstances are so urgent that they require immediate exercise of the power without the authority of a warrant or the order of a court*”.

230. A police officer can also apply for a warrant under section 263, to enter onto any land or premises to search for and seize any documents identifying, locating or quantifying the defendant’s property.

*Identification and Tracing of Property subject to Confiscation (c. 3.4):*

231. Authorities, including police officers, are amply empowered to identify, trace and even seize tainted property. The Banking Commissioner has comprehensive powers to assist in identifying and tracing property. Under section 167 the Banking Commissioner has the following powers:

- *to enter the premises of any financial institution or cash dealer during ordinary business hours to inspect any record, make notes and take copies of the whole or any part of the record;*
- *to request additional information where he has reasonable grounds to believe that such information is essential to discovering ML activity;*
- *to apply for a warrant to enter any premises belonging to or in the possession or control of a financial institution, cash dealer, or any officer or employee thereof, and to search the premises and remove any documents, materials, or other things therein for the purposes of preventing ML activity, as so ordered by the High Court and specified in the warrant.*

232. The Attorney General also has powers under section 609 of the Office of the Attorney-General Act 2002, to summon individuals or entities to appear, testify and/or produce for examination any books, papers, documents, records, data or objects which the Attorney-General deems relevant or material to the inquiry.

233. Under section 251 of the POCA, a police officer may conduct a search on person, enter upon land or premises in search of tainted property and seize such property found in the course of the search. This search (and seizure) may be effected either with the consent of the person to be searched

or occupier of the land/premises as the case may be; or by virtue of a warrant under section 252 or in cases of emergencies as authorized under section 254.

*Protection of Bona Fide Third Parties (c. 3.5):*

234. Rights of third parties are protected under various provisions of the POCA. Section 217 requires the Attorney General when applying for a confiscation or pecuniary penalty order to give no less than 14 days notice to any person who may have an interest in the property and such person may appear and adduce evidence in the hearing.

235. Pursuant to section 225, a person who claims an interest in the property being the subject of a confiscation order, may apply to the High Court, before the confiscation order is made, for an order in respect of that property. If the Court is satisfied that:

- *the person was not in any way involved in the commission of the offense; and*
- *where the person acquired the interest during or after the commission of the offense, that he or she acquired the interest for sufficient consideration and without knowing, and in circumstances such as not to arouse reasonable suspicion, that the*
- *property was, at the time he or she acquired it, tainted property;*
- *the Court shall make an order declaring the nature, extent and value of the person's interest.*

236. If the confiscation order has already been made, a person claiming interest may before the end of 12 months from the day the confiscation order was made, apply to the Court for an order. In both these circumstances, the applicant is required to give the Attorney General 14 days notice. A receiver or fiduciary appointed under section 48 shall on application by any person who has obtained an order under section 25, direct that the property or the interest to which the applicant relates, be returned to the applicant or direct that an amount equal to the value of the interest be paid to the applicant.

237. Before entering a restraining order, under section 239 the High Court may require notice to be given to any person who appears to have an interest in the property unless the Court is of the opinion that such notice before making the order would result in the disappearance, dissipation or reduction in value of the property.

*Power to Void Actions (c. 3.6):*

238. Pursuant to section 224 of the POCA, the High Court may before making a confiscation order and in the case of property in respect of which a restraining order was made and served, set aside any conveyance or transfer of the property that occurred after the seizure of the property or the service of the restraining order, unless the conveyance or transfer was made for valuable consideration to a person acting in good faith and without notice.

*Additional Elements (Rec 3)—Provision for a) Confiscation of assets from organizations principally criminal in nature; b) Civil forfeiture; and, c) Confiscation of Property which Reverses Burden of Proof (c. 3.7):*

239. There are no provisions for the confiscation of assets of organized criminal groups. RMI's closest concept to an organized criminal group is "conspiracy", is a serious offence under section 120 of the *Criminal Code*. It exists "If two or more persons conspire, either to commit any crime against

*the Republic, or to defraud the Republic in any manner or for any purpose, and one or more of such parties do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be guilty of conspiracy...*” As a serious offence, any tainted property related to the conspiracy shall be covered by the confiscation provisions of the POCA but it requires the commission of a criminal act pursuant to the conspiracy.

240. There is no civil forfeiture regime in RMI.

241. Under section 222 (2) of the POCA, in determining whether property is tainted or not, the High Court may presume, in the absence of contrary evidence:

*(a) that the property was used in or in connection with the commission of the offense if it was in the person’s possession at the time of, or immediately after the commission of the offense for which the person was convicted;*

*(b) that the property was derived, obtained or realized as a result of the commission of the offense if it was acquired by the person before, during or within a reasonable time after the period of the commission of the offense of which the person was convicted, and the High Court is satisfied that the income of that person from sources unrelated to criminal activity of that person cannot reasonably account for the acquisition of that property.*

### **Statistics and effectiveness**

242. While the RMI authorities maintain relevant statistics on criminal investigations, prosecutions and convictions, no statistics were available in relation to property frozen under the POCA.

### **2.3.2. Recommendations and Comments**

243. Effectiveness of the confiscation provisions cannot be measured due to the absence of relevant statistics. During the meetings with the legal authorities and law enforcement agencies, the assessment team was informed that most of the charges brought before the prosecutors and the courts have been the subject of plea bargaining, which is allowed under the *Criminal Code*. This may account as one of the reasons for the absence of data on confiscation.

244. RMI should fully implement R3 by undertaking the following:

- Amend both the POCA, and *Banking Act* to ensure that “tainted property” covers instrumentalities intended for use in the commission of any ML, FT or other predicate offences and is the same in both Acts.
- Ensure that provisional measures and confiscation applies to property of corresponding value.

### **2.3.3. Compliance with Recommendation 3**

	Rating	Summary of factors underlying rating
<b>R.3</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• The term “tainted property” does not cover instrumentalities intended for use in the commission of any ML, FT or other predicate offences, and property of corresponding value.</li> <li>• Lack of effective implementation.</li> </ul>

## 2.4. Freezing of funds used for terrorist financing (SR.III)

### 2.4.1. Description and Analysis

#### *Legal Framework:*

245. Sections 108, 113, and 122 of the *Counter Terrorism Act* (CTA) concerns the freezing, seizure and confiscation of funds associated with any terrorism offence.

246. Section 113(5) of the CTA authorizes the Attorney General to take appropriate measures, in accordance with the Constitution and the laws of the Marshall Islands “...to identify, detect, freeze, seize, and obtain forfeiture of any funds used or allocated for the purpose of committing any terrorism offense as well as the proceeds derived from such offenses”.

247. Section 122, any law enforcement officer or customs official of the Marshall Islands (1) “may seize and detain any funds, that the officer or official has probable cause to believe were derived from or intended for terrorism, including, without limitation, funds being imported into or exported from the Marshall Islands. (2) Funds of, or intended for, terrorist organizations shall be frozen, seized, and in accordance with this section detained, where the organization has been designated as a terrorist organization by the United Nations Security Council, or by the Minister pursuant to regulations promulgated pursuant to this Act, or where there is probable cause to believe that the entity involved is a terrorist organization”.

248. Section 122 authorizes the seizure and detention of terrorist funds but does not provide how the seizure and detention will be actually implemented.

249. The seizure and detention under the foregoing sections cover “funds” which are defined under the section 105 (13) of the CTA to mean “property and assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such property or assets, including, but not limited to, bank credits, travelers checks, bank checks, money orders, shares, securities, bonds, debt instruments, drafts, letters of credit, and currency”, and is in accord with the FT Convention’s definition of funds. Such seizure and detention is effected only by law enforcement or customs official. Judicial intervention would only come in for purposes of determining the justification for the continued detention of the subject funds (section 122(3)-(7)).

#### *Freezing Assets under S/Res/1267 (c.III. 1) and 1373 (c. III.2):*

250. The provisions contained in the CTA, specifically in section 122, are meant to address the requirements of UNSCR 1267. The RMI has taken the option of empowering law enforcement and the High Court to administer and enforce freezing actions, rather than enacting supplementary legislation or regulation that places responsibility for freezing the funds or other assets of designated persons (UNSCR 1267 or otherwise) on the person or entity holding the funds or other assets (e.g. financial institutions and cash dealers) and subjecting them to sanctions for non-compliance.

251. Section 122 (2) of the CTA authorizes the funds of, or intended for, terrorist organizations as designated by the UN Security Council, to be frozen and seized. However, section 122 does not include individual terrorists. Further, there is no definition of “frozen” or “seized” or “seizure” in the CTA, although there is a definition of funds as noted earlier, in section 105(13). However, in the context of section 122 of the CTA, seizure has the same intended effect as to prohibit the transfer, conversion, disposition or movement of funds i.e. freeze.

252. The period of detention of funds after seizure under section 122 (1)-(2) is no more than 48 hours but may be extended by the High Court, upon valid grounds and with due hearing for maximum period of two years. However, the maximum period of detention is 2 years as stated under section 122 (4), which is not consistent with the requirement of UNSCR 1267 for freezing indefinitely or until the finalization of some investigation or review process.

253. There has been no instance where sections 122 and 108 (3) have been utilized as there has been no terrorism or FT-related investigation made as of the time of the on-site.

254. The assessment team asked both the Attorney General and Chief Justice how the RMI would use its powers under section 122 to give effect to UNSCR 1267 obligations. While RMI authorities indicated the powers are available under the CTA, they acknowledged the lack of clear procedures would make it difficult to achieve the desired freezing without delay required under UNSCR 1267, should circumstances warrant such an action.

255. The Attorney General and High Court also mentioned the possible use of restraining orders. However, restraining orders are governed by the POCA. They are issued against the covered property held by or under the effective control of a “defendant”, defined under the POCA as “person charged or about to be charged with a serious offence, whether or not he or she has been convicted of the offence (section 205 (1)(i), POCA). It is doubtful if the POCA could be made to apply to those designated under UNSCR 1267.

256. The use of constraining orders under the CTA is also limited by section 108 of the same act i.e. they can only be used for criminal forfeiture after a conviction of a terrorism offence.

*Freezing Assets under S/Res/ 1373 (c. III.2):*

257. Section 122 (2) provides that, “funds of, or intended for, terrorist organizations shall be frozen, seized, and in accordance with this section detained, where the organization has been designated as a terrorist organization by the United Nations Security Council, or the Minister pursuant to regulations promulgated pursuant to this Act, or where there is probable cause to believe that the entity involved is a terrorist organization”.

258. While the second half of section 122 (2) may have been designed to authorize the Minister to designate domestically, the provision is deficient as it does not include individual terrorists. As of the time of the on-site, the RMI has neither designated a terrorist organization or individual nor established procedures to allow for such designation.

*Freezing Actions Taken by Other Countries (c. III.3):*

259. As with c.III.1 and III.2, there are no procedures in place for the local designation of terrorists, whether individuals or entities, in response to any potential freezing actions taken by other countries.

*Extension of c. III.1-III.3 to funds or assets controlled by designated persons (c. III.4):*

260. As stated in section 122 (2), the seizure and detention is limited only to the funds of designated terrorist organizations (Please refer to the discussions under c.III.1 and c.III.2).

*Communication to the Financial Sector (c. III.5):*

261. Section 122(2) does not detail how the financial sector is notified of the freeze, seizure and detention made under the CTA. During the on-site interview with representatives of the banking sector, the assessment team was informed that the sector was aware of, and was furnished with, a copy of the UNSCR 1267 Sanctions List and referred to the UN 1267 website. However, it would seem that awareness is limited, and only exists within the banking sector.

*Guidance to Financial Institutions (c. III.6)*

262. There is no detailed guidance provided to the financial sector of the process to follow in the event of a match or false name match, given the authorities themselves have not developed detailed implementation procedures for the CTA.

*De-Listing Requests and Unfreezing Funds of De-Listed Persons (c. III.7) and those Inadvertently Affected by the Freezing Mechanisms (c.III. 8)):*

263. There are no existing procedures for delisting either with UNSCR 1373 or 1267. An RMI national included in the UNSCR 1267 List has no remedy under the CTA or under any other legal framework that would allow such person to apply to have his or her name removed from the 1267 list.

264. The freezing, seizure and detention of funds of UNSCR designated terrorist organizations are made pursuant to section 122(2) of the CTA. But there are no clear cut procedures as to how funds subject to freezing, seizure and detention will be released. Section 122(5), however, provides that such funds can be released upon order of the High Court when, among others, the judge of the High Court is satisfied that the continued detention is no longer justified. An application to this effect can be made by or on behalf of the person whose property was affected.

*Access to frozen funds for expenses and other purposes (c. III.9):*

265. Under section 238(2) of the POCA, a restraining order may be subject to such conditions as the High Court deems fit providing for meeting out of the property or specified part of the property the reasonable living expenses of the defendant's immediate family. This is allowed under extreme cases where undue hardship to innocent parties would otherwise occur. However, this provision is limited to criminal proceeds and not the funds of 1267 listed entities.

*Review of Freezing Decisions (c. III.10):*

266. Upon application by or on behalf of the person whose funds have been seized or detained and subject to any contrary view of the Attorney General, the High Court may order the release of said funds in whole or in part (section 122 (5), CTA).

267. Section 217 of the Proceeds of Crime Act provides for the defendant or any other known interested third party to “*appear and adduce evidence at the hearing for application for confiscation; section 244 of the Proceeds of Crime Act provides for the review of restraining orders.*”

*Freezing, Seizing and Confiscation in Other Circumstances (applying c. 3.1-3.4 and 3.6 in R.3, c. III.11)*

268. The definition of the term “funds” subject to seizure, detention and freeze is the same as that defined under the FT Convention. Under the CTA, it includes those derived or intended for terrorism or for terrorist organizations (section 122(1), CTA). It does not cover property of corresponding value.

269. The freeze, seizure and detention under section 122 is implemented by law enforcement or customs officials whenever, among others, there is probable cause to believe that the subject funds are derived or intended to be used for terrorism purposes. Judicial review under the same section is only for the purpose of determining whether or not the continued detention is still justified after considering the attendant circumstances.

270. For purposes of forfeiture proceedings, a temporary restraining order or seizure warrant may be entered upon the AG's application without notice or opportunity for a hearing where there is probable cause that the subject property would be forfeited in the event of conviction or that exigent circumstances exist that would place the life and health of a person in danger (section 108(3), CTA).

271. Section 108, CTA provides further that the foregoing provisions shall be implemented without prejudice to the rights of third parties acting in good faith.

*Enforcing the Obligations under SR III (c. III.13):*

272. As stated above, so in so far as UNSCR 1267 and 1373 are concerned, the freeze, seizure and detention powers are limited to terrorist organizations designated by the UN Security Council. There are no procedures in place for the designation or delisting, unfreezing of assets within the context of UNSCR 1373. There are no specific procedure and timeframes to demonstrate that freezing can be effected "without delay" as required under UNSCR 1267.

273. There are no procedures in place to monitor compliance with the UNSCR requirements.

#### **2.4.2. Recommendations and Comments**

274. The CTA provides ample authority to freeze, seize and detain funds. What is lacking is the specific procedure that would show that the remedies can be effected without delay. As noted above, the authority under section 122(2) is limited to designated terrorist organizations. There are no procedures for domestic designation, delisting and un-freezing pursuant to UNSCR 1373.

275. The RMI should implement the following to address the deficiencies in SR.III:

- Adopt specific procedure, timeframes and ensure sanctions for non-compliance, through the promulgation of regulations pursuant to the CTA, to enable freezing "without delay" in relation to the requirements of UNSCR 1267.
- Adopt specific procedures for the designation and delisting of persons or entities within the context of UNSCR 1373.
- Implement an effective mechanism or communication systems or guidelines to subject persons.
- Provide for publicly known procedures for delisting and unfreezing.
- Develop and implement procedures to monitor compliance by the RMI government.

#### **2.4.3. Compliance with Special Recommendation III**

	Rating	Summary of factors underlying rating
SR.III	NC	<ul style="list-style-type: none"> <li>• The absence of specific procedure and timeframes to demonstrate</li> </ul>

		<p>freezing “without delay” in relation to the requirements of UNSCR 1267.</p> <ul style="list-style-type: none"> <li>• Total period permissible for freezing funds detailed under CTA is 2 years</li> <li>• There are no procedures for the designation and delisting of persons or entities within the context of UNSCR 1373.</li> <li>• No effective communication systems or guidelines to subject persons.</li> <li>• No publicly known procedures for delisting and unfreezing.</li> <li>• No procedures in place to monitor compliance by the RMI government.</li> </ul>
--	--	---

## 2.5. The Financial Intelligence Unit and its Functions (R.26)

### 2.5.1. Description and Analysis

#### *Legal Framework:*

276. Section 167 of the *Banking Act* provides the Banking Commissioner with a range of statutory powers, including to receive, store and disseminate reports from cash dealers and financial institutions to law enforcement i.e. powers of a financial intelligence unit (FIU).

#### *Establishment of FIU as National Centre (c. 26.1):*

277. In an attempt to delineate the Banking Commission’s regulatory and supervisory powers and functions from its FIU powers and functions, the Nitijela Cabinet established the Domestic Financial Intelligence Unit (DFIU) on 21 November 2000, as documented in Cabinet Minute 236. This Cabinet decision established the DFIU to comprise of the Banking Commissioner as Head, the Commissioner of Police, and Chief of Revenue and Taxation Division and a representative from the Attorney General’s Department in a supportive role.

278. The DFIU serves as the national centre for the receipt, analysis and dissemination of reports of transactions to other competent authorities based on powers vested in sections 167 and 170 of the *Banking Act*. Section 167 covers all aspects of the DFIU functions, while section 170 covers STR reporting and section 80 covers CTRs. Sections 5 and 6 of the revised *AML/CFT Regulations* provide the process and procedure for the reporting of STRs and CTRs to the Banking Commissioner.

279. The DFIU functions as an administrative FIU and has no formal investigative role with respect to ML/FT or predicate offences. Even though section 167 of the *Banking Act* provides the Banking Commissioner with law enforcement powers (in association with law enforcement agencies), including the freezing and confiscation of funds suspected to be the proceeds or related to ML/FT activities, this power has not been utilized.

280. The DFIU has, since its inception, developed an identity and profile separate to the Banking Commission, although the day-to-day operations of the DFIU are conducted by staff of the Banking Commission, and records and associated database are also housed in the Commission. The reference to the Banking Commissioner in this section of the report is in the context of the position’s dual role as DFIU Head.

281. The DFIU has standard operating procedures (SOPs) for overall DFIU operations, including CTRs and a separate one for STR analysis, although the former (sections 5 - 9) also includes procedures for processing STRs. From 2005 to September 2010, the two banks submitted a total of 211 STRs. No STRs have been received from other financial institutions or cash dealers.

*(a) STR Submission, Receipt and Storage*

282. Financial institutions and cash dealers are required under section 170 of the *Banking Act* to report STRs within 3 days of a transaction. Reports are submitted electronically, although there is scope for hard copy reports to be submitted.

283. STRs are submitted in accordance with Instruction 6 – Preparation Guidelines for Suspicious Activity Report Form (STR) – effective August 27, 2001 and in other guidance provided (see c.26.2 below).

284. The DFIU, on receipt of a report, assigns a unique reference number to each report and establishes an electronic record in the DFIU database that allows for electronic filing and analysis of STRs and CTRs.

*(b) Prioritization/Initial Screening of STRs*

285. The DFIU, on receipt of an STR, refers the STR to an analyst who follows the SOP to analyse the STR. This includes carrying out checks on the database to determine if previous STRs or CTRs have been reported for the same entity. If an STR is FT related, a check is made of the United Nations or other terrorist list.

286. If there is no suspicious activity, the report will be noted ‘No Further Action’. For all other reports, the analyst will allot a priority rating of High, Medium or Low for processing.

287. There is also scope at the point of screening under the ‘Immediate Action’ scenario. According to the SOP, the Banking Commissioner may take a number of steps, including referral to law enforcement or instructing the financial institution or cash dealers to take such steps as may be appropriate to facilitate any investigation anticipated.

*(c) Analysis*

288. If there are other linked STRs, the analyst will carry out additional checks and update the current data base with additional information e.g. ID documents, linked accounts, other addresses etc. It should be noted here that not all STRs are analyzed in detail due to a lack of staff in the DFIU.

289. The DFIU database is integrated and searches of STRs and CTRs can be conducted simultaneously.

290. Analysts may seek further information from the following external sources:

- **Reporting entity** - Where the information contained in the STR, including cash transaction reports is insufficient or unclear, a formal letter of request is sent to the institution under the signature of the Banking Commissioner, pursuant to section 170(2) of the *Banking Act*.

- **Competent Authorities - Police, Revenue and Taxation, Immigration, Attorney General.** Where information from law enforcement is required, the DFIU may request information in an informal manner between DFIU, Commissioner of Police and the Chief of Revenue and Taxation. Section 167 of the *Banking Act* does not explicitly provide for the DFIU to request information from law enforcement authorities. Section 167(1)(n) of the *Banking Act* provides for the DFIU to conduct investigations with law enforcement authorities where the Commissioner of Banking has reasonable grounds to suspect ML activities.
- **World Check or internet search** - The analyst will include a number of additional checks including World Check and Google.
- **Foreign FIUs** - This is available under section 167(1)(j) of the *Banking Act*.

291. In practice, many of these requests are made by email or phone call in an informal manner. Some of the requests are recorded by either the DFIU or the competent authority making the request; however, not all requests for information are formally recorded. The informal requests for information are not being captured for statistical purposes, so a true picture of the number of requests made between the DFIU and the competent authorities cannot be gained.

*(d) Dissemination*

292. At the completion of the analysis process, the report is sent to the Commissioner of Banking with a recommendation, either: (a) for it be disseminated to the relevant law enforcement agency, where the analyst believes there are reasonable grounds to suspect, pursuant to section 167(1)(b) of the *Banking Act*, or (b) for some future action, or (c) no further action to be taken (NFA).

293. DFIU refers STRs to the Criminal Investigation Division (CID) in the Department of Public Safety (DPS). The CID does not keep statistics on the receipt and action of STRs and does not provide feedback to the DFIU on the outcomes of STRs received. Any feedback received is generally a result of follow up from the Head of the DFIU.

294. The deficiency in the above analysis process is at the first stage, in the culling and prioritization process where a decision not to undertake any further action seems to be limited to a review of any linkages with earlier STRs or CTRs submitted, or in the case of FT, on available FT list. If other information is included in the initial prioritization analysis process, a different conclusion might result. All STRs are not investigated due to a lack of staff resources.

*Guidelines to Financial Institutions on Reporting STR (c. 26.2):*

295. The DFIU and the Banking Commission have issued the following joint guidance to financial institutions and cash dealers relating to the form and manner of reporting STRs and CTRs. No guidance has been issued for DNFBPs:

- *Advisory A - 10 (a): STR reporting of financing of terrorism*, issued in August 2010, advising financial institutions and cash dealers of the new STR reporting obligations
- *Guideline 2: Suspicious Transactions*, issued in August 2004, providing detailed guidance of suspicious transaction indicators

- *Instruction 6 – Preparation Guidelines for Suspicious Activity Report Form (STR)*, including the STR form issued in August 2001
- *Instruction 7 – Currency Transaction Report (CTR)*, replicates Form 4789 of the Internal Revenue Service of the United States, and has been modified in line with the RMI banking requirements.

*Access to Information on Timely Basis by FIU (c. 26.3):*

296. Section 167 of the *Banking Act* does not contain any specific or explicit reference which enables timely access by the Commissioner of Banking to information from other competent authorities. In practice, the Chief of Police, Customs and the Attorney General, as DFIU members, are not constrained in accessing information held by other competent authorities.

297. The DFIU advised the assessment team that it has accessed information from other competent authorities such as the Police, Immigration and the Registrar of Incorporation during the analysis process. The list below provides the statistics on the number of times the DFIU has accessed information from other competent authorities.

**DFIU: Number of Information Request to Domestic Partners:**

Agency	2005	2006	2007	2008	2009
Registrar of Non-Residents Corporations	5	2	8	4	8
Immigration	-	-	-	1	1
Department of Public Safety	-	-	-	-	2
Division of Customs, Revenue, Taxation, & Treasury	-	-	-	1	2

*Additional Information from Reporting Parties (c. 26.4):*

298. The Commissioner of Banking or the Attorney General has the authority to request additional information from financial institutions and cash dealers pursuant to section 170(2) of the *Banking Act* in relation to submitted STRs. The Banking Commissioner has requested additional information in 18 instances relating to submitted STRs from financial institutions and cash dealers. (Refer to the *Statistics* section below for yearly totals.)

299. Where additional information is required for suspected ML activity and for analysis purposes, the Banking Commissioner under section 167(1)(i) “...shall have the authority to request additional information from financial institutions and cash dealers where the Commissioner has reasonable grounds to believe that such information is essential in discovering money laundering activity...” This power enables the Banking Commissioner to request additional information from the original financial institution and/or cash dealer reporting the transaction report, and a financial institution or cash dealer other than the reporting institution.

300. In instances relating to a lack of or incomplete information in reports, the DFIU contacts the relevant financial institution and/or cash dealer with notification the transaction report is incomplete. The reporting entity submits an amended form which is attached to the original report thus ensuring completeness of the information submitted.

*Dissemination of Information (c. 26.5)*

301. The Commissioner of Banking, pursuant to section 167(1)(b) of the *Banking Act*, authorizes the dissemination of transaction reports received pursuant to section 170 of the *Banking Act*. The Commissioner of Banking may compile statistics and records, disseminate financial information to authorities within the RMI or elsewhere and make recommendations in relation to information received pursuant to section 167(1)(f). In the period from 2005-2010, 19 STRs were disseminated to law enforcement out of a total of 211 STRs received. However, this total is distorted by an unusually high dissemination figure of 13 in 2008. This matter relates to a taxation evasion case which was settled by way of repayments to the Taxation Department.

302. The legal powers of information exchange contained in section 167 of the *Banking Act* and section 116 of the CTA do not preclude the spontaneous exchange of information. In fact, under section 118 of the CTA, the RMI is tasked to, "...cooperate in the prevention of terrorism by exchanging information to provide early warning of possible terrorism..."

*Operational Independence (c. 26.6):*

303. The DFIU, although housed in the Banking Commission, is autonomous and operates independently. The Commissioner of Banking, in her dual role as the Head of the DFIU, has the power under sections 170(1)(b) and (d) to disseminate reports to law enforcement, if there are reasonable grounds to suspect the transaction is suspicious or proceeds of crime.

304. Despite the dual roles of the Banking Commissioner, there is no evidence or suggestion of any conflict of interest arising out of this arrangement. There has been a conscious attempt to delineate the Banking Commissioner's prudential supervisory functions from her DFIU functions.

305. The annual budget for the DFIU is within the Banking Commission's budget.

*Protection of Information Held by FIU (c. 26.7):*

306. The Commissioner of Banking has the authority to obtain and protect the secrecy of information held within the DFIU. Pursuant to the *Banking Act* Part XIII – Money Laundering section 167(1) (m) and Part XI – General Section 154 (2), the Banking Commissioner and every officer and employee working under the Commissioner adheres to the secrecy of all information collected from banks and any other client. A breach against section 154(2) is subject to a fine not exceeding \$5,000. However, these secrecy provisions do not preclude information sharing as described in c26.5.

307. There is no formal confidentiality requirement for law enforcement receiving STR or other information from the DFIU. Further, there is no formal MOU in place between the DFIU and law enforcement agencies e.g. Bureau of Public Safety.

308. The DFIU is located in the main government building and co-located/housed within the Banking Commission's Office. The security of the DFIU is maintained by a locked door with access only permitted by the staff of the DFIU. Visitors are escorted and security is maintained by ensuring visitors do not view material they are not authorized to see.

309. STR information is held in a stand-alone computer in the Banking Commissioner's Office. The three DFIU/Banking Commission staff are able to access the computer using a password. Hard copy files of all DFIU related documents are kept in a separate security cabinet.

310. STR database information is backed up daily onto a CD. There is no clear procedure for the backup of information contained in the DFIU's database. Any loss of data may have serious ramifications for the DFIU's ability to conduct its core functions in a timely manner.

*Publication of Annual Reports (c. 26.8):*

311. Neither the Banking Commission nor the DFIU produces an annual report. There is no requirement in the *Banking Act* for the production of an annual report. However, under the *Banking Act Amendment Bill 2010*, there is inclusion of a new section. 167(1)(o), which states, "...shall prepare annually a report of the activities of the Domestic Financial Intelligence Unit that shall include statistics, typologies and trends as well as information regarding the activities of the Domestic Financial Intelligence Unit, which shall be submitted to Cabinet before the end of each financial year."

*Membership of Egmont Group (c. 26.9):*

312. The DFIU became a member of Egmont in June of 2002.

*Exchange of Information among FIUs (c. 26.10)*

313. Pursuant to section 167(1)(b) of the Banking Act, the Commissioner of Banking may disseminate financial information to authorities within the RMI or elsewhere, including foreign FIUs. The DFIU continues to operate under Egmont rules, including its principles for information exchange between FIUs. The *Banking Act* does not apply restrictions on which FIUs may be the subject of information sharing. The DFIU currently has Memoranda of Understanding (MOUs) with Australia and Chinese Taipei. There are four MOUs pending with Malaysia, United Arab Emirates, Kingdom of Saudi Arabia and Japan.

314. The DFIU shares information on request from foreign FIUs when the requesting FIU is an Egmont member. The DFIU has received the following information requests from foreign FIUs. The DFIU advised they responded to those requests. While detailed statistics are not available, authorities advised that most were for information on companies incorporated under RMI's non-resident domestic company registrar. The DFIU, in responding, liaised with TCMI to obtain the information requested, where available.

**Table: Information Requests by Foreign FIUs**

Year	Jurisdictions	Number
2005	Slovenia, Cyprus, Serbia	3
2006	Croatia	2
2007	Mauritius, Belgium, Cyprus Romania, Belarus, Greece Macedonia, Serbia	8
2008	United Kingdom, Turkey Australia, Luxembourg	8
2009	Croatia, Bulgaria, Ukraine Slovakia, Serbia, Montenegro, Bulgaria	7

315. The DFIU exchanged financial information on 12 occasions in 2009 with FIUs which are members of Egmont. The DFIU made two requests – both to the US in 2008. In 2010 the DFIU requested financial information from one foreign FIU.

*Adequacy of Resources to FIU (c. 30.1):*

316. The DFIU currently does not have adequate human and technical resources to perform the core FIU functions. In practice the DFIU is comprised of three operational staff. The three operational staff members are the Banking Commissioner/Head of the DFIU, the Assistant Banking Commissioner who provides a support role, and an analyst who serves as an administrative officer. The three staff are also responsible for AML/CFT supervision, and broader prudential supervision of RMI's financial sector. All these roles are conducted on a part-time basis.

317. The Commissioner of Police and Chief of Customs, given their seniority and other portfolio responsibilities, are not involved in daily DFIU operational matters. However, they do meet regularly to discuss operational matters. The schedule of meeting is proposed on a monthly or as required basis; however, the former is not always met due to work priorities. While it is difficult to estimate, the actual DFIU staffing number is probably the equivalent of one full time staff member.

318. The current staffing establishment has constrained the development of financial intelligence expertise. The Banking Commission's limited staffing resources have meant that no individual staff member has focused exclusively on FIU or AML/CFT functions. They are required to do all three functions, i.e. FIU, AML/CFT supervision and prudential supervision.

319. A proposal for one additional part-time staff member for the DFIU has been submitted. This is an outstanding recommendation made in the last MER which recommended the appointment of one staff member to focus on AML/CFT matters between the DFIU and the Chief of Police.

320. The US, through its Embassy in Majuro, has provided an IT system for CTR and STR analysis and intelligence work to the DFIU.

*Integrity of FIU Authorities (c. 30.2):*

321. All Banking Commission/DFIU staff are subject to standard RMI government requirements, although there does not appear to be a regular process or police background checks or any requirement to declare potential conflicts of interest. There are no separate written procedures for the conduct and behaviour of Banking Commission staff when performing DFIU functions.

322. The provisions in Part XXVIII of the *Criminal Code* on "Public Officers and Employees" are applicable to the Banking Commission, and therefore staff performing DFIU functions and non Banking Commission staff as part of the broader DFIU.

*Training for FIU Staff (c. 30.3):*

323. Staff within the DFIU have limited training on intelligence analysis, ML and FT risk assessment and typologies. They have undertaken some training, however, there has been limited scope to utilize those skills.

324. During 2009 and 2010, DFIU staff participated in FIU training programs provided by Australia (AUSTRAC and AMLAT)<sup>2</sup>, and the UNODC (Pacific Anti-Money Laundering Program (PALP)).

*Statistics (applying R.32 to FIU):*

**a) Number of suspicious transaction reports received and disseminated;**

325. STRs have only been submitted by the banking sector as outlined below:

**Table: STRs received: Banks**

Year	Total
2005	46
2006	19
2007	34
2008	50
2009	34
2010	28
Total	211

**Table: STRs disseminated to law enforcement agencies**

Year	Number of STRs disseminated to DPS
2006	3
2007	2
2008	Cases involved 13 STRs
2009	1

**Table: DFIU's additional information requests to FIs/ CDs relating to STRs**

Year	Number of requests
2005	1
2006	4
2007	2
2008	4
2009	7

---

<sup>2</sup> AMLAT is a section within the Australian Government Attorney-General's Department.

**Table: CTRs received**

<b>Year</b>	<b>Number of CTRs received</b>
2007	2,817
2008	2,653
2009	1,624
2010 (Jan – May)	930

## Effectiveness

326. The FIU has been inadequately resourced to fulfil its role and functions because of the dual roles undertaken by DFIU staff. The DFIU has, however, been able to achieve its key outputs despite those circumstances and some deficiencies in its screening process for STRs and internal administrative procedures.

327. The authorities have submitted a *Banking Act Amendment Bill 2010* to the Nitijela with proposed amendments to section 167 of the Act. The amendments to section 167, if made, may address some of the deficiencies identified in this report. It should be noted, however, that the proposed amendments do not relate to the structure and resources of the DFIU, which are of concern to the assessors and impact on the effectiveness of the DFIU. At the time of on-site and the period immediately after, consideration of the Bill was deferred until the next Parliamentary session in January 2011.<sup>3</sup>

### 2.5.2. Recommendations and Comments

328. The RMI should undertake the following to enhance the DFIU:

- Ratify as soon as possible the *Banking Act Amendment 2010 Bill*, including the new section 167, which will address current deficiencies and further improve the operations of the DFIU. The Bill should include a clear provision for the DFIU to access information from other competent authorities, and vice versa.
- Review the STR analysis SOP to ensure all relevant information (including UNSCR 1267 and other lists) is considered in the screening, prioritization and analysis process.
- Develop and implement sector specific STR guidance and feedback for financial institutions and cash dealers.
- Publish a DFIU annual report to include statistics, typologies and trends. A sanitized version of the annual report should be publicly available.
- Develop an SOP to ensure all FIU data is backed-up on a regular basis and stored in an off-site secure location.

---

<sup>3</sup> Not passed in January 2011

- Provide a separate budget for the DFIU, and dedicate one full time staff member to DFIU and AML/CFT functions (see recommendation also for FATF Recommendation 23 and 30).
- Develop or enhance SOPs to ensure all information requested or received between the DFIU and competent authorities (i.e. CID), or reporting entities, are officially recorded by all competent authorities, whether receiving or requesting, for audit and statistical purposes.

### 2.5.3. Compliance with Recommendation 26

	Rating	Summary of factors relevant to s.2.5 underlying overall rating
<b>R.26</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Deficiencies in the STR analysis, screening and prioritization process</li> <li>• No clear legal authority to obtain information from LEAs to assist in the analysis of the STRs</li> <li>• Lack of sector specific STR guidance</li> <li>• No publicly available FIU annual report, including statistics</li> <li>• No back up of data is performed</li> </ul>
<b>R.30</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Lack of DFIU dedicated resources and specialized financial intelligence expertise</li> </ul>

## 2.6. Law enforcement, prosecution and other competent authorities—the framework for the investigation and prosecution of offences, and for confiscation and freezing (R.27, & 28)

### 2.6.1. Description and Analysis

#### *Legal Framework:*

329. The Department of Public Safety (DPS) is a quasi-military organization which was established pursuant to the *Public Safety Act 1988*. The functions, powers and duties are contained in Part 11, Division 3 (Powers and Duties), Part V (General) and Part VI (Undercover Investigation Division). The DPS provides policing, prison, fire, emergency and sea patrol services through its various divisions. The DPS's divisions include a Patrol and Investigation Division, Criminal Investigation Division (CID), Vice and Drug Division, Correction and Juvenile Division, Fire Division, and the Sea Patrol/Search and Rescue.

330. The legal framework under which the DPS carries out its role and functions for suppressing ML and FT is contained in the following legislations:

- *Criminal Code*;
- *Proceeds of Crimes Act*;
- *Criminal Procedure Act (Criminal Extradition)*;
- *Counter Terrorism Act (2002)*;
- *Foreign Evidence Act (2002)*;
- *Narcotics Drugs Act (1987)*
- *The Mutual Assistance in Criminal Matters Act (2002)*; and
- *The Banking Act of 1987, as amended in 2009*

*Designation of Authorities ML/FT Investigations (c. 27.1):*

331. The Commissioner of Police confirmed with the assessment team during the on-site that the CID is the designated police unit within the DPS to carry out investigations into ML, FT and other predicate offences pursuant to the *Banking Act*, *Criminal Code*, *Proceeds of Crime Act* and the *Counter Terrorism Act*.

332. The CID is the lead agency for ML investigations in the RMI, which it undertakes in consultation with the Attorney General and the DFIU. The Banking Commissioner under section 167(1) of the *Banking Act* can also conduct investigations in conjunction with law enforcement authorities, where the Banking Commissioner has reasonable grounds to suspect ML activity is occurring.

333. The Office of the Attorney General (OAG) is the primary authority under the *Counter Terrorism Act*, including the authority to prosecute under section 104 (4), and the authority to investigate, under Part III section 113. The Attorney General has the authority to direct the CID to undertake investigations in relation to terrorist activities.

*Ability to Postpone / Waive Arrest of Suspects or Seizure of Property (c. 27.2):*

334. The RMI *Criminal Procedures Act (Parts II-III)* provides for warrant, arrest, search and seizure provisions. There is no provision or prohibition within the Act for the postponement or waiver of the arrest of suspects or seizure of property. Conversely, the legislation does not specifically preclude such actions.

335. The *Counter Terrorism Act* in section 107 (5) authorizes law enforcement officers to detain a person (s) for 48 hours for the purposes of investigation; however, this timeframe may be extended for an additional 7 days without charges being laid.

*Additional Element—Ability to Use Special Investigative Techniques (c. 27.3):*

336. The Undercover Investigation Division has the powers under the *Public Safety Act*, Part VI Undercover Investigations Division, section 542, to carry out undercover activities of sensitive matters, including, but not limited to, controlled substances, national security, corruption in government, environmental law violations, trade in restricted or prohibited goods, tax evasion and other matters as may be determined by the President and Cabinet.

*Additional Element—Use of Special Investigative Techniques for ML/FT Techniques (c. 27.4):*

337. The RMI authorities have not employed special investigative techniques in relation to ML or FT activities. At the time of the mutual evaluation, the Undercover Investigation Unit had carried out undercover activities in relation to offences under the *Prostitute Prohibition Act 2001*.

338. The DPS and OAG have the legal basis to use special investigative techniques; however, they have not been in a position to carry out those functions due to a lack of training, resources and equipment.

*Additional Element—Specialized Investigation Groups & Conducting Multi-National Cooperative Investigations (c. 27.5):*

339. The RMI authorities indicated they have insufficient human (financial investigators) and financial resources to establish specialized financial investigative groups, either permanent or temporary, in investigating the proceeds of crime. The CID rarely carries out ML investigations due to a lack of training. This has prevented staff from learning the necessary skills and knowledge required. The management of ML investigations is under the responsibility of the Police Commissioner, who works with the OAG and the DFIU.

*Additional Elements—Review of ML & FT Trends by Law Enforcement Authorities (c. 27.6):*

340. Information in relation to ML and FT is reviewed by the CID and there has been an ongoing, although informal, effort to share information among the relevant agencies where possible.

Recommendation 28

*Ability to Compel Production of and Searches for Documents and Information (c. 28.1):*

341. Section 516 provides general powers to collect evidence and section 514 of the *Public Safety Act* provides “(3)... every Police Officer promptly to obey and execute all orders and warrants lawfully issued to him by any competent authority..”

342. The *Criminal Procedures Act*, under “*Part III: Searches and Seizures*”, provides general powers to law enforcement authorities. However, the search and seizure powers are limited to searches and seizures in connection with arrests, and not for gathering evidence in the absence of an arrest warrant.

343. The POCA provides measures for “*identifying, tracing, freezing and seizure and confiscation of proceeds of serious crime and property used in the commission of a serious offence and, for other purposes*”. In addition, section 251 of the POCA provides powers to search for, and seize tainted property subject to a search warrant from a judge in section 252, where a police officer has probable cause. However the use of such powers is limited to “tainted property” as discussed under FATF Recommendation 3. Search warrants were issued on two occasions for the years 2007-2009.

344. Part V of the POCA provides “*Production Orders and Other Information Gathering Powers*” to police. These powers are quite comprehensive but they can only be used when “*a defendant has been charged with or convicted of a serious offence and police has probable cause.*”, as specified in section 258 of the POCA.

345. Section 167 (I) of the *Banking Act* provides the Banking Commissioner with the following investigative powers,

*“shall have the authority and ability to apply for a warrant to enter any premises belonging to or in the possession or control of a financial institution, cash dealer or any officer or employee thereof, and to search the premises and remove any documents, materials, or other things therein for the purposes of preventing money laundering activity, the financing of terrorism, or tracing the proceeds of crime, as so ordered by the High Court and specified in the warrant other than as authorized in Subsection (c) and (i) above;”.*

However, these powers are limited to financial institutions and cash dealers, and exclude DNFBPs. Furthermore, the Banking Commissioner cannot delegate these powers to anyone outside of the Banking Commission.

346. The CTA contains measures to counter FT; however, the emphasis is on freezing, seizure and forfeiture. The CTA is silent on search or production warrant powers, although law enforcement is tasked in section 113 (5) to ‘*identify, detect,*’ in addition to “*freeze, seize and obtain forfeiture of funds*” as part of the measures outlined in section 113 of the CTA.

*Power to Take Witnesses’ Statement (c. 28.2):*

347. As indicated, the police are empowered to collect evidence in section 516 of the *Public Safety Act*. Evidence is not defined in this Act; it is defined in the *Evidence Act 1989*, which includes ‘Prior Statements of Witnesses’ under Rule 613 of the *Evidence Act*. There is no specific mention of powers to collect witness statements. However, the competent authorities advised the assessment team during the on-site that more than 50 witness statements have been taken in the previous 12 months.

*Adequacy of Resources to Law Enforcement and Other AML/CFT Investigative or Prosecutorial Agencies (c. 30.1):*

348. The Commissioner of Police is the Head of the DPS with three (3) Police Majors from the three main forces or divisions within the Police Department. A Police Major heads each of the RMI law enforcement agencies; Majuro Force, Ebeye Force and Sea Force.

349. The DPS consists of 164 sworn police officers and civilian officers, including the Commissioner of Police. The total population of the RMI is 60,000. The breakdown of staff against each law enforcement agency (police) is as follows:

- Majuro Police Force – 109
- Ebeye Police Force – 28
- Sea Force – 27

350. The CID consists of six detectives within the Majuro Force, two (2) within the Ebeye Force, and one (1) within the Sea Force. Only one CID detective has successfully completed basic criminal investigation training. A request has been submitted for a proposed restructure of the Police Department which would include the recruitment of 20 additional police officers.

351. A Transnational Crime Unit (TCU) was established within the DPS and currently has one investigator full time and the TCU utilizes the office assistant for administrative work. Training of new TCU staff was conducted in mid-June 2010. All international requests for information are managed through the TCU to Interpol. In the previous 12 months only one request was made. Due to the Interpol fee not being paid, the TCU will not receive the results of the information requested until the fee is paid. This request was in relation to a background check for a foreign investment licence.

352. The CID has one investigator trained in basic financial investigation. The authorities have acknowledged the lack of financial investigative skills has hampered the ability to investigate potential ML and proceeds of crime cases, particularly taxation related violations. Due to this lack of experience, it has been considered appropriate to investigate the predicate offence which has a higher

prospect of a successful prosecution. This in turn has prevented ML or proceeds of crime cases being brought before the court.

*Integrity of Competent Authorities (c. 30.2):*

353. The DPS completes a security check on all staff, through Interpol, prior to the commencement of employment. The *Public Safety Act*, Part IV *Discipline*, sets out the conduct for police and prison officers. There is no ongoing integrity, drug testing or financial requirements for employees of competent authorities.

*Training for Competent Authorities (c. 30.3):*

354. Training courses undertaken by officers of the DPS include:

- Proceeds of Crime – delivered by Pacific Anti-Money Laundering Program/ United Nations Office of Drugs and Crime (PALP/ UNODC)
- UNODC AML Computer Based Training software is within the Ministry of Finance training room

355. In September 2009 the RMI, assisted by the Australian Federal Police (AFP), established the Police Academy for training of cadets and serving police officers.

356. The AFP is delivering a five year capacity building program with the RMI police and has completed a review of the DPS Police Force. The review has resulted in a two stage approach focusing on organisational, human resources and financial issues.

357. Twelve RMI police have been trained in the AFP's Leadership training through the Micronesia Leadership Development Program.

*Additional Element (Rec 30) - Special Training for Judges (c. 30.4):*

358. Training for the judiciary is limited, though the Chief Justice of the RMI High Court has attended two AML/CFT training courses. The RMI judiciary received AML/CFT training in May 2007 at a sub-regional judicial workshop on ML and FT hosted by Palau. The workshop was co-hosted by UNODC/PALP and Australia (AMLAT). Judges from Palau, Papua New Guinea, Solomon Islands, Tuvalu, the RMI and Fiji attended the workshop.

*Statistics (applying R.32):*

359. There have been a number of opportunities for ML offences to be investigated; however to date, there have only been two cases of ML investigation, though both led to prosecution of predicate offences only. The decision on whether to prosecute ML offence lies with the Attorney General, and the lack of ML expertise has deterred authorities from pursuing ML investigations and prosecutions.

360. The statistics below are for the years 2007-2009 inclusive. Statistics relating to the use of police powers in 2010 are detailed in the table below:

**Table: Use of Police Powers**

<b>Police Powers</b>	<b>No.</b>	<b>Offence</b>
Search Warrants	2	1 x drug offence; 1 x illegal importation of cigarettes (dismissed by the Court)
Telephone Records	1	Grand larceny resulting in prosecution with a custodial sentence of 1 year with 6 months probation
Witness Statements	50	
Information	6	Requested from financial institutions

**Table: Offences Investigated by the DPS**

	<b>2007</b>	<b>2008</b>	<b>2009</b>
Assault and battery with a dangerous weapon (ABWDW)	63	7	36
Affray	12	13	4
Aggravated Assault	3	0	2
Assault	28	4	3
Assault & Battery	67	142	12
Attempted Suicide	1	0	56
Auto-Theft	3	0	3
Burglary	120	26	54
Conspiracy	1	0	
Counterfeiting	0	4	1
Disturbing the Peace	769	1088	480
Drunken Disorderly Conduct	442	936	353
Embezzlement	5	0	3
Escape	30	45	64
Forgery	1	0	3
Grand Larceny	43	0	44
Malicious Mischief	98	106	69
Misconduct Public Office	1	0	0
Murder 1st Degree	1	2	1
Obstructing Justice	5	3	4
Petit Larceny	55	5	72
Possession of Firearms	1	0	0
Rape	0	1	2
Riot	0	3	2
Robbery	1	4	1
Suicide	5	2	7
Trespass	21	63	24
<b>Grand Total</b>	<b>1776</b>	<b>2456</b>	<b>1302</b>

**Effectiveness:**

361. The CID has only undertaken two ML investigation cases; however, there is some confusion whether these were formally classified as ML investigation cases or not. Both cases led to prosecution for predicate offences only.

362. The lack of investigation and prosecution of ML and proceeds of crime cases are due to numerous factors, including a lack of financial investigative skills, understanding of ML and the greater likelihood of achieving a predicate crime conviction.

**2.6.2. Recommendations and Comments**

363. For ML investigations and prosecutions to proceed, the CID will need to consider ways of enhancing the current skills and knowledge of the CID to include financial investigation techniques. This will provide the CID with the necessary tools to investigate ML, proceeds of crime and taxation related violations on equal footing with predicate offences investigation.

364. The following recommendations are made to enhance the financial investigative skills and knowledge of the CID and other relevant authorities:

- Provide additional training to develop sufficient expertise in ML, proceeds of crime and financial investigations for the DFIU, DPS, judicial and prosecutorial agencies.
- Develop a plan to build expertise in investigations, with an initial focus on simpler cases of potential ML, proceeds of crime and taxation related violations.
- Ensure there are sufficient funds from the national budget to guarantee ongoing access to the Interpol system. At the time of the mutual evaluation the fee had not been paid and there remained one outstanding request for information.

**2.6.3. Compliance with Recommendations 27 & 28**

	Rating	Summary of factors relevant to s.2.6 underlying overall rating
<b>R.27</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Predicate offence investigations are pursued at the expense of ML investigations.</li> <li>• Lack of implementation of available ML investigation powers.</li> </ul>
<b>R.28</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Certain powers not explicitly provided in legislation.</li> <li>• Effectiveness of police powers has not been tested in relation to ML and FT.</li> </ul>
<b>R.30</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Implementation is impeded by the lack of financial investigative expertise.</li> <li>• Lack of expertise and dedicated resources to undertake financial investigation/s of ML/FT and proceeds of crime.</li> </ul>

**2.7. Cross Border Declaration or Disclosure (SR.IX)****2.7.1. Description and Analysis***Legal Framework:*

365. The Ministry of Finance, headed by the Secretary of Finance, has three subdivisions: Administration & Accounting; Budget, OIDA, Procurement & Supply; and Customs, Treasury, Revenue & Taxation. Customs is charged with enforcing the *Currency Declaration Act (CDA) of 2009* and the *Import Duties Act of 1989*.

366. The CDA was passed by the Nitijela (Parliament) in May 2009 and came into effect in August 2009. The purpose of the CDA is to detect the physical cross-border transportation of currency. Under section 29(3), a person who enters or leaves the RMI with currency amounting to US\$10,000 or more, or its equivalent in any other currency, shall make a declaration to an authorized officer in the form prescribed. Currency is defined in section 2 (1) to include currency of the RMI or another country, monetary instruments including bearer negotiable instruments, precious metals and stones, any other kind of monetary instrument, and currency in electronic form.

367. The term FT is not used in the CDA; however, it may be covered under the definition of “*unlawful conduct*” which means conduct that is unlawful under the criminal law of the RMI; or unlawful under the criminal law of another country or territory. The *Counter-Terrorism Act* provides for criminal penalties and criminal forfeiture.

*Mechanisms to Monitor Cross-border Physical Transportation of Currency (c. IX.1):*

368. As stated above, the CDA provides a definition of currency which includes cash (paper money and coins of the RMI or a foreign country), bearer negotiable instruments and precious stones and metals.

369. Section 3(1) of the CDA clearly states there is an obligation for person/s entering or leaving the RMI to declare amounts of currency of US\$10,000 or more. The CDA does not define ‘person’ or ‘persons’ to include both natural and legal person (s). However, the RMI currently has an inwards declaration system in place and neither the definition of currency nor penalties for false declaration is included in the actual Customs Declaration Form; the actual form used is different to the prescribed form in Schedule 1 of the CDA. For outwards declaration of currency, work is to commence on the creation and introduction of a suitable form.

370. Customs is currently considering the creation of large posters outlining the obligation of passengers to declare currency of US\$10,000 or more at the time of arrival or departure. These posters will also be displayed at the RMI Post Office, shipping agents’ premises and at the RMI Customs Office.

371. The CDA does not specifically provide for declaration of currency through general shipping or by containerized cargo. It would seem that no breach is committed under the CDA if a person sends currency through these channels without declaration.

372. Banks have an informal arrangement to notify Customs of importation of currency of US\$10,000 or more. The currency shipments are deemed as cargo as they are for a commercial purpose, and the banks are required to complete a Customs Form 725 for cargo. Generally, this relates only to inwards movement of currency, as there is very little outwards movement of large amounts of currency by the banks of the RMI.

373. The CDA does not specifically provide for the movement of currency posted through the mail system; however, in an attempt to monitor any activity of mail through the post, the RMI Customs has stationed an officer at the post office. The main role of the RMI Customs at the post is to collect revenue and monitor possible illegal activity.

*Request Information on Origin and Use of Currency (c. IX.2)*

374. Section 4 of the CDA provides for the RMI Customs to have authority as an “*authorised officer*” to question arriving or departing passengers on the source, ownership, acquisition, use, or intended destination of currency for amounts of US\$10,000 or more. The legislation does provide for the search of “*craft*”<sup>4</sup>, if an authorised officer has reasonable grounds to suspect there is an amount of US\$10,000 or more on the craft.

375. Failure by a passenger to answer questions carries a pecuniary penalty not exceeding US\$5,000. The RMI Customs has a general authority under the *Taxation Act*, Part VI – Enforcement – General Powers and duties of Customs Officers to ask questions in relation to imported and / or exported goods.

*Restraint of Currency (c. IX.3):*

376. Section 6 of the CDA provides authorised officers with the power to seize or restrain currency, in whole or in part, if the officer has reasonable grounds for suspecting that the currency is recoverable; intended for use in unlawful conduct; or undeclared intended for use in unlawful conduct. Section 7 (1) of the CDA provides authorised officers with the power to detain currency seized under section 6, for a period of 72 hours, if the officer continues to have reasonable grounds for his suspicion. The RMI High Court, under section 7 (2) (a) has the authority to issue an order, on application of an authorized officer, to extend the 72 hour time limit to three months and on the issuance of a further order under section 7 (2) (b) to a period of two (2) years from the date of the first order.

*Retention of Information of Currency and Identification Data by Authorities when appropriate (c. IX.4):*

377. The CDA does not provide for the identification data of the bearer (s) to be retained for use by appropriate authorities in instances where the declaration exceeds the prescribed threshold (US\$10,000); or where there is a false declaration; or where there is suspicion of ML or FT.

378. The RMI Customs currently has a manual filing system in place for the recording of cross-border movement of currency and other customs related offences.

*Access of Information to FIU (c. IX.5):*

379. The legislation does not provide for the DFIU to have access or to receive the information relating to the importation of the cross-border movement of currency of US\$10,000 or more. However on the Schedule 1 Form ‘*Declaration of International Transportation of Currency Form* (currency form) there exists a provision for a copy of the original currency form to be forwarded to the Banking Commission, and a copy is retained by RMI Customs. It is understood the original document will be forwarded to the DFIU when amendments to the currency form have been completed.

380. There is currently no formal process for the sharing or transferring of information from the RMI Customs to the DFIU. Discussions indicated this would be carried out in an informal basis,

---

<sup>4</sup> S.2 (1) – Craft means any vehicle or vessel that is used for transportation on land, the sea, or in the air.

where matters of cross-border movement of currency are raised during meetings held with the Head of the DFIU, the Commissioner of Police and the Chief of Customs.

381. The RMI Customs is considering an MOU with the DFIU and law enforcement agencies on matters relating to ML and FT. This will formalize the current information sharing process.

382. As there has never been a currency declaration over the threshold amount or any detection of undeclared/false declaration (s) of cross-border movement of currency, the Chief of Customs indicated the *Division of Customs, Revenue and Taxation Inspection Report* (Inspection Report) taken at the time of the importation would be sighted by the DFIU for their records. The original inspection Report is numbered by the Customs Officer and stored in a manual filing system and kept for three years.

*Domestic Cooperation between Customs, Immigration and Related Authorities (c. IX.6):*

383. The RMI Customs, Immigration, Labour, the Marshall Islands Social Security Administration (MISSA), and Majuro Atoll Local Government (MALG) has a Memorandum of Agreement (MOA) on the sharing of financial information in relation to government taxes; it does not include the sharing of information for the purposes of detecting and deterring money laundering and terrorist financing. The MOA is currently under review by the Attorney General to include such information between these agencies.

384. The agreement also details the requirement for regular monthly meetings to be undertaken and other special meetings as and when required.

385. The RMI Customs currently has an MOU with the Ministry of Finance. The RMI Customs does not currently have an MOU with the Immigration Department; however, there is an informal agreement that Immigration officials when checking passports of departing passengers, to ask if any person is carrying in excess of US\$10,000.

*International Cooperation between Competent Authorities relating to Cross-border Physical Transportation of Currency (c. IX.7):*

386. The RMI works closely with the US Immigration and Customs Enforcement (ICE) given RMI's international flight connections are through either, Guam or Hawaii. Further, under the Compacts of Free Association, the US still provides support to the RMI on national security.

387. RMI is a member of the Oceania Customs Organization (OCO). During annual meetings, ML schemes are usually one of the topics for presentation, discussion and information sharing. In addition, RMI Customs works together with other Customs in the Pacific and Oceania region, including World Customs Organisation through the OCO; in 2008 the RMI hosted the OCO Annual Meeting in 2008.

*Sanctions for Making False Declarations / Disclosures (applying c. 17.1-17.4 in R.17, c. IX.8)*

388. The CDA provides for a number of penalties to be incurred for breaches against the Act. These include, in section 3(2), a fine not exceeding US\$50,000 for persons failing to declare currency on arrival or departure, and/or forfeiture of currency under section 10 of the CDA. There is no explicit provision for false declaration.

*Sanctions for Cross-border Physical Transportation of Currency for Purposes of ML or FT (applying c. 17.1-17.4 in R.17, c. IX.9):*

389. The sanctions imposed for the cross-border physical transportation of currency applies in two instances, the first being the failure to declare currency at the point of arrival or departure which incurs a fine on conviction of US\$50,000; and the second, failure or refusal to answer questions incurs a fine on conviction of US\$5,000 pursuant to sections 3(2) and 4(2) of the *Currency Declaration Act 2009* respectively. The RMI Customs has the power to seize currency pursuant to section 7 (1) for a period of 72 hours. Currency may be detained for a period greater than 72 hours by an order of the RMI High Court i.e. for an additional three months or beyond the end of the period of two years from the date of the first order under sections 7 (2) (a) and (b) respectively.

390. This process also applies to any craft, which includes any vehicle, aircraft or water craft or by way of any other transport.

391. The *Currency Declaration Act* does not explicitly cover legal persons (c. 17.1) or directors or senior managers of businesses (R17.3).

392. The RMI Customs has the power to apply sanctions, as mentioned previously. However, RMI Customs is required to apply to the RMI High Court for matters relating to extensions of time for detained currency, release of detained currency and forfeiture (c.17.2).

393. The sanctions contained in the CDA are limited, as described above, and are not broad or proportionate to the severity of the situation, nor does it provide for the withdrawal, restriction or suspension of licences.

*Confiscation of Currency Related to ML/FT (applying c. 3.1-3.6 in R.3, c. IX.10):*

394. Section 10 of the CDA provides for forfeiture of currency. While currency is detained under section 7, an application for the forfeiture of the whole or any part of it may be made to the High Court by an authorized officer. The Court under section 10 (2) may order all or any part of it, if it is satisfied that the currency or part is recoverable currency (i.e. obtained through unlawful means) or is intended for use in unlawful conduct. It is silent on currency actually used as an instrument of an offence.

395. As indicated in c. IX.3, there are provisional measures available. Under section 6, currency may be seized if there is a suspicion the funds are for an illegal purpose and these funds can be detained for a period of 72 hours. An extension may be requested from the RMI High Court as described earlier in this report.

396. In matters relating to the financing of terrorism, the penalties are outlined in the *Counter-Terrorism Act* Part II, Prohibition and Punishment which provides for criminal penalties and forfeiture, including liabilities of corporations, civil penalties, private causes of action and injunction/s against those carrying out terrorist activities, sections 106 – 112 respectively.

*Confiscation of Currency Pursuant to UNSCRs (applying c. III.1-III.10 in SR III, c. IX.11):*

397. The RMI Customs were not aware of how to locate the *UNSCR 1267* list relating to the Al-Qaida, the Taliban and Associated Individuals and Entities. This information was provided and the RMI Customs will look to this list on a regular basis.

*Notification of Foreign Agency of Unusual Movement of Precious Metal and Stones (c. IX.12):*

398. The cross-border movement of precious metals and stones is included in the CDA's definition of currency. The RMI Customs indicated, if unusual movement of precious metals and stones were located, either through the inwards Customs declaration or not, it would in the first instance notify the DFIU and the OAG. The matter would be discussed with the DFIU members (the Head of the DFIU, the Police Commissioner and the Chief of Customs and the Attorney General) and then the relevant foreign Customs agency would be notified.

399. To date, no cases of unusual movement of precious metals and stones have been declared or located.

*Safeguards for Proper Use of Information (c. IX.13):*

400. The RMI Customs does not have any specific policy in relation to the proper use of information. The sharing of cross-border information is managed on a case-by-case basis, and as previously mentioned, this is an informal process between the Chief of Customs, the Police Commissioner and the Head of the DFIU.

401. The types of records kept in relation to the sharing of information are those relating to email requests; these are kept in the computer but telephone conversations relating to requests are not recorded.

*Training targeting, data collection and enforcement (c.IX14)*

402. With regard to arriving passengers, the RMI Customs has an arrangement with airline companies to notify Customs if there is a suspicion of a passenger carrying large amounts of currency, either on their person, or results of x-rayed luggage at the point of origin.

*Supra-national approach (c.IX15)*

403. The RMI is not party to any supra-national arrangement on customs. Under section 241 of the Revised Compact of Free Association, the RMI is not included in the customs territory of the US.

*Additional Element—Computerization of Database and Accessible to Competent Authorities (c. IX.16)*

404. The RMI Customs has applied several elements of the *FATF International Best Practices Paper Detecting and preventing the illicit cross-border transportation of cash and bearer negotiable instruments*. It has set the declaration threshold lower than indicated by the FATF and has included precious metal and stones in the definition of currency.

405. The RMI did not have X-ray facilities in place at the time of the on-site. Funding to renovate the airport has been approved and this will provide x-ray facilities for passengers.

*Additional Element—Computerization of Database and Accessible to Competent Authorities (c. IX.17)*

406. The RMI Customs currently has a manual filing system in place for the recording of cross-border movement of currency and other customs related offences.

*Recommendation 30.1*

407. The number of Customs officers in the RMI during the on-site was 14. There are two Customs officers assigned to the Amata Kabua International Airport and the Delap/Uliga Sea Ports. The officers are familiar with the CDA; however, they have limited understanding of ML and FT issues.

*Recommendation 30.2*

408. The DPS completes a security check through Interpol prior to the commencement of employment of staff within the RMI Customs.

*Recommendation 30.3*

409. The RMI Customs has undergone limited training in relation to ML and FT, and there is a need to ensure they have access to similar training opportunities as the RMI DPS.

**Table: Training undertaken by the RMI Customs**

Training	Year	Duration	Location
Customs Modernization	2005	1 month	Taipei
Pacific Customs Management Program	2007	1 month	Australia
Pacific Customs Management Program	2009	1 month	Australia
Customs Administration Seminar	2009	2 weeks	Japan
Basic Investigation Techniques Training	2009	1 week	RMI
Intellectual Property	2009	3 days	Hawaii
Intellectual Property	2009	3 days	Hawaii
Identity and Intel Training	2010	2 weeks	FSM
Identity and Intel Training	2010	1 weeks	FSM

*Recommendation 32*

410. Since the passage of the CDA in 2009, no cross-border declarations of currency or bearer negotiable instruments have been made to Customs or any other authority. To date, there have been no identified instances of illegal cross-border movement of currency.

*Effectiveness*

411. The CDA provides the RMI Customs with adequate powers to check for cross-border movement of currency; however, it does not include the movement of currency through air/ sea cargo nor through the mail system. There are deficiencies in the current inward declaration form. The form does not include the definition of currency and there is no sanction mentioned for failure to declare or for false declaration. The RMI has not implemented a departure declaration system as yet.

412. It is difficult to establish the level of expertise of RMI Customs Officers as there appears to be a lack of training opportunities available. Although the law is recent, the RMI Customs has demonstrated its understanding of implementation issues and has managed to work well under the circumstances.

## 2.7.2 Recommendations and Comments

413. The following recommendations are made to enhance the RMI's physical cross border declaration system:

- Amend the CDA to include the declaration of currency and bearer negotiable instrument for the postal system and containerized cargo.
- Amend the CDA to explicitly include both natural and legal persons.
- Revise the current inward declaration form to include the definition of currency, and sanctions for failure to declare currency and for false declaration.
- Implement a departure declaration system to compliment the inwards declaration system in line with the CDA.
- Implement as a system which retains the information and identification data in instances where currency declared in excess of US\$10,000.
- Provide the legal basis for customs to share information with the DFIU, and formalise processes and procedures for the sharing and transferring of information among Customs, the DFIU, Immigration and other relevant agencies in the form of a MOU.
- Provide for a range of proportionate and dissuasive sanctions, including for false declaration.
- Implement procedures for the proper use and safeguarding of information reported or recorded.
- Upgrade the current manual system to a computerized database.

### 2.7.3. Compliance with Special Recommendation IX

	Rating	Summary of factors relevant to s.2.7 underlying overall rating
<b>SR.IX</b>	<b>NC</b>	<ul style="list-style-type: none"> <li>• Cross border currency declaration system does not include mail and cargo</li> <li>• CDA does not clearly cover legal persons.</li> <li>• Inwards RMI Customs declaration does not include a definition of 'currency' to include bearer negotiable instruments; and warning for failure to declare and/or false declaration.</li> <li>• No outwards currency declaration form available as required in the CDA.</li> <li>• Not clear if the RMI Customs has access to the UNSCR1267 list.</li> <li>• CDA does not provide for data to be retained for use by authorities.</li> <li>• No legal basis for the DFIU to receive or access cross border information</li> <li>• No broad nor proportionate sanctions available.</li> <li>• No adequate procedures to safeguard information</li> <li>• Lack of formalized information sharing arrangements</li> <li>• No clear implementation of the declaration system</li> </ul>
<b>R.30</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Lack of training, awareness and expertise in AML/CFT</li> </ul>

### 3. PREVENTIVE MEASURES —FINANCIAL INSTITUTIONS

#### 3.1. Risk of money laundering or terrorist financing

414. The RMI has a relatively small domestic financial sector with only two banks, two money remittance agencies, several non-deposit taking lenders, and three insurance intermediaries acting as agents for foreign underwriters. Cash remains a significant means of payment in the economy and no EFTPOS facilities are available. One bank issues debit cards and credit cards but these are not currently widely held by residents of the RMI. There are no registrations or licensing requirements for non-bank providers of financial services, except for the licensing requirement for providers of money or value transmission services, both formal and informal, under section 121 (1) of the CTA which has not yet been implemented by the RMI authorities. The authorities are aware of at least one informal money remitter, two non-deposit taking motor vehicle lenders and one life insurance intermediary that meet the statutory definition of financial institution or cash dealer but have not yet been subject to AML/CFT supervision, STR and CTR reporting requirements, or compliance monitoring by the Banking Commission. The Government owned Marshall Islands Development Bank, which provides both consumer and business loans but does not take deposits, also appears to be a financial institution under the *Banking Act* but is not yet subject to AML/CFT obligations or compliance monitoring by the Banking Commission.

415. Until the *AML Regulations 2002* were revised in 2010 there were no risk-based CDD requirements in place. There is no evidence that the non-bank domestic financial institutions have adopted risk based CDD in advance of the revised regulatory requirements. However, the authorities have advised that risk-based CDD policies and procedures including enhanced due diligence for high risk customers, and originator information requirements for wire transfers have been largely implemented within the two banks ahead of the passage of the revised regulations. With respect to the two banks, the BOG is an FDIC-insured branch of a US chartered bank and is therefore also required to comply with US AML/CFT requirements including the USA Patriot Act and US Bank Secrecy Act requirements, and CTR and STR reporting requirements through FINCEN. The Banking Commission has established from AML-focused onsite examinations and third party review reports that BOMI has also been implementing policies and procedures to comply with US AML/CFT requirements in advance of the revised RMI AML/CFT regulatory requirements becoming fully effective.

416. There are no offshore banks in RMI although the *Banking Act* provides for licensing of offshore banks. The authorities have advised that there is no intention to issue offshore banking licences. The evaluation team notes that offshore banking can significantly increase the risk of ML and FT and recommends that the authorities remove all references to offshore banks from the *Banking Act*. If there is sound justification to permit offshore banking at some future time, the authorities should then establish a robust separate offshore banking legislative framework consistent with international standards.

417. The RMI authorities have not yet carried out a national AML/CFT risk assessment. However, there are number of jurisdiction-specific factors which lead the assessment team to conclude that the domestic financial sector presents a moderately low risk of ML and FT at the present time, even though the comprehensive legislative requirements to achieve the full scope of FATF preventive measures have only recently been passed into law. These factors include: the small size of the financial sector which is dominated by two banks that are supervised for AML/CFT purposes; bank policies and procedures which prevent non face-to-face account opening; the absence of (inward) correspondent banking relationships; no use of third party intermediaries by the banking

sector; and a relatively low incidence of ML through financial institutions as identified from analysis of STR and CTR reports to the Banking Commission.

### **Laws, regulation and other enforceable means**

418. The legislative and regulatory framework for AML/CFT obligations applying to financial institutions and cash dealers comprises the following:

- Part XIII of the *Banking Act* (including amendments to sections 167 and 170A in June 2009).
- The revised *Anti-Money Laundering Regulations 2010*, as issued in May 2010, by the Banking Commissioner pursuant to the *Banking Act* (hereafter referred to as the revised *AML/CFT Regulations*). The Schedule and Appendix to the Regulations are an integral part of the regulatory requirements, for which the sanctions in section 7 apply.
- Advisory notices issued by the Banking Commissioner. Where such advisory notices are regulatory requirements issued pursuant to the Banking Commissioner's regulatory powers under the *Banking Act* or revised *AML/CFT Regulations*, they have the effect of "Other Enforceable Means".<sup>5</sup>
- Guidelines and other guidance issued by the Banking Commissioner to assist entities in complying with their obligations, which are not other enforceable means.

419. The Banking Commissioner has provided examples of Advisory notices issued to financial institutions and cash dealers as follows:

- i. Advisory A-05 – Notification of requirement for annual audit for AML/CFT compliance, issued to banks pursuant to section 134(11) of the *Banking Act*, in February 2005, which includes an annexed sample internal controls questionnaire.
- ii. Advisory A-10 (a) – Notification of the requirement for STRs in relation to the financing of terrorism pursuant to the 2009 amendments to the *Banking Act* sections 167 and 170A, issued on 13 August 2010.
- iii. Advisory A-10 (c) issued by the Banking Commission on 23 September 2010, providing a short grace period until 22 October 2010 for financial institutions and cash dealers to implement the revised *AML/CFT Regulations* that were passed in May 2010.

420. The Banking Commissioner has provided examples of AML/CFT guidance issued to subject entities as follows:

- i. Guidelines on suspicious transactions, and Preparation Guidelines for Suspicious Activity Report Form;

---

<sup>5</sup> Advisory notices A-05 and A-10(a) (see para 353) have the status of 'other enforceable means' as they set out regulatory requirements under the Banking Act. Sanctions for non-compliance with those requirements are respectively established in sections 164 and 181 of the Act. Advisory A-10(c) is a notice from the Banking Commissioner who subject entities are entitled to rely on but does not itself need to be enforceable against subject entities, as it is a temporary regulatory dispensation, rather than a regulatory requirement.

ii. Instructions and reporting form for Currency Transaction Report.

421. The evaluation team noted that these guidance materials do not appear to be directly enforceable in their own right and therefore do not have the character of ‘other enforceable means’. These guidance materials were all issued several years ago and should be updated to be consistent with the requirements and obligations set out in the amended *Banking Act* and revised *AML/CFT Regulations*.

422. A draft Bill has been prepared by the authorities which will amend section 167 to: (i) clarify the role of the Banking Commission in respect of the functions of the domestic financial intelligence unit; (ii) clarify that subsections (1) (f) and (g) which refer to guidelines and training provided by the Banking Commission to entities subject to the *Banking Act*, which currently refer to financial institutions only should also refer to cash dealers; and (iii) require that an annual report of the activities of the domestic financial intelligence unit and relevant statistics and typologies and trends be provided to Cabinet before the end of each financial year.

### Scope

423. “Financial institutions” and “cash dealers” as defined in the *Banking Act* are required to comply with all AML/CFT requirements of the RMI. Financial institutions include persons who conduct banking business, any person who carries on a business of lending, financial leasing, money transmission services, issuing and administering means of payment, portfolio management and advice, money and securities market services other financial sector business and safe custody services. Cash dealers include insurers and insurance intermediaries, currency dealing and exchange business, and casinos. Preventive measures covering the core AML/CFT requirements of customer due diligence, suspicious activity reporting, currency transaction reporting, and recordkeeping for financial institutions and cash dealers were previously set out in the *Banking Act* (sections 168 to 170, and 180) and the AML Regulations 2002.

424. The amendment to section 167 of the *Banking Act* passed in June 2009 extended the scope of the Banking Commission’s AML supervision, enforcement and information exchange powers to consistently encompass matters relating to proceeds of crime, ML activity, and the financing of terrorism.

425. The revised *AML/CFT Regulations* impose detailed obligations for: internal policies, procedures and audit; risk-based CDD; wire transfers, correspondent banking; non face-to-face transactions and new technologies; foreign branches and subsidiaries; and prohibition on dealings with shell banks. The Regulations also empower the Banking Commission to issue guidelines to assist compliance by financial institutions and cash dealers. The Regulations provide examples in Appendix 1 of situations where risk-based obligations should be applied, including enhanced due diligence for higher risk categories of customers and simplified due diligence for lower risk customers. Schedule 1 to the Regulations sets out procedures required to be followed in verifying identity for individuals, corporate entities, and partnerships or unincorporated businesses.

## 3.2. Customer due diligence, including enhanced or reduced measures (R.5 to 8)

### 3.2.1 Description and Analysis

#### Recommendation 5

*Prohibition of Anonymous Accounts (c. 5.1):*

426. Both the *Banking Act* and the revised *AML/CFT Regulations* prohibit financial institutions and cash dealers from opening or keeping anonymous accounts or accounts that are in fictitious or incorrect names. Although there is no provision in the *Banking Act* banning numbered accounts, in effect they are not permitted as financial institutions are required to maintain all accounts in the name of the account holder. Section 168 (1) of the *Banking Act* states that a financial institution or cash dealer shall maintain accounts in the name of the account holder. They shall not open or keep anonymous accounts or accounts which are not fictitious or incorrect names. This requirement is also covered by section 3B.1 of the revised *AML/CFT Regulations*. Section 3B.7 requires that all customer and transaction records must be available on a timely basis to the Banking Commission on request. The Banking Commission has confirmed through onsite examinations that bank accounts are recorded in the name of the account holder only.

*When CDD is required (c. 5.2):*

427. The revised *AML/CFT Regulations* requires financial institutions and cash dealers to undertake risk-based customer due diligence, in addition to the general CDD obligations contained in section 168 of the *Banking Act*. Section 3B.3 of the revised *AML/CFT Regulations* requires that financial institutions and cash dealers must identify and verify the identity of a customer at any time that the person: applies for a business relationship; seeks to engage in a threshold occasional transaction (one or more occasional transactions when the total value of the transactions exceeds \$10,000); seeks to carry out a wire transfer (except where a threshold exemption is issued under section 3M), or engages in a suspicious activity. The same measures are required where doubts have arisen as to the veracity or adequacy of previously obtained identification data on the person.

428. Section 3B.2 of the Regulations defines a “threshold occasional transaction” is one or more occasional transactions whereby the total value of the transactions exceeds US\$10,000. A “suspicious activity” is any business or transaction in any instance where there is suspicion that the person is involved in ML or FT.

*Identification measures and verification sources (c. 5.3):*

429. Both the *Banking Act* and revised *AML/CFT Regulations* require financial institutions and cash dealers to identify and verify the identity of the customer, whether they be occasional or usual clients, using reliable, independent source documents. Section 168 of the *Banking Act* requires financial institutions and cash dealers to record and verify customer identity by using documents providing convincing evidence of their legal existence and the powers of their legal representative, or any other official or private documents.

430. Section 3B.4 of the revised *AML/CFT Regulations* states that financial institutions and cash dealers are required to verify the identity of the physical customer by using reliable, independent source documents, data, or information as provided for in Schedule 1 of the Regulations. Paragraph 1 of Part A of the Schedule sets out comprehensive CDD procedures for verification of identity of individuals. Paragraph 2 of Part A requires that paragraph 1 shall also apply to the verification of identity of the beneficial owners of all financial institutions and cash dealers.

431. The Banking Commission has advised that detailed CDD identification and verification measures are in place in banks and other financial institutions consistent with this requirement. However, there has been no formal compliance monitoring conducted yet in respect of the more detailed requirements of the revised *AML/CFT Regulations*. Available identification documents used in RMI include:

- RMI Government-issued national identity card (optional), passport, or drivers licence which all contain photo ID;
- Other officially-used ID such as Marshall Island Social Security card; and
- For customers who are RMI nationals living in the outer islands and do not have these documents, the local bank has established an in-house ID card for bank transactions following identity verification using credible third party referees.

*Identification of Legal Persons or Other Arrangements (c. 5.4):*

432. The revised *AML/CFT Regulations* requires financial institutions and cash dealers to identify and verify the identity/establishment of customers who are legal persons or legal arrangements. Section 3B.5 of the Regulations requires that for customers who are legal persons or legal arrangements, financial institutions and cash dealers must obtain and verify: the customer's name and legal form, including by obtaining proof of incorporation or similar evidence of establishment or existence (such as a trust instrument); the names and addresses of members of the customer's controlling body (such as directors or trustees); the legal provisions that set out the power to bind the customer; the legal provisions that authorize persons to act on behalf of the customer; and the identity of the physical person purporting to act on behalf of the customer, using source documents as required under section 3B.4.

433. Part B of Schedule 1 of the Regulations sets out detailed procedures for verification of corporate entities and Part C sets out detailed requirements for verification of identity of partnerships or unincorporated businesses.

434. Financial institutions in RMI have well established and robust procedures for obtaining necessary documents and verification with respect to corporate entities that are customers. However, the detailed requirements of the Regulations have only recently been advised to the institutions and were still being implemented at the time of the evaluation team visit. Compliance monitoring to assess the effectiveness of implementation of the new detailed requirements has yet to be carried out by the Banking Commission.

*Identification of Beneficial Owners (c. 5.5; 5.5.1 & 5.5.2):*

435. Section 3.C of the revised *AML/CFT Regulations* establishes requirements on financial institutions and cash dealers for the determination of the beneficial owner of the customer. Under section 1 of the revised *AML/CFT Regulations*, beneficial owner means the "beneficiary" as defined in the Trust Act 1994, i.e. a person entitled to benefit under a trust or in whose favour discretion to distribute property held on trust may be exercised. This definition is not consistent with FATF definition of beneficial owner, i.e. the natural person who ultimately owns or controls the customer and/or the person on whose behalf a transaction is being conducted.

436. Section 3C.1 of the revised *AML/CFT Regulations* requires financial institutions and cash dealers to take reasonable measures to determine if a customer is acting on behalf of one or more beneficial owners. If so, the financial institution or cash dealer should take reasonable steps to verify the identity of the beneficial owner by using relevant information or data obtained from a reliable source such that the financial institution and cash dealer is satisfied that it knows the identity of the beneficial owner. Section 3B.5 requires that for customers who are legal persons or legal arrangements, the financial institution and cash dealer must obtain and verify the identity of the

physical person purporting to act on behalf of the customer, using source documents as provided in section 3B.4.

437. For customers that are legal persons or legal arrangements, the Regulations require financial institutions and cash dealers to take reasonable measures to understand the ownership and control structure of the customer, including the ultimate natural person(s) who owns or controls a legal person, including natural persons with a controlling interest as described in section 3C. With respect to companies, limited partnerships, or similar arrangements, identification should be made of each natural person who owns directly or indirectly 10 percent or more of the vote or value of an equity interest in; and exercises management of the company, limited partnership or similar arrangement. With respect to a trust or similar arrangements, identification should be made of the settler (s), trustee(s), and beneficiaries whose vested interest is 10 percent or more of the value of the trust corpus.

438. However, from discussions with financial institutions, it is not clear that identification details of the ultimate beneficial owner (natural person) of a legal person are always obtained by financial institutions in RMI at present.

*Information on Purpose and Nature of Business Relationship (c. 5.6):*

439. Section 3C.1 of the revised *AML/CFT Regulations* requires financial institutions and cash dealers to obtain information on the purpose and intended nature of the business relationship. Banks and the non-deposit taking finance company are already carrying out this requirement as a matter of course.

*Ongoing Due Diligence on Business Relationship (c. 5.7; 5.7.1 & 5.7.2):*

440. Section 3I.1 of the revised *AML/CFT Regulations* requires financial institutions and cash dealers to conduct monitoring of customer transactions. Monitoring must include the scrutiny of customer transactions to ensure that they are being conducted according to the financial institution and cash dealer's knowledge of the customer and the customer profile, and where necessary, the source of funds, and may include predetermined limits on amount of transactions and type of transactions. Section 3H.1 requires that financial institutions and cash dealers must gather and maintain customer information on an ongoing basis. Documents, data, or information collected under the CDD process should be kept up to date and relevant by taking reviews of existing records at appropriate times, particularly for higher risk categories of customers or business relationships.

441. Banks and the non-deposit taking finance company have already implemented transaction monitoring, review of patterns of transactions, and periodic updating of CDD information.

*Risk—Enhanced Due Diligence for Higher Risk Customers (c. 5.8):*

442. Section 3K of the revised *AML/CFT Regulations* requires financial institutions and cash dealers to conduct enhanced CDD for customers and beneficial owners identified as high risk customers and politically exposed persons that are likely to pose a higher risk of ML or FT ("enhanced CDD"). Enhanced CDD should include reasonable measures to establish the source of wealth and source of funds of customers and beneficial owners identified as higher risk customers and politically exposed persons, and should be applied at each stage of the CDD process. Enhanced CDD procedures for non-face to face transactions may include: certification of documents presented; requisition of additional documents to complement those that are required for face to face customers; or development of independent contact with the customer.

443. Part B of Appendix 1 to the Regulations, sets out the relevant factors in determining if a customer is higher risk include if the person, is:

- a. *establishing customer relations other than “face to face”;*
- b. *a non-resident, or if the nationality, current residency, and previous residency of the person suggests greater risk of ML or TF;*
- c. *connected with jurisdictions that lack proper standards in the prevention of ML or TF;*
- d. *a politically exposed person (“PEP”) or linked to a PEP;*
- e. *a high net worth individual, especially if the potential customer is a private banking customer or the source of funds is unclear;*
- f. *engaged in a business that is particularly susceptible to money laundering or terrorism financing;*
- g. *a legal person or arrangement that is a personal asset holding vehicle;*
- h. *a legal person or arrangement whose ownership structure is complex for no good reason;*
- i. *a company with nominee shareholders or shares in bearer form; and*
- j. *higher risk for other reasons based on relevant information.*

444. The banks and the non-deposit taking finance company have established AML/CFT customer risk grading frameworks to identify higher risk customers and apply enhanced due diligence requirements.

445. One bank in RMI provides internet banking facilities for customers, to make transfers between accounts at the bank and payments to banks offshore. The offshore payment transactions are subject to head office monitoring to ensure compliance with US regulatory compliance. (There are no electronic transactions between banks in RMI.) The bank also provides Visa debit card access to its accounts and a limited number of credit card facilities for customers. Each of these types of accounts is subject to head office approval and scrutiny at opening and on an ongoing basis.

446. The other bank offers mobile phone banking for transactions between accounts at the bank and for cash withdrawals and deposits with a number of approved merchants in outlying islands, and bill payments to businesses holding accounts at the bank. The mobile phone transactions facility is provided to existing customers who have completed full account opening and CDD procedures. It requires an additional chip card to be inserted in the customers’ mobile phone to provide account access and security arrangements, and the facilities are subject to detailed issuing and operating policies and procedures, and transactions limits.

447. The Banking Commission has not yet carried out compliance monitoring with respect to the new enhanced due diligence requirements or the policies and procedures in place for the mobile phone banking facility.

*Risk—Application of Simplified/Reduced CDD Measures when appropriate (c. 5.9):*

448. Section 3L of the revised *AML/CFT Regulations* allows financial institutions and cash dealers to apply simplified CDD measures for lower risk customers, but only if permission has been granted by the Banking Commission for procedures that comply with the requirements of the section. In general, customers must be subject to the full range of CDD measures including the requirement to identify the beneficial owner. Where the risk of ML and FT is lower and where information on the identity of the customer and the beneficial owner of the customer is publicly available, or where adequate checks and controls exist in national systems, in such circumstances it would be reasonable

for financial institutions and cash dealers to apply simplified or reduced CDD measures when identifying and verifying the identity of the customer or beneficial owner.

449. Examples of lower risk customers are set out in Part C of Appendix 1 of the Regulations, including:

- a. *Any other financial institution or cash dealer (other entities that are subject to supervision by the Banking Commission under the Regulations);*
- b. *non-resident financial institutions that are subject to adequate regulation and supervision as limited by section 3L;*
- c. *public companies (or other legal persons or legal arrangements) quoted on an exchange regulated by the Banking Commission( there are no such exchanges at present), and certain public companies quoted on a foreign exchange approved for this purpose by the Banking Commission that is subject to adequate supervision and providing the company is subject to adequate regulatory disclosure requirements, as limited by section 3L;*
- d. *domestic government administrations or enterprises, and certain foreign government administrations or enterprises as limited by section 3L;*
- e. *life insurance policies where the annual premium is no more than \$1,000.00 or a single premium of no more than \$2,500.00;*
- f. *insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral;*
- g. *pension, superannuation, or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;*
- h. *beneficial owners of non-resident pooled accounts, provided they are subject to adequate regulation and supervision as limited by 3L;*
- i. *small scale accounts and micro-credit accounts with an annual turnover of under \$200.00.*

450. Non-resident and foreign entities described in Appendix 1 (Part C (b), (c), (d) and (h)) may only qualify for reduced CDD if they are located in a jurisdiction that is implementing the FATF standards effectively. In making this determination, financial institutions and cash dealers should take into account the information available on whether these countries adequately apply the FATF standards, including by examining the approved list provided by the Banking Commission and reports, assessments, and reviews published by FATF, APG, IMF, and World Bank.

451. The Banking Commission has not yet granted any authorizations or approvals for simplified CDD under section 3L of the revised *AML/CFT Regulations*. Simplified CDD measures are not acceptable whenever a customer has been identified by the Banking Commission as non-complying with the FATF standards, or for which the financial institution and cash dealer have independent credible reason to believe are not complying with the FATF standards, or for any reason that there is suspicion of ML or FT or specific higher risk scenarios apply.

452. Simplified CDD has been implemented in practice to date only in limited circumstances, such as by one bank where bank customers in the outer islands do not have access to a full range of identification documentation. Such instances relate only to low value, low risk transactions and accounts, where an independent referee may be used to confirm identity, in addition to the social

security card, and the customer will then be given a bank-generated identification document to use for future transactions.

*Risk—Simplification / Reduction of CDD Measures relating to overseas residents (c. 5.10):*

453. Section 3L.3 of the revised *AML/CFT Regulations* requires that simplified or reduced CDD measures when applied to customers that are residents in another country is limited to countries that are in compliance with and have effectively implemented the FATF standards. The approval of the Banking Commissioner is also required, under section 3L.1.

*Risk—Simplified/Reduced CDD Measures Not to Apply when Suspensions of ML/TF or other high risk scenarios exist (c. 5.11):*

454. Section 3L.4 of the revised *AML/CFT Regulations* states that simplified or reduced CDD measures are not acceptable whenever there is a suspicion of ML, FT, or in specific higher risk scenarios.

*Risk Based Application of CDD to be Consistent with Guidelines (c. 5.12):*

455. Section 3A. 2 of the revised *AML/CFT Regulations* states that CDD must be applied on a risk basis, which must include enhanced CDD for higher risk customers and politically exposed persons and may include simplified CDD for lower risk customers. Examples of high risk and low risk categories of customers are provided in Appendix 1 of the Regulations.

456. Both banks and the non-deposit taking finance company have established internal customer risk classification systems with respect to the type of customer, nature of business and potential AML/CFT risk factors which will assist in applying the new requirements for higher risk and lower risk customers. There is a lack of further guidance to assist entities to apply the risk-based approach to CDD.

*Timing of Verification of Identity—General Rule (c. 5.13):*

457. Section 3B.3 of the revised *AML/CFT Regulations* requires that in order to ensure proper customer identification, the financial institution and cash dealer must identify and verify the identity of the customer at any time that the person applies for a business relationship; or the person seeks to engage in a threshold occasional transaction. Note that under section 3A.1, the CDD obligations in respect of customers include the beneficial owners of the customer.

*Timing of Verification of Identity—Treatment of Exceptional Circumstances (c.5.14 & 5.14.1):*

458. Section 3D of the revised AML/CFT Regulation allows financial institutions and cash dealers to delay completion of the verification of the identity of the customer applying for a business relationship or engaging in a threshold occasional transaction, and of beneficial owners, but only if permission has been granted by the Banking Commission where the financial institution and cash dealer presents a procedure that complies with the procedures and requirements of section 3D. The section further states that financial institutions and cash dealers may delay verification only if: verification occurs as soon afterwards as reasonably practical, the delay is essential to not interrupt the normal course of business, and the ML and FT risks are effectively managed. Procedures to manage risk concerning delayed customer identification should include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed, and enhanced

monitoring of large and complex transactions being carried out outside of the expected norms for that type of relationship.

459. Appendix 1 Part A of the revised *AML/CFT Regulations* provides examples of situations where it may be essential not to interrupt the course of the normal conduct of business as followed including: non face-to-face business; securities transactions; and life insurance in relation to identification and verification of the beneficiary under the policy, which may take place after the business relationship with the policyholder is established, but in all such cases, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

460. Banks have confirmed that such risk mitigation measures are in place where verification of identity cannot be completed at the time of opening a business relationship. No business relationships are opened or occasional transactions conducted without face to face contact.

*Failure to Complete CDD before commencing the Business Relationship (c. 5.15):*

461. Section 3G.1 of the revised *AML/CFT Regulations* requires that financial institutions and cash dealers should not accept as customers those persons whose identity and beneficial owner as required in 3B, 3C, and 3D cannot be assured or for whom sufficient information to form a customer profile cannot be gathered. In such cases, financial institutions and cash dealers should determine if they should file a suspicious activity report.

*Failure to Complete CDD after commencing the Business Relationship (c. 5.16):*

462. Section 3J.1 of the revised *AML/CFT Regulations* requires that if the financial institution and cash dealer has already commenced a business relationship and is unable to comply with the CDD required for a customer, it should terminate the customer relationship and determine if it should file a suspicious activity report. Banks advise that such procedures are in place.

*Existing Customers—CDD Requirements (c. 5.17):*

463. Section 3A.3 of the revised *AML/CFT Regulations* states that CDD must be applied to existing customers on the basis of materiality and risk, and CDD must be conducted on such existing relationships at material times. Banks are in the process of progressively obtaining additional CDD information from existing customers where documentation is considered less than complete. It is noted that this process will be more challenging with respect to low value personal accounts held by customers in remote outer islands. The Banking Commission has not yet carried out compliance monitoring for this new requirement.

*Existing Anonymous-account Customers – CDD Requirements (c. 5.18):*

464. Section 3A.4 of the revised *AML/CFT Regulations* requires that CDD must be applied to any existing customers that have anonymous accounts or accounts in fictitious names.

## **Recommendation 6**

*Foreign PEPs – introduction*

465. The compliance obligations in respect of foreign PEPs and other higher risk customers are contained in section 3K of the revised *AML/CFT Regulations*. PEPs are defined in section 1(b)(16), and are limited to foreign PEPs. The authorities have advised that both banks and the non-deposit

taking finance company have established measures for foreign PEPs consistent with FATF Recommendation 6 prior to the commencement of the new requirements. One money remitter has procedures in place to identify foreign PEPs who are occasional customers. However, it is not clear whether the new requirements have yet been fully implemented by other non-bank financial institutions and cash dealers, as the Banking Commission has not yet carried out compliance monitoring for the new foreign PEP requirements.

*Foreign PEPs—Requirement to Identify (c. 6.1):*

466. Section 3K.1 of the revised *AML/CFT Regulations* requires that financial institutions and cash dealers must apply enhanced CDD for customers that are likely to pose a higher risk of ML or FT (“enhanced CDD”). Appendix 1 Part B, 4 provides additional information on procedures that may be appropriate for determining who is a PEP, including: seeking relevant information from the potential customer; referring to publicly available information; and making access to commercial electronic databases of PEPs.

*Foreign PEPs—Risk Management/approval (c. 6.2; 6.2.1):*

467. Section 3K.5 of the revised *AML/CFT Regulations* requires that financial institutions and cash dealers must put in place appropriate risk management systems to determine whether a potential customer or the beneficial owner is a high risk customer or a politically exposed person. Section 3K.2 of the revised *AML/CFT Regulations* requires that no customers and beneficial owners identified as higher risk customers and politically exposed persons should be accepted as a customer unless a senior member of the financial institution and cash dealer’s management has approved. Section 3K.3 of the *AML/CFT Regulations* requires that where a customer or beneficial owner has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a higher risk customer or politically exposed person, financial institutions and cash dealers must obtain senior management approval to continue the business relationship.

*Foreign PEPs—Requirement to Determine Source of Wealth and Funds (c. 6.3):*

468. Section 3K.1 of the revised *AML/CFT Regulations* requires that enhanced CDD should include reasonable measures to establish the source of wealth and source of funds of customers and beneficial owners identified as higher risk customers and politically exposed persons. Enhanced CDD should be applied to customers and beneficial owners identified as higher risk customers and politically exposed persons at each stage of the CDD process.

*Foreign PEPs—Ongoing Monitoring (c. 6.4):*

469. Section 3K.4 of the revised *AML/CFT Regulations* requires that where financial institutions and cash dealers are in a business relationship with a higher risk customer or a politically exposed person, they must conduct enhanced ongoing monitoring of that relationship.

*Domestic PEPs—Requirements (Additional Element c. 6.5):*

470. There are no requirements for enhanced CDD measures for domestic PEPs. However, the local bank applies the same measures for domestic PEPs as for foreign PEPs, and broadly similar procedures are adopted by the foreign bank.

*Domestic PEPs—Ratification of the Merida Convention (Additional Element c. 6.6):*

471. The RMI is not a party to the UN Convention on Corruption.

## **Recommendation 7**

### *Cross Border Correspondent Accounts and Similar Relationships – introduction*

472. Section 3N (subsections 1 to 6) of the revised *AML/CFT Regulations* establishes RMI's AML/CFT framework for correspondent banking relationships, but approval of establishing correspondent relationships and documentation of AML/CFT responsibilities for each institution are not covered by the revised *AML/CFT Regulations*. The authorities have advised that there are no correspondent banking relationships provided by banks in RMI, and that banks have adopted policies and practices consistent with the requirements of FATF Recommendation 7. The local bank has appropriate policies and procedures in place to meet US requirements as a respondent bank and the foreign bank complies with US correspondent banking requirements as directed from the head office in Guam.

#### *Requirement to Obtain Information on Respondent Institution (c. 7.1):*

473. Section 3N.2 of the revised *AML/CFT Regulations* requires that banks must develop and implement policies and procedures concerning correspondent banking and gather sufficient information about respondent banks to understand their business and determine from publicly available information the reputation of the institution, quality of supervision, and whether it has been subject to a ML or terrorism financing investigation or regulatory action.

#### *Assessment of AML/CFT Controls in Respondent Institution (c. 7.2):*

474. Section 3N.2 of the revised *AML/CFT Regulations* requires that in order to provide correspondent banking services, a bank must first assess the respondent's controls against ML and FT and determine that they are adequate and effective. A bank should, in general, establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the bank is effectively supervised by the relevant authority. In particular, a bank should not establish or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which the bank has no presence and which is unaffiliated with a regulated financial group (i.e. a shell bank).

#### *Approval of Establishing Correspondent Relationships (c. 7.3):*

475. No requirements are currently in place to directly meet this criterion. The Banking Commissioner has advised that RMI intends to amend the *AML/CFT Regulations* soon to include a requirement regarding "obtaining approval from senior management before establishing new correspondent relationships".

#### *Documentation of AML/CFT Responsibilities for Each Institution (c. 7.4):*

476. No requirements are currently in place to directly meet this criterion. The Banking Commissioner has advised that RMI intends to amend the *AML/CFT Regulations* soon to include a requirement to document the AML/CFT responsibilities for each institution as one of its amendments.

#### *Payable-Through Accounts (c. 7.5):*

477. Section 3N.6 of the revised *AML/CFT Regulations* requires that particular care should be exercised where the bank's respondent allows direct use of the correspondent account by third parties to transact business on their own behalf (i.e. payable-through accounts). A bank must be satisfied

that the respondent bank has performed the customer due diligence required in these Regulations for those customers that have direct access to the accounts of the correspondent, and that the respondent is able to provide relevant customer identification information on request of the correspondent. No payable through accounts are provided as part of correspondent bank facilities in RMI.

## **Recommendation 8**

### *Misuse of New Technology for ML/FT (c. 8.1):*

478. Section 3N.7 of the revised *AML/CFT Regulations* requires financial institutions and cash dealers to have policies in place and take such measures as are needed to prevent the misuse of technological developments in ML or FT schemes. Internet banking facilities are available to account holders of one bank, and the other bank has made available secure mobile phone banking transactions available to account holders using chip-based password protection. Comprehensive AML/CFT policies and procedures are in place in both cases. However, the Banking Commission has not yet carried out compliance monitoring to confirm the effectiveness of policies and procedures are in place with respect to mobile phone banking facilities.

### *Risk of Non-Face to Face Business Relationships (c. 8.2 & 8.2.1):*

479. Section 3N.8 of the revised *AML/CFT Regulations* requires that financial institutions and cash dealers have policies and procedures in place to address specific risks associated with non face-to face business relationships or transactions. These policies should apply when establishing customer relationships and when conducting ongoing due diligence. This should include specific and effective CDD procedures that apply to non face-to-face customers. The authorities have confirmed that financial institutions and cash dealers do not conduct non-face to face business. All account opening arrangements and occasional transactions require the customer to be identified at the physical office.

## **Effectiveness**

480. **Recommendation 5.** The scope of the CDD requirements under the revised *AML/CFT Regulations* is generally consistent with the requirements of Recommendation 5. However, the new regulatory requirements are still being implemented in some cases. Several entities that meet the definition of financial institution or cash dealer do not yet appear to be subject to AML/CFT obligations. Effectiveness of arrangements to comply with the detailed obligations of the revised *AML/CFT Regulations* has not yet been verified by the Banking Commission through compliance monitoring. Therefore effectiveness can only be show in part at the present time.

481. **Recommendation 6.** The two banks, finance company and money remitter have effective measures in place with respect to foreign PEPs, however effectiveness has not yet been established for other non-bank financial institutions and cash dealers.

482. **Recommendation 7.** No correspondent banking facilities are currently provided by banks in RMI but they have established polices consistent with FATF Recommendation 7. However, two of the essential criteria are not yet adopted through legal measures.

483. **Recommendation 8.** Measures to manage the risk of non-face to face business have been effectively achieved as non-face to face business is not carried out at present. Banks have established robust policies and procedures to date where new technologies have been adopted. Effectiveness of arrangements in respect of new technologies has not yet been verified through compliance monitoring.

### 3.2.2. Recommendations and Comments

484. **Recommendation 5.** The banks have already implemented policies and procedures to meet a significant proportion of the CDD requirements of the revised *AML/CFT Regulations*. The RMI authorities should take further steps to ensure all entities meeting the definition of non-bank financial institution or cash dealer are aware of their CDD compliance obligations. The authorities should undertake outreach regarding the new obligations, issue comprehensive guidance on risk based CDD and the detailed obligations under the Regulations, and subsequently obtain off-site compliance monitoring information or conduct on-site reviews to confirm that the full range of the new obligations are fully implemented.

485. The authorities should ensure that financial institutions and cash dealers have a proper understanding of the need to take reasonable measures to determine the ownership and control structure, and the ultimate natural person(s) who control customers that are legal persons, and have implemented adequate policies and procedures in accordance with section 3C of the revised *AML/CFT Regulations*.

486. The definition of “beneficial owner” in the revised *AML/CFT Regulations* should be amended to be consistent with FATF Recommendations, i.e. “the natural person who ultimately owns or controls the customer and/or the person on whose behalf a transaction is being conducted”.

487. **Recommendation 6.** The RMI authorities should consider signing, ratifying and fully implementing the UN Convention on Corruption, including the obligation to apply FATF Recommendation 6 to domestic PEPs.

488. **Recommendation 7.** The revised *AML/CFT Regulations* (section. 3N) should be amended to require senior management approval before establishing new correspondent relationships and to require both correspondent and respondent institutions to agree and record their respective AML/CFT responsibilities.

489. **Recommendation 8.** With respect to the requirements to prevent misuse of new technological developments, the Banking Commission should provide guidance on, and review the implementation of arrangements established for mobile banking facilities and other new technology innovations to ensure the associated AML/CFT risks are mitigated effectively.

### 3.2.3. Compliance with Recommendations 5 to 8

	Rating	Summary of factors underlying rating
<b>R.5</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• CDD obligations under the revised <i>AML/CFT Regulations</i> have not yet been implemented by a number of entities meeting the definition of financial institution or cash dealer.</li> <li>• Effectiveness of arrangements to comply with the detailed CDD obligations of the revised <i>AML/CFT Regulations</i> has not yet been verified by the Banking Commission through compliance monitoring.</li> <li>• Financial institutions and cash dealers do not have adequate policies and procedures to determine the natural persons who ultimately control customers who are legal persons.</li> <li>• The definition of beneficial owner in the revised <i>AML/CFT Regulations</i> is not consistent with that required under the FATF Recommendations.</li> </ul>
<b>R.6</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• PEPs obligations under the revised <i>AML/CFT Regulations</i> have not yet</li> </ul>

		<p>been implemented by a number of entities meeting the definition of financial institution or cash dealer.</p> <ul style="list-style-type: none"> <li>Effectiveness of arrangements to comply with obligations under the revised <i>AML/CFT Regulations</i> has not yet been verified through compliance monitoring.</li> </ul>
<b>R.7</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>No requirement for senior management authorization of correspondent bank accounts.</li> <li>No requirement for both parties to correspondent banking relationships to document their respective AML/CFT responsibilities.</li> </ul>
<b>R.8</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>Effectiveness of arrangements to comply with obligations under the revised <i>AML/CFT Regulations</i> has not yet been verified through compliance monitoring.</li> </ul>

### 3.3. Third Parties and Introduced Business (R.9)

#### 3.3.1. Description and Analysis

##### *Legal Framework:*

490. Section 3F of the revised *AML/CFT Regulations* establishes new requirements for the use of third party introducers, consistent with FATF Recommendation 9. Exclusions from the requirements of this section are provided for: outsourcing or agency relationships, i.e. where the agent is acting under a contractual arrangement with the financial institution or cash dealer to carry out its CDD functions; and for business relationships, accounts, or transactions between financial institutions and cash dealers for their clients.

491. The Banking Commission has confirmed that third party introducers are not currently used in RMI, and financial institutions' policies and procedures do not permit the use of intermediaries.

##### *Requirement to Immediately Obtain Certain CDD elements from Third Parties (c. 9.1):*

492. Section 3F.4 of the revised *AML/CFT Regulations* requires that in each instance of reliance on intermediaries, the financial institution and cash dealer must immediately obtain from the third party the CDD and beneficial ownership information required in sections 3B and 3C of the Regulations.

##### *Availability of Identification Data from Third Parties (c. 9.2):*

493. Section 3F. 4 of the revised *AML/CFT Regulations* states that while it is not necessary to obtain copies of the CDD documentation from the intermediary, financial institutions and cash dealers must take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the information obtained under section 3F.3 will be made available without delay, if requested.

##### *Regulation and Supervision of Third Party (c.9.3 applying R. 23, 24 & 29, c. 9.3):*

494. Section 3F.3 of the revised *AML/CFT Regulations* states that financial institution(s) and cash dealers may rely upon non-resident intermediaries if the financial institution and cash dealer is satisfied that the third party is adequately regulated and supervised and has measures in place to comply with the CDD requirements in this Regulation. Financial institutions and cash dealers must be satisfied that a non-resident intermediary is subject to, and is supervised in respect of ML and FT policies comparable with the FATF standards and has not been subject to any material disciplinary action that calls into question its execution of its policies. Financial institutions and cash dealers must ensure that non-resident intermediaries are located in a jurisdiction that is effectively implementing the FATF standards.

*Adequacy of Application of FATF Recommendations (c. 9.4):*

495. Section 3F.5 of the revised *AML/CFT Regulations* states that financial institutions and cash dealers may not rely upon intermediaries identified by the Banking Commission as non-compliant with the FATF standards, or intermediaries for whom the financial institution and cash dealer have independent credible reason to believe are not complying with the FATF standards.

*Ultimate Responsibility for CDD (c. 9.5):*

496. Section 3F.6 of the revised *AML/CFT Regulations* states that the ultimate responsibility for implementation of the customer due diligence requirements of these Regulations remains with the financial institution and cash dealer. The scope of the obligations for third party introducers is further clarified by sections 3F.7 and 3F.8 of the Regulations, which state that the requirements of section 3F do not apply to outsourcing or agency relationships, i.e. where the agent is acting under a contractual arrangement with the financial institution or cash dealer to carry out its CDD functions, or to business relationships, accounts, or transactions between financial institutions and cash dealers for their clients.

### 3.3.2. Recommendations and Comments

497. Third party intermediaries are not currently used by financial institutions in RMI. Robust regulatory requirements have been established to cover any future use of third party intermediaries or introducers.

### 3.3.3. Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
<b>R.9</b>	<b>C</b>	<ul style="list-style-type: none"> <li>The recommendation is fully observed.</li> </ul>

## 3.4. Financial Institution Secrecy or Confidentiality (R.4)

### 3.4.1. Description and Analysis

*Legal Framework:*

*Inhibition of Implementation of FATF Recommendations (c. 4.1):*

498. Section 154 (1) of the *Banking Act* 1987 requires officers and employees of licensed banks to preserve the secrecy and confidentiality of banking information. Section 154(1)(d) provides for the disclosure of banking information as an exception to the confidentiality requirements in order to comply with the provisions of the *Banking Act* or any other written law of the RMI. Subsection 2 of

section 154 requires that except in the performance of their duties under the Act, the Banking Commission and staff must maintain the confidentiality of information relating to the affairs of licensed banks that may come to their knowledge in the course of their business.

499. Section 167(1) (m) of the *Banking Act* specifically overrides any other secrecy provisions in the Act by granting the Banking Commission the authority and ability to obtain AML/CFT information from financial institutions and cash dealers under the powers of section 167, notwithstanding any secrecy or other restrictions on disclosure of information imposed elsewhere in the *Banking Act*.

500. The RMI authorities have confirmed that these information gathering powers have operated effectively in all cases and there is no evidence of constraint on the implementation of AML/CFT requirements because of secrecy.

### 3.4.2. Recommendations and Comments

501. The current legal provisions and powers to override secrecy requirements appear to be adequate and effective in practice.

### 3.4.3. Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
<b>R.4</b>	<b>C</b>	<ul style="list-style-type: none"> <li>The recommendation is fully observed.</li> </ul>

## 3.5. Record keeping and wire transfer rules (R.10 & SR.VII)

### 3.5.1. Description and Analysis

#### *Legal Framework:*

502. Both the *Banking Act* and the revised *AML/CFT Regulations* require financial institutions and cash dealers to maintain records on all transactions for at least six years following the completion of the transaction, and to maintain copies of relevant identification data, account files and business correspondence for at least 6 years following the termination of the business relationship (or longer if requested by the Banking Commission). The *AML Regulations 2002* had previously established record keeping requirements for transaction records and identification data. The Banking Commission has confirmed through onsite monitoring that the *Banking Act* record keeping requirements, which are consistent with Recommendation 10, have been fully implemented by financial institutions.

503. Obligations for maintaining originator information with wire transfers were initially established for all persons providing wire transfer services under section 121(2) of the *Counter Terrorism Act* which commenced in November 2003. The revised *AML/CFT Regulations* issued in 2010 include requirements consistent with SRVII in section 3M. Banks and money remitters have been meeting the requirements of SRVII as they are effectively subject to US requirements because they use US-based providers in all cases.

504. All cross border wire transfers in effect have a second layer of scrutiny regarding compliance with US wire transfer and OFAC list requirements, in addition to RMI requirements. The two sub-agents of an international remittance company send all transactions via its regional office based in another jurisdiction which includes system checks. The two banks do not have direct access to

SWIFT from their RMI operations. One bank sends outward wire transfers through its head office where they are further reviewed before transmission. Another bank relies on a correspondent bank in the US to provide SWIFT wire transfers on its behalf, and also uses the network of an international money remittance company. This bank's international remittance wire transfer business is not run as a separate business but is fully integrated into the bank's operations and AML/CFT policies and procedures.

505. In practice, there are currently no facilities for domestic wire transfers between banks or other financial institutions and cash dealers in RMI. Domestic inter-bank daily settlements are by manual exchange of cheques.

*Record-Keeping & Reconstruction of Transaction Records (c. 10.1 & 10.1.1):*

506. Section 169 (1) of the *Banking Act* and section 4 of the revised *AML/CFT Regulations* require that every financial institution or cash dealer shall retain records for all transactions for a period of at least 6 years after the completion of the transaction. These records shall be kept in a readily recoverable form. Section 169 (3) of the *Banking Act* requires that records regarding financial transactions shall contain particulars sufficient to identify the following:

- (a) name, address and occupation (or where appropriate business or principal activity) of each person:*
  - (i) conducting the transaction; or*
  - (ii) if known, on whose behalf the transaction is being conducted as well as the method used by the financial institution or cash dealer to verify the identity of each such person;*
- (b) nature and date of the transaction;*
- (c) type and amount of currency involved;*
- (d) the type and identifying number of any account with the financial institution or cash dealer involved in the transaction;*
- (e) if the transaction involves a negotiable instrument other than currency, the name of the drawer of the instrument, the name of the institution on which it was drawn, the name of the payee (if any), the amount and date of the instrument, the number (if any) of the instrument and details of any endorsements appearing on the instrument;*
- (f) the name and address of the financial institution or cash dealer, and of the officer, employee or agent of the financial institution or cash dealer who prepared the report;*
- (g) multiple transactions which, altogether, exceed ten thousand dollars, shall be treated as single transaction if they are undertaken by or on behalf of any one person during any twenty-four hour period. In such a case, when a financial institution or cash dealer, its employees, officers or agents have knowledge of these transactions, they shall record these transactions.*

*Record-Keeping for Identification Data (c. 10.2):*

507. Both section 169 (2) the *Banking Act* and section 3B.6 of the revised *AML/CFT Regulations* require financial institutions and cash dealers to maintain records of identification data, account files, and business correspondence for at least six years following the termination of the account or business relationship. Legible file copies must be made and retained of the relevant identification data, account files, and business correspondence for at least six years following the termination of an account or business relationship (or longer if requested by the Banking Commissioner).

*Availability of Records to Competent Authorities (c. 10.3):*

508. Section 3B.7 and 3C.9 of the revised *AML/CFT Regulations* require that financial institutions and cash dealers must ensure that all customer and transaction records are available on a timely basis to the Banking Commissioner upon request. The Banking Commission has confirmed that through onsite examinations and in the course of obtaining follow-up information on suspicious transactions that financial institutions and cash dealers comply with the record keeping and account file maintenance requirements and that such records are available on request.

*Obtain Originator Information for Wire Transfers (c.VII.1, applying c. 5.2 & 5.3 in R.5):*

509. Section 3M.1 of the revised *AML/CFT Regulations* requires that financial institutions and cash dealers must ensure that all persons ordering wire transfers obtain and maintain full originator information, and verify that the information is accurate and meaningful. This requirement is in addition to the general obligation established for all providers of wire transfer services under section 121 (2) of the CTA which requires that all credit and financial institutions and all persons, and their agents, that provide a service for the transmission of money or value by wire transfer, shall include accurate and meaningful originator information (including name, address and account number) on funds transfers and related messages that are sent, such information to remain with the transfer or related message through the payment chain. Section 3M.2 of the revised *AML/CFT Regulations* clarifies that full originator information includes: the name of the originator; the originator's account number (or a unique reference number if there is no account number); the originator's address; and the originator's identification card number. Financial institutions have established policies and procedures to comply with the originator information requirements of SRVII.

*Inclusion of Originator Information in Cross-Border Wire Transfers (c. VII.2):*

510. Section 3M.3 of the revised *AML/CFT Regulations* requires that for cross-border wire transfers (including batch transfers and transactions using a credit or debit card to effect a funds transfer), the ordering financial institution and cash dealer should be required to include full originator information in the message or payment form accompanying the wire transfer, except in the circumstances provided below for batch transfers. In addition, section 3M.6 states that if a cross-border wire transfer is contained within a batch transfer and is sent by a financial institution and cash dealer, it may be treated as a domestic wire transfer provided the requirements for domestic wire transfers are met. Section 3M.7 of the revised *AML/CFT Regulations* requires that every financial institution and cash dealer should ensure that non-routine transactions are not batched where this would increase the risk of ML or FT.

511. Section 3M.9 of the revised *AML/CFT Regulations* states that financial institutions and cash dealers may apply to the Banking Commission for authorization to exempt wire transfers below \$3,000 from the requirements of section 3M.3 and 3M.4 (which relate to the inclusion of originator information). Permission will be granted by the Banking Commission only if the financial institution or cash dealer presents a procedure that complies with section 3M. The Banking Commissioner has advised that no consideration has been given to approval of a de-minimis threshold at this stage.

512. The evaluation team notes that FATF Special Recommendation SRVII permits jurisdictions to adopt a de-minimis threshold of EUR/USD 1,000 only, for obligations to verify identity of the originator (criteria VII.1) and inclusion of originator information in cross-border wire transfers (criteria VII.2). If the Banking Commissioner used section 3M.9 of the revised *AML/CFT Regulations* to approve a de-minimis threshold of US\$3,000 for section 3M.3, it would not comply with criteria VII.2 (which permits a threshold of \$1000). Furthermore, any threshold approved in respect of

domestic wire transfers (section 3M.4) would not comply with criteria VII.3. The RMI authorities should amend section 3M.9 to be consistent with SRVII, reducing the available exemption to US\$1,000, and permitting it to apply to the cross border originator information requirements of section 3M.3 and the verification of originator information requirements of section 3M.1 only.

*Inclusion of Originator Information in Domestic Wire Transfers (c. VII.3):*

513. Section 3M.4 of the revised *AML/CFT Regulations* requires that for domestic wire transfers (including transactions using a credit or debit card as a payment system to effect a money transfer), the ordering financial institution and cash dealer must include either: full originator information in the message or payment form accompanying the wire transfer, or only the originator's account number or, where no account number exists, a unique identifier, within the message or payment form. Section 3M.5 of the revised *AML/CFT Regulations* states that section 3M.4 b may be used only if full originator information can be made available to the beneficiary financial institution and cash dealer and the Banking Commission within three working days of receiving a request. However, at present there are no domestic wire transfers between banks or other financial institutions in RMI.

*Maintenance of Originator Information (c. VII.4):*

514. Section 3M.8 of the revised *AML/CFT Regulations* requires that each intermediary in the payment chain should maintain all the required originator information with the accompanying wire transfer. Both banks and money transfer businesses are complying with this requirement. There are no categories of related domestic wire transfers that prevent the transmission of originator information by an intermediary institution.

*Risk Based Procedures for Transfers Not Accompanied by Originator Information (c. VII.5):*

515. Section 3M.10 of the revised *AML/CFT Regulations* states that beneficiary financial institutions and cash dealers must identify and handle wire transfers that are not accompanied by complete originator information on the basis of perceived risk of ML and FT. Procedures to address these cases should include the financial institution and cash dealer first requesting the missing originator information from the financial institution and cash dealer that sent the wire transfer. If the missing information is not forthcoming, the financial institution and cash dealer should consider whether, in all the circumstances, the absence of complete originator information creates or contributes to suspicion about the wire transfer or a related transaction. If the wire transfer is deemed to be suspicious, then it should send a suspicious activity report to the Banking Commission. In addition, the financial institution and cash dealer may decide not to accept the wire transfer. In appropriate circumstances, beneficiary financial institutions and cash dealers should consider restricting or terminating business relationships with financial institutions and cash dealers that do not comply with this section.

*Monitoring of Implementation of SR VII (c. VII.6):*

516. The Banking Commission conducts onsite inspections of financial institutions and cash dealers to ensure they are in compliance with wire transfer originator information requirements. However, no inspections have been carried out to date in respect of compliance the new detailed requirements of section 3M of the revised *AML/CFT Regulations*.

*Sanctions (c. VII.7, applying c. 17.1-17.4 in R.17)*

517. Sanctions may be applied with regards to non-compliance with wire transfer requirements consistent with other AML/CFT requirements as provided for banks under Part III of the *Banking Act*, and for all financial institutions and cash dealers under section 7 of the revised *AML/CFT Regulations*.

*Additional elements*

*Maintenance of Originator Information for incoming cross border wire transfers (c. VII.8):*

518. There is no mandatory requirement that all incoming cross border wire transfers must contain full and accurate originator information.

*Maintenance of Originator Information for outgoing cross border wire transfers below EUR/USD 1000 (c. VII.9):*

519. In the absence of an exemption under section 3M.9 of the revised *AML/CFT Regulations*, all outgoing cross-border wire transfers are required to contain full and accurate originator information.

### 3.5.2. Recommendations and Comments

520. Record keeping requirements have been in place for some time including obligations to maintain business files and correspondence, and appear to be well understood and effective. The Banking Commission confirms that compliance is good. However, there has only been an onsite inspection of one bank in the last three years to check that full compliance is being maintained.

521. The detailed wire transfer requirements have only just been introduced and took effect from October 2010, although originator information requirements have been in place since 2003. The relevant institutions (two banks and one money remitter) have been indirectly subject to US wire transfer requirements, and all providers obtain and maintain originator information as a matter of course. No onsite inspections have been carried out to verify compliance with the detailed new wire transfer requirements. There are no domestic wire transfers occurring between financial institutions in RMI.

522. The RMI authorities should amend section 3M.9 of the revised *AML/CFT Regulations* to be consistent with SRVII, reducing the available exemption to US\$1,000, and permitting it to apply to the cross border originator information requirements of section 3M.3 and the verification of originator information requirements of section 3M.1 only. Until the Regulations are amended accordingly, the Banking Commission should not approve a de-minimis wire transfer threshold that does not comply with SRVII. Current financial institution practice is satisfactory without any exemption which suggests that no such threshold exemption is necessary.

### 3.5.3. Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
<b>R.10</b>	LC	<ul style="list-style-type: none"> <li>Lack of recent compliance monitoring limits ability to assess effectiveness.</li> </ul>
<b>SR.VII</b>	LC	<ul style="list-style-type: none"> <li>The Banking Commissioner's powers to authorize a de-minimis threshold of US\$3,000 are not consistent with SRVII.</li> <li>Effectiveness of arrangements to comply with wire transfer obligations under the revised <i>AML/CFT Regulations</i> has not yet been verified</li> </ul>

		through compliance monitoring.
--	--	--------------------------------

### *Unusual and Suspicious Transactions*

## **3.6. Monitoring of Transactions and Relationships (R.11 & 21)**

### **3.6.1. Description and Analysis**

#### **Recommendation 11**

##### *Legal Framework:*

523. There is no obligation in the *Banking Act* for financial institutions to pay special attention to all complex and unusual large transactions. However, the revised *AML/CFT Regulations* include a new section 31 on “Ongoing Monitoring of Customer Transactions”, which meets the requirements of Recommendation 11 and establishes RMI’s unusual and complex transactions monitoring obligations.

##### *Special Attention to Complex, Unusual Large Transactions (c. 11.1):*

524. Section 31.2 of the revised *AML/CFT Regulations* requires that, “*financial institutions and cash dealers must pay special attention to all complex, unusual large transactions, or unusual pattern of transactions that have no visible economic or lawful purpose.*” The definition of “financial institutions” and “cash dealers” as set forth then the *Banking Act* is comprehensive and encompasses all entities which should be considered in an AML/CFT regime, even though some are not in actual existence in the RMI.

525. Both banks and the finance company interviewed demonstrated the understanding, ability, and capacity to note complex and/or unusual large transactions and have the appropriate systems in place to ensure monitoring of such transactions.

##### *Examination of Complex & Unusual Transactions (c. 11.2):*

526. Section 31.2 of the revised *AML/CFT Regulations* requires that “*financial institutions and cash dealers must examine as far as possible the background and purpose of such transactions and set forth their findings in writing.*”

527. The banks demonstrated their ability to examine the background and purpose of complex and unusual transactions. The global money remittance company did not provide any affirmation that such practices were taking place in the RMI, rather than it was indicated that such examination of transactions was conducted at their centralized global compliance department.

##### *Record-Keeping of Findings of Examination (c. 11.3):*

528. Section 31.2 of the revised *AML/CFT Regulations* requires that “*financial institutions and cash dealers must keep such findings available for examination by the Banking Commission, auditors, and any other competent authorities, for a minimum of six years. In such cases, financial institutions and cash dealers should determine if they should file a suspicious activity report.*” This requirement is in excess of the five years required under the standards.

529. The two banks maintain records for the duration required under the act and such reports are readily available to the Banking Commission upon request.

## Recommendation 21

*Special Attention to Countries Not Sufficiently Applying FATF Recommendations (c. 21.1 & 21.1.1):  
Examinations of Transactions with no Apparent Economic or Visible Lawful Purpose (c. 21.2):*

530. There are neither specific provisions in the *Banking Act* nor in the revised *AML/CFT Regulations* that require special attention to countries not sufficiently applying FATF recommendations. There are also no formalized procedures for the Banking Commission to maintain an adequate and updated listing of countries that are not sufficiently applying FATF Recommendations, nor do processes or procedures exist relating to advisories to financial institutions and cash dealers. Further, the Banking Commission has not issued advisories to financial institutions or cash dealers about weaknesses in the AML/CFT systems of other countries.

531. However, the Banking Commission has indicated it intends to introduce and/or amend the *AML/CFT Regulations* in the near future, and will include this requirement as one of its amendments. No specific dates have been provided for the promulgation and adoption of such regulations or amendments to existing regulations.

*Ability to Apply Counter Measures with Regard to Countries Not Sufficiently Applying FATF Recommendations (c. 21.3):*

532. There have not been any counter measures put in place due to the lack of regulations. The *Banking Act* does not contain empowering provisions allowing for the implementation of counter measures applied to countries that are not sufficiently applying FATF Recommendations. The Banking Commission has indicated that they will be seeking technical assistance in the near future to review and implement regulations that would adequately address this recommendation.

### 3.6.2. Recommendations and Comments

533. **Recommendation 11:** The revised *AML/CFT Regulations* contain all requirements pertaining to this FATF Recommendation. However, the Banking Commission should address the minor scope and implementation issues associated with the Commission's incomplete coverage of all non bank financial institution and cash dealers as defined under the *Banking Act*.

534. **Recommendation 21:** The Banking Commissioner should seek to amend the *Banking Act* or *AML/CFT Regulations* to meet the requirements of this Recommendation.

### 3.6.3. Compliance with Recommendations 11 & 21

	Rating	Summary of factors underlying rating
<b>R.11</b>	LC	<ul style="list-style-type: none"> <li>Detailed obligations under revised AML Regulations not fully implemented by some non-banks and cash dealers.</li> </ul>
<b>R.21</b>	NC	<ul style="list-style-type: none"> <li>There are no regulations in place to require special attention to business relations and transactions with high risk countries.</li> <li>There are no regulations in place to require financial institutions to examine and document the background of transactions which have no apparent economic or visible lawful purpose.</li> </ul>

		<ul style="list-style-type: none"> <li>There is no specific statute or regulation that allows for issuance or implementation of counter measures.</li> </ul>
--	--	--

### 3.7. Suspicious Transaction Reports and Other Reporting (R.13-14, 19, 25 & SR.IV)

#### 3.7.1. Description and Analysis

##### Recommendation 13 and SR.IV

##### *Legal Framework:*

535. The RMI's STR reporting framework is established under section 170, Part XIII of the *Banking Act* and section 5 of the revised *AML/CFT Regulations*.

##### *Requirement to Make STRs on ML and TF to FIU (c. 13.1 & IV.1):*

536. Section 170 (1) of the *Banking Act* states the following:

*“financial institutions and cash dealers shall, within 3 days of the transaction, report to the Commissioner all suspicious transactions, including but no limited to those which are ten thousand dollars (\$10,000) or more or multiple transactions which, altogether, exceed ten thousand dollars (\$10,000) if they are undertaken by or on behalf of any one person during any twenty-four hour period or, complex or unusual transactions, whether completed or not, and all unusual patterns of transactions, and otherwise significant but periodic transactions, which have no apparent economic or lawful purpose. The Commissioner may provide additional information or criteria to be used in identifying suspicious transactions under this subsection.”*

537. Section 170(1) does not specifically mention that STR reporting is required when it suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity. However this requirement is provided in section 5(a)(2)(c) of the revised *AML/CFT Regulations*, which defines a suspicious transaction as:

*“one which the financial institution or cash dealer knows, or suspects or has reasonable reasons to suspect that (i) involves funds or other assets derived from illegal activity:”*

538. The STR reporting requirements do not cover all predicate offences as discussed under FATF Recommendation 1.

539. Both the *Banking Act* and the revised *AML/CFT Regulations* require financial institutions and cash dealers to file an STR to the Commissioner of Banking, who is the head of the Financial Intelligence Unit.

##### *STRs Related to Terrorism and its Financing (c. 13.2, SRIV):*

540. Section 170A (1) of the *Banking Act* requires that *“financial institutions and cash dealers must report any transaction, attempted transaction or other activity where they suspect or have reasonable grounds to suspect that the transaction, attempted transaction or other activity may be*

*related to terrorism, terrorist acts, a terrorist organization, an individual terrorist, terrorist property or financing of terrorism.”*

541. Furthermore, section 170A(3) states “*such suspicion must be reported in writing to the Commissioner as soon as reasonably practicable and in any event, within three days of the forming of such suspicion.*”

542. Section 5(a)(1)(A) of the revised *AML/CFT Regulations*, states this requirement similarly, “*where a financial institution or casher dealer suspects that any transaction or any other activity could constitute or be related to terrorist financing, terrorist acts, a terrorist organization, an individual terrorist or to terrorist property the financial institution must report such suspicion to the Banking Commissioner within three working days of forming of such suspicion.*”

543. There has been no FT related STR submitted or received.

*Attempted Transactions (c. 13.3, SRIV):*

544. Section 170 (1) of the *Banking Act* states clearly that attempted transactions are covered. Section 5(a)(2)(b) of the revised *AML/CFT Regulations* states, “*which is conducted or attempted to be conducted at a financial institution or cash dealer*”.

545. Concerning FT, section 170A(2) of the *Banking Act* further states, “*All suspicious transactions, **attempted transactions** and other activities that may be related to terrorism, terrorist acts, a terrorist organizations, an individual terrorist, terrorist property or financing of terrorism must be reported regardless of the amount involved in the transaction, **attempted transaction\_or activity***”.

*Making of ML and TF STRs Regardless of Possible Involvement of Tax Matters (c. 13.4, c. IV.2):*

546. Section 5(a)(1) of the revised *AML/CFT Regulations* states that, “*Every financial institution and cash dealer shall file with the Banking Commission to the extent and in the manner required by this section 5, a Suspicious Activity Report (STR) of any suspicious transaction. A financial institution or cash dealer **may** also file a STR regarding any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by this section.*” However, as noted earlier, section 5(a)(2)(c)(i) defines a suspicious transaction as, “*involve funds or other assets derived from illegal activity*”.

547. The language of the revised *AML/CFT Regulations*, as it is written, may allow for non-reporting of tax matters.

*Additional Element - Reporting of All Criminal Acts (c. 13.5):*

548. There is no explicit requirement for reporting of all criminal acts, although as noted, the revised *AML/CFT Regulations* define a suspicious transaction to include all illegal activity.

## Recommendation 32

**Table: STRs received: Banks**

Year	Total
2005	46
2006	19

2007	34
2008	50
2009	34
2010	28
Total	211

## Effectiveness

549. As shown in the above table, the only entities reporting at this time are the two banks. Other entities that are non-banks, or defined as cash dealers in the *Banking Act* are not reporting to the DFIU, as required by statute and regulations. The reason given by these “non-reporting” institutions is that there have never been any transactions that have cause to be reported, given the relatively small scale of their transactions. The requirements of Recommendation 13 are covered fully in the *Banking Act* and Revised Regulation, with the exception of a requirement to report STRs regardless of whether they are thought, among other things, to involve tax related matters. The main deficiency is in effective implementation of this requirement by non bank financial institutions.

## Recommendation 14

### *Protection for Making STRs (c. 14.1):*

550. This requirement is covered in section 178 of the *Banking Act* which states, “no action, suit or other proceedings shall lie against any financial institution or cash dealer, or any officer, employee or other representative of the institution acting in the ordinary course of the person’s employment or representation, in relation to any action taken in good faith by that institution or person pursuant to this Act.” There has never been a case whereby a customer has attempted to take action against any of the persons listed for submitting a STR.

### *Prohibition Against Tipping-Off (c. 14.2):*

551. The prohibition against tipping off is covered in section 170 (4) of the *Banking Act* , “financial institution and cash dealers, its employees, officers or directors, shall not notify any person or entity other than the Commissioner or Attorney-General, a court of competent jurisdiction upon process issued, or other person as may be authorized by law, of the information, record, or report that has been prepared, or otherwise referred or furnished to the Commissioner, Attorney-General or court of competent jurisdiction, or other lawfully authorized person. Any person or financial institution or cash dealer who improperly discloses such information commits an offense, punishable by a fine of not more than \$2,000,000 or imprisonment for not more than 20 years, or both.”

552. The wording of section 170 (4) does not explicitly prohibit tipping off in the period after a suspicion has been formed and before a STR has been prepared or submitted.

### *Additional Element—Confidentiality of Reporting Staff (c. 14.3):*

553. Part VIII of the *Banking Act* and revised *AML/CFT Regulations* do not state any requirement for the FIU to protect the names and details of staff of financial institutions. Section 154 (2) nevertheless specifies the Commissioner and every officer and employee working under the Commissioner must adhere to the secrecy of all banking information.

## Recommendation 19

*Consideration of Reporting of Currency Transactions Above a Threshold (c. 19.1):*

554. Both the *Banking Act* and the revised *AML/CFT Regulations* require financial institutions and cash dealers to file a currency transaction report for any currency transaction exceeding US\$10,000 in a single transaction or multiple transactions within a 24 hour period when aggregated.

555. Section 180 of the *Banking Act* states that

*“the Commissioner of Banking may prescribe a regulation that requires a financial institution or cash dealer involved in a transaction for the payment, receipt or transfer of currency to file a report on the transaction with the Commissioner’s office and collect and maintain supporting documentation pertaining to such transaction. The requirements for when a currency transaction report must be filed may include, but are not limited to, a currency transaction that exceeds \$10,000 or involves multiple transactions, taken by or on behalf of a single person within a 24 hour period and, when aggregated, exceeds \$10,000.”*

556. This requirement is also provided in section 6 of the revised *AML/CFT Regulations*. Additional guidance on CTR reporting is provided in Instruction 7 - Currency Transaction Report issued by the Banking Commission. Statistics on CTR submitted are detailed under Recommendation 26.

*Additional Element— Computerized Database for Currency Transactions Above a Threshold and Access by Competent Authorities (c. 19.2):*

557. CTRs are filed electronically through the DFIU’s CTR-STR Reporting System. Reports are available to competent authorities for AML/CFT purposes upon written request to the Banking Commissioner/ Head of the DFIU.

558. The computerized or digitized filing of CTRs is implemented only for the two banks. Cash dealers are not covered under this electronic reporting regime.

*Additional Element—Proper Use of Reports of Currency Transactions Above a Threshold (c. 19.3):*

559. There are safeguards in place within the Banking Commission to ensure that filed CTRs are secured and are disseminated to designated persons only upon a written request. Only members of the national coordinating committee are allowed access to CTRs.

## **Recommendation 25**

*Feedback to Financial Institutions with respect to STR and other reporting (c. 25.2):*

560. There is currently no mechanism in place to provide financial institutions and cash dealers with adequate and appropriate feedback on STR filings. Banks indicated that there are no regular communications, follow up and/or feedback regarding filed STRs or CTRs which have been acted upon by the DFIU.

561. The banks indicated that there have been no communications from the Banking Commission on matters relating to guidelines issued.

### **3.7.2. Recommendations and Comments**

562. The following actions are recommended to enhance RMI’s monitoring and STR reporting regime:

**Recommendation 13**

- The remaining FATF predicate offences, once incorporated into an amended *Banking Act*, should be reflected in the revised *AML/CFT Regulations*, and in further guidance to financial institutions and cash dealers.
- Tax matters and other suspicious transactions related to any criminal act should be clarified in the revised *AML/CFT Regulations* to remove any doubt or confusion caused by the current wording.
- Undertake measures to enhance compliance with STR reporting requirements with non bank financial institutions and cash dealers.

**Recommendation 14**

- Amend section 170(4) of the *Banking Act* to prohibit tipping off in the period after a suspicion has been formed and before a STR has been prepared or submitted.

**Recommendation 25**

- The Banking Commission/DFIU should establish internal guidelines and procedures to provide consistent, timely, and appropriate feedback to financial institutions and cash dealers on STR reporting to enhance the effectiveness of the reporting regime.
- The *Banking Act* and/or regulations should be amended to include specific provisions that protect the identity or maintain the confidentiality of person(s) reporting STRs to the DFIU.

**3.7.3. Compliance with Recommendations 13, 14, 19 and 25 (criteria 25.2), and Special Recommendation IV**

	Rating	Summary of factors underlying rating
<b>R.13</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• STR reporting does not cover all predicate offences.</li> <li>• STR filing on tax matters or on suspected proceeds of other crimes defined under RMI laws are not specifically provided for in the <i>Banking Act</i> or revised <i>AML/CFT Regulations</i>.</li> <li>• The lack of STR reporting from non-banking entities indicates weakness in effectiveness of implementation.</li> </ul>
<b>R.14</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• No explicit provision in section 170 (4) of the <i>Banking Act</i> to prohibit tipping off in the period after a suspicion has been formed and before a STR has been prepared or submitted.</li> </ul>
<b>R.19</b>	<b>C</b>	<ul style="list-style-type: none"> <li>• The recommendation is fully observed</li> </ul>
<b>R.25</b>	<b>NC</b>	<ul style="list-style-type: none"> <li>• There are no formalized processes and procedures to provide adequate and appropriate feedback to financial institutions and cash dealers on STRs filed.</li> <li>• Guidelines issued are outdated</li> <li>• Feedback is not provided on a regular basis to reporting entities.</li> </ul>
<b>SR.IV</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Unable to confirm effectiveness due to recent implementation of mandatory reporting requirements.</li> </ul>

### *Internal controls and other measures*

## **3.8. Internal Controls, Compliance, Audit and Foreign Branches (R.15 & 22)**

### **3.8.1 Description and Analysis**

#### *Legal Framework:*

563. Section 2A of the revised *AML/CFT Regulations* covers requirements pertaining to ‘*Internal Policies, Procedures, Controls, and Training*’.

#### *Establish and Maintain Internal Controls to Prevent ML and TF (c. 15.1, 15.1.1 & 15.1.2):*

564. The specific requirements concerning internal policies, procedures and control; designation of a compliance officer; and access to CDD information, transaction record and other relevant information are detailed in section 2A.2 and 2A.7 respectively.

565. Based on discussions during the on-site with financial institutions and cash dealers, both banks and the global money remittance company have adequate internal policies, procedures, and controls to ensure prevention of ML and FT, and have designated compliance officers at management level. The remittance company, however, is limited in its operations staff and therefore most compliance responsibilities fall upon the comptroller.

#### *Independent Audit of Internal Controls to Prevent ML and FT (c. 15.2):*

566. Section 2A.4 imposes the obligation to maintain an internal or independent audit function to test compliance with the policies, procedures and controls mandated in section 5.

567. The banks have adequate internal audit functions, although the locally chartered institution also relies on external audits to test compliance with established policies, procedures and controls. The two banks and the cash dealer have independent audits conducted of their established internal controls.

#### *Ongoing Employee Training on AML/CFT Matters (c. 15.3):*

568. Section 2A.5 imposes the requirement to establish ongoing employee training to cover the areas stipulated under this FATF Recommendation.

569. The two banks conduct ongoing employee training on AML/CFT matters; this training also includes US OFAC and BSA training pertinent to the jurisdiction. The finance company also conducts regular training for all staff on AML/CFT requirements. The global money remittance company did not indicate that they conduct ongoing staff and management training on AML/CFT matters.

#### *Employee Screening Procedures (c. 15.4):*

570. Section 2A.6 imposes the requirement to establish screening procedures to ensure appropriate standards when hiring employees.

571. The Banking Commission does not test screening procedures during its onsite and the revised *AML/CFT Regulations* do not prescribe minimum criteria for employees at financial institutions and

cash dealers. However, banks have indicated screening is undertaken of all employees for purposes not solely related to AML/CFT.

*Additional Element—Independence of Compliance Officer (c. 15.5):*

572. Under the revised *AML/CFT Regulations*, section 2A.2, financial institutions and cash dealers must designate a compliance officer at the management level. The compliance officer and other appropriate staff should have timely access to customer identification data and customer due diligence (CDD) information, transaction records, and any other relevant information. The compliance officer should have the authority to act independently and to report to senior management above the compliance officer's next reporting level or the board of directors or equivalent body.

573. The two banks' structures allow for appropriate levels of independence of designated compliance officers. Despite the size of the operations of the finance company and money remitter, the designated manager appeared to have required levels of management authority and autonomy, as well as adhered to a set reporting structure.

574. Overall, there is compliance by the two banks with the requirements specified in section 2 of the revised *AML/CFT Regulations*. For non-bank financial institutions and cash dealers, implementation is still in progress.

## **Recommendation 22**

*Application of AML/CFT Measures to Foreign Branches & Subsidiaries (c. 22.1, 22.1.1 & 22.1.2): Requirement to Inform Home Country Supervisor (c. 22.2):*

575. Section 9 of the revised *AML/CFT Regulations* states that, "Financial institutions and cash dealers must ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with the requirements in the Marshall Islands and the FATF Recommendations." Section 9 further outlines the specific obligations that essentially restate FATF Recommendation 22, with the exception of the absence of the additional element concerning the application of CDD measures by financial institutions at the group level.

576. There are no foreign branches or subsidiaries of financial institutions or cash dealers incorporated in the RMI at the present time. However, the Banking Commission is considering an application for the locally chartered bank to establish an office in Hawaii.

*Additional Element—Consistency of CDD Measures at Group Level (c. 22.3):*

577. This additional element cannot be assessed as the financial institutions incorporated in the RMI do not have branches or subsidiaries outside of the RMI.

### **3.8.2. Recommendations and Comments**

578. The requirements of Recommendation 15 are covered fully in the *Banking Act* and revised *AML/CFT Regulations*. The deficiency is in effective implementation of this requirement by non bank financial institutions. While there is no specific recommendation under Recommendation 15, the Banking Commission should provide sector specific guidance on AML/CFT internal procedures for non-bank financial institutions (see Recommendation 25) and conduct regular examinations to assess compliance (see Recommendation 23).

**3.8.3. Compliance with Recommendations 15 & 22**

	Rating	Summary of factors underlying rating
<b>R.15</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>Some NBFIs and cash dealers have not fully implemented the requirements of the revised <i>AML/CFT Regulations</i>.</li> </ul>
<b>R.22</b>	<b>C</b>	<ul style="list-style-type: none"> <li>The Recommendation is fully observed.</li> </ul>

**3.9. Shell Banks (R.18)****3.9.1. Description and Analysis***Legal Framework:*

579. The requirements to take measures with respect to shell banks are set out in section 3N, subsections 9, 10 and 11 of the revised *AML/CFT Regulations*. These requirements are fully consistent with FATF Recommendation 18. The Banking Commission has advised that the two banks have already put in place the required measures to prevent any dealings with shell banks, and that no shell banks are permitted to be licensed in RMI.

*Prohibition of Establishment Shell Banks (c. 18.1):*

580. Section 3N.9 of the revised *AML/CFT Regulations* states that it is not permissible to establish or accept the operation of a shell bank in the Marshall Islands. Shell Bank is defined in section 1B. 18 consistent with the FATF's definition. The Banking Commission has confirmed that bank licensing policies and procedures are consistent with that provision. In addition, under section 108 of the *Banking Act*, applicants for a foreign banking licence must provide a letter from the home supervisory authority where the bank is chartered, confirming that the applicant is being supervised on a consolidated basis and that there is no objection to the establishment of a branch in the RMI.

*Prohibition of Correspondent Banking with Shell Banks (c. 18.2):*

581. Section 3N.10 of the revised *AML/CFT Regulations* requires that financial institutions and cash dealers must not enter into correspondent banking relationships with shell banks. No such facilities are provided by banks in RMI.

*Requirement to Satisfy Respondent Financial Institutions Prohibit of Use of Accounts by Shell Banks (c. 18.3):*

582. Section 3N.11 of the revised *AML/CFT Regulations* requires that financial institutions and cash dealers must satisfy themselves that respondent financial institutions and cash dealers in a foreign country do not permit their accounts to be used by shell banks. The Banking Commission has confirmed that no correspondent banking facilities are provided by banks in RMI.

**3.9.2. Recommendations and Comments**

583. No shell banks are permitted in RMI, and no dealings are conducted with shell banks. No correspondent banking facilities are provided by banks in RMI. The regulatory framework, existing AML/CFT examination procedures/scope and bank practices taken together ensure that effective measures are in place to comply with the requirements of Recommendation 18.

**3.9.3. Compliance with Recommendation 18**

	Rating	Summary of factors underlying rating
<b>R.18</b>	<b>C</b>	<ul style="list-style-type: none"> <li>The recommendation is fully observed.</li> </ul>

*Regulation, supervision, guidance, monitoring and sanctions***3.10. The Supervisory and Oversight System - Competent Authorities and SROs: Role, Functions, Duties and Powers (Including Sanctions) (R.23, 30, 29, 17, 32 & 25)****3.10.1. Description and Analysis***Authorities/SROs roles and duties & Structure and resources - R.23, 30***Recommendation 23 (Supervisory authorities)***Designated supervisory authorities and application of AML/CFT measures**Legal Framework:*

584. The *Banking Act* and revised *AML/CFT Regulations* issued in May 2010 comprise the regulatory and supervisory framework for monitoring and enforcing compliance with AML/CFT requirements in the RMI. The powers are vested in the Banking Commission as the AML/CFT supervisor. There are no other competent authorities in RMI with respect to AML/CFT supervision.

*Regulation and Supervision of Financial Institutions (c. 23.1):*

585. Adequate powers to regulate and supervise compliance by financial institutions and cash dealers with AML/CFT requirements are generally contained in sections 167 to 170A of the *Banking Act 1987*. More detailed obligations on those entities consistent with the FATF Recommendations are set out in the revised *AML/CFT Regulations*.

586. An AML Examination Procedures manual has been established to guide staff of the Banking Commission in the conduct of onsite AML examinations. However, the manual will need to be reviewed as to its scope and completeness following the passage of the revised *AML/CFT Regulations* and revised to ensure the manual covers compliance with the detailed obligations of the Regulations.

587. The only off-site AML/CFT supervisory monitoring information available to the Banking Commission appears to be AML/CFT audit reports from banks, information obtained in the course of annual re-licensing of banks, and annual reports to the Commission by each financial institution and cash dealer on their ownership and control. The Banking Commission does not appear to have access to regular (e.g. annual) information on AML/CFT compliance arrangements and effectiveness from non-bank financial institutions and cash dealers to supplement the information periodically obtained in onsite examinations.

588. Some gaps are apparent in the lack of application of the AML/CFT requirements to a number of entities that clearly meet the definition of financial institution or cash dealer under the *Banking Act*. The Banking Commission acknowledges that these gaps in the scope of the regime reflect insufficient staff resources within the office of the Commissioner and prioritization of scarce resources to deal

with currently supervised entities. Discussions are currently underway to include MIDB under AML supervision by the Banking Commission as it is a non-deposit taking lender with the majority of its US\$14 million loan portfolio being consumer lending. Two other non-deposit taking car lenders, one life insurance intermediary and at least one money remitter have yet to be engaged by the Banking Commission to ensure compliance with AML supervision and regulatory requirements.

*Designation of Competent Authority (c. 23.2):*

589. The Banking Commissioner is the sole designated competent authority under the *Banking Act* with powers set out in section 167 of the Act. The Banking Commissioner is responsible for the following AML/CFT supervisory functions: to ensure financial institutions and cash dealers adequately comply with AML/CFT requirements; and to provide for information exchange domestically and internationally. The Banking Commission conducts the onsite AML/CFT inspections of financial institutions and cash dealers and has the power to obtain additional information relevant to discovering ML, proceeds of crime or financing of terrorism.

***Structure and resources of supervisory authorities***

*Adequacy of Resources for Competent Authorities (c. 30.1):*

590. The office of the Banking Commission has three full time staff including the Banking Commissioner to carry out both prudential and AML/CFT compliance functions for all subject entities in RMI, as well as all FIU functions. The Banking Commissioner is having on-going dialogue with the MOF on adequate staffing of the Banking Commission, with the objective of increasing the staff complement by at least one technical staff by the end of 2010. The evaluation team has been advised that given the jurisdiction's lack of resources to fully implement, monitor compliance with, and enforce detailed requirements of the revised *AML/CFT Regulations*, technical assistance has been requested from PALP to assist with the development of detailed AML/CFT guidelines for industry and a revised supervision procedures and examination manual for the Banking Commission.

*Integrity of Competent Authorities (c. 30.2):*

591. The staff of the Banking Commission are subject to integrity checks prior to appointment, consistent with standards for all staff of the government of RMI. Specific legislative provisions relating to integrity of government employees are contained in the *Ethics in Government Act* Title 3, Chapter 17 of 1993 which is administered by the Government Ethic Board. This Act provides for standards of ethical conduct and conflicts of interest. The Public Service Commission which is headed by the Chief Secretary is responsible for appointment of government employees including staff of the Banking Commission. There are currently no additional codes of conduct requirements in place for the staff of the Banking Commission.

*Training for Competent Authorities (c. 30.3):*

592. The staff of the Banking Commission are competent in conducting onsite examinations for AML purposes under the previous regulatory requirements using the current examination manual. There may be risk of losing those examination skills if staff changes occur or there are not sufficiently regular onsite examinations conducted to keep the expertise current. Further on the job training is required for staff of the Banking Commission to operationalize on-site examination and compliance monitoring against the detailed requirements of the new *AML/CFT Regulations*. Technical assistance has been requested from PALP for early 2011 to assist in such training.

## ***Authorities Powers and Sanctions – R.29 & 17***

### **Recommendation 29 (Supervisory powers)**

#### *Power for Supervisors to Monitor AML/CFT Requirement (c. 29.1):*

593. Broad powers are provided to the Banking Commission to ensure compliance with the AML/CFT requirements of Part XIII of the *Banking Act* and the revised *AML/CFT Regulations*, under section 167 of the Act. The Regulations form an integral part of the obligations on subject entities. In addition, the Banking Commission has more specific powers with respect to monitoring and ensuring compliance by licensed banks under Parts II to XII of the Act.

#### *Authority to conduct AML/CFT Inspections by Supervisors (c. 29.2):*

594. Section 167(1) (c) of the *Banking Act* provides for the Banking Commission to enter the premises of any financial institution or cash dealer to inspect records and ask questions and take copies of any records. Specific powers are provided for the Banking Commission to conduct examinations of licensed banks and their affiliates to determine that the requirements of the law have been complied with, in section 138 of the *Banking Act*. From time to time, the Banking Commission conducts AML/CFT examinations of both banks and non-banks that are subject to the AML/CFT requirements.

595. Onsite examinations were carried out for AML/CFT purposes on five entities in the period from 2004 to 2007, after which there was a significant gap until the most recent examination of one bank in August 2010. Some entities including two of the three insurance intermediaries, and a recently commenced money transfer business have not yet been examined onsite. None of the examinations were based on the detailed requirements of the revised *AML/CFT Regulations*.

#### *Power for Supervisors to Compel Production of Records (c. 29.3 & 29.3.1):*

596. Adequate powers are provided to obtain information for AML/CFT purposes and are not predicated by the need to obtain a court order. Section 167(1)(i) provides for the Banking Commission to request additional information from financial institutions and cash dealers where the Banking Commission has reasonable grounds to believe that the information is essential to discovering ML activity. Section 138(2) of the Act additionally provides for information to be made available for inspection by the Banking Commission, by a licensed bank which is the subject of an examination.

597. The Commission also has power under section 167 (1) (l) of the *Banking Act* to apply for a warrant to enter and search the premises of any financial institution or cash dealer, or of any officer or employee thereof, and remove any documents, materials or other things for the purposes of preventing ML, in addition to the powers in section 167(1)(c) and (i).

598. There is no regular collection of, or offsite monitoring of AML/CFT compliance information from financial institutions and cash dealers, except audit reports, although the Banking Commission has powers to do so.

#### *Powers of Enforcement & Sanction (c. 29.4):*

599. The principal powers for enforcement and sanction for non-compliance with AML/CFT requirements under the *Banking Act* and revised Regulations are contained in section 181 of the Act and are further detailed in section 7 of the Regulations.

600. For licensed banks, with the approval of the Cabinet the Banking Commission has additional powers to suspend, revoke or vary a bank's licence under section 113 of the *Banking Act*, for failure to comply with terms and conditions of its licence or violation of any provisions of the Act or regulations, or knowingly providing untrue or misleading information to the BC. Additional grounds are provided in section 113 (1) (m), where the Banking Commission is satisfied that there are reasonable grounds to believe that ML activity is taking place. Section 114 provides for additional powers to direct a licensed bank to prohibit transactions or requiring it to take certain steps or pursue a particular course of action where a notice of suspension has been issued under section 113. Section 142 of the Act provides for the Banking Commission to issue a cease and desist order to a licensed bank for failure to comply with any provisions of the Act or any terms or conditions of its licence.

### **Recommendation 17 (Sanctions)**

#### *Availability of Effective, Proportionate & Dissuasive Sanctions (c. 17.1):*

601. Section 181 (1) of the *Banking Act* provides that in addition to any criminal penalties or fines authorized by Part XIII of the Act, civil money penalties of up to US\$10,000 per violation can be imposed, in enforcement proceedings through the High Court, against a financial institution or cash dealer, and any partner, officer, employee or person conducting the affairs of the business. The civil money penalties apply to breaches of both Part XIII of the *Banking Act* and the revised *AML/CFT Regulations*, and are also specifically provided for in section 7 of the Regulations. The resignation, termination of employment or participation in the affairs of any partner, director, officer, employee, or person participating in the conduct of the affairs of a financial institution or cash dealer shall not affect the jurisdiction of the high court to issue judgment against such person or entity within six years of their resignation, termination of employment or termination of participation in the affairs of the financial institution or cash dealer.

602. Separate sanctions for wilfully violating the record keeping and suspicious transactions reporting requirements of sections 169 and 170 are set out in section 169 (5) of the Act, for which offences are punishable by a fine of not more than US\$2 million or imprisonment for not more than 20 years, or both. Improper disclosure of an STR report or related information by any person, financial institution or cash dealer, is subject to the same sanctions under section 170 (4).

603. The Banking Commission has advised that since the commencement of AML/CFT requirements under the *Banking Act*, no sanctions have yet been exercised over any financial institution or cash dealer. Breaches of requirements that have been identified in the course of AML/CFT supervision, analysis of STR reporting and onsite examinations have been advised in writing to the subject entity, and are rectified on request. As a general rule, the Banking Commission will conduct an onsite follow-up review to verify that rectification is completed.

#### *Designation of Authority to Impose Sanctions (c. 17.2):*

604. The responsibility for applying sanctions for non-compliance with AML/CFT obligations against financial institutions and cash dealers resides with the Banking Commission in accordance with the *Banking Act* and revised *AML/CFT Regulations*. Section 181(2) states that the Banking Commissioner shall refer all violations under subsection (1) above to the Office of the Attorney General for enforcement proceedings in the High Court of the Republic of the Marshall Islands.

*Ability to Sanction Directors & Senior Management of Financial Institutions (c. 17.3):*

605. The provisions for civil money penalties and sanctions for breaches of sections 169 and 170 of the Act are applicable to employees, officers and directors of financial institutions and cash dealers, as well as to the entity itself.

*Range of Sanctions—Scope and Proportionality (c. 17.4):*

606. There are no routinely available sanctions such as administrative fines or compliance orders for breaches of AM/CFT requirements. The range of sanctions for non-compliance with the detailed requirements of the revised *AML/CFT Regulations* or failure to comply with the Banking Commission's powers under section 167 of the Act by non-bank financial institutions and cash dealers is limited to civil money penalties. There is no scope to apply administrative sanctions over non-bank entities. Only in the case of record keeping or STR reporting breaches of sections 169 and 170 are there heavier sanctions available for all subject entities.

607. For licensed banks, the Banking Commission can impose a wider range of administrative sanctions including suspending, revoking or varying a bank's licence under section 113 of the *Banking Act*, for failure to comply with terms and conditions of its licence or violation of any provisions of the Act or regulations. Section 114 provides for additional powers to direct a licensed bank, to prohibit transactions or to require it to take certain steps or pursue a particular course of action where a notice of suspension of licence has been issued under section 113. Section 142 of the Act provides for the Banking Commission to issue a cease and desist order to a licensed bank where it has contravened or failed to comply with any provisions of the Act or any terms or conditions of its licence.

608. It appears that these direction, and cease and desist powers in relation to licensed banks could *in extremis* be used by the Banking Commission to require the replacement, or a restriction on the powers, of individual managers or directors for violation of the Act or regulations.

609. There appears to be a material difference in the severity of sanctions between the maximum civil money penalties of US\$10,000 for most AML/CFT compliance offences, and sanctions for breaches of sections 169 and 170, for which offences are punishable by a fine of not more than US\$2 million or imprisonment for not more than 20 years, or both. Review of the scope of sanctions and quantum of penalties would seem appropriate to provide the Banking Commission with a more graduated, but ultimately dissuasive range of actions and sanctions in the future, particularly with respect to non-bank financial institutions and cash dealers where the range of options is currently rather narrow.

**Market entry – Recommendation 23***Fit and Proper Criteria and Prevention of Criminals from Controlling Institutions (c. 23.3 & 23.3.1):*

610. Fit and proper criteria are applied to bank directors, senior managers and owners of more than 10% of the issued stock of banks at the time of application for a licence under section 108 of the *Banking Act*. Banking licences are required to be renewed annually and updated fit and proper information is obtained as part of the consideration of licence renewal. Section 139 sets out criteria for disqualification of directors of domestic banks, including being a member of the Nitijela, being a bankrupt, or having been convicted of any offence involving dishonesty or fraud. Section 140 provides that any change in directors or principal officers of a domestic bank requires the prior

approval of the Banking Commission upon written application. Section 141 sets out criteria for disqualification for employment as a manager or other official of a licensed bank. Under section 1 of the previous AML Regulations and revised *AML/CFT Regulations*, all financial institutions and cash dealers are required to maintain records and make annual reports to the Banking Commission of the identity of any controlling owners during the year (whether acting alone or collectively) and to ascertain whether any institution affiliated party who has been convicted of any offence involving dishonesty, breach of trust, or ML.

611. There are not any explicit provisions prohibiting criminals or their associates from holding or being beneficial owners of a controlling interest in, or being a senior manager or director of a non-bank financial institution or cash dealer. The Banking Commission has no powers to remove a person from such a position. Likewise there are no fit and proper procedures or powers provided to the Banking Commission in respect of non-bank financial institutions and cash dealers.

*Licensing or Registration of Value Transfer/Exchange Services (c. 23.5):*

612. The CTA, in section 120 (1) on “Measures to suppress financing of terrorism”, requires “*any person, that provides a service for the transmission of money or value, including transmission through an alternative remittance system or informal money or value transfer system or network, or the agent of such person, shall be required to be licensed by the competent authorities of the Marshall Islands, and shall be subject to the disclosure requirements prescribed by the relevant authorities in relation to that type of business.*” However, the RMI authorities have not yet operationalized this provision by establishing a formal licensing authority or process for MVTs. Informal MVT providers are discussed under SRVI.

613. There are no requirements for licensing or registration of money exchange services. The authorities advise that there are no businesses other than banks providing money exchange facilities at present.

614. One MVT business has been subject to AML compliance monitoring by the Banking Commission and on-site inspection for compliance with the AML Regulations 2002. Another MVT business has recently commenced operations and has been apprised of its compliance obligations. The authorities are not currently able to determine whether there are other providers of MVT or money exchange business which should be subject to AML requirements, and acknowledge that there are possibly one or more other businesses that should be subject to the requirements. The RMI authorities have advised that a TA request has been submitted for assistance in the establishment of a central registry for MVTs and MSBs.

*Licensing and AML/CFT Supervision of other Financial Institutions (c. 23.7):*

615. There are no licensing or registration requirements for other non-bank financial institutions and cash dealers. The absence of mandatory licensing or registration creates some uncertainty about which entities should be subject to AML/CFT requirements under the *Banking Act* and regulations.

616. There are currently one non-deposit taking lender and two insurance intermediaries (not underwriters) that are properly captured within the AML supervisory net (although other entities appear to be meeting the definitions in the Act). AML supervision is primarily effected through on-site examinations, with the non-deposit taking lender and one insurance intermediary examined in 2006. The arrangements in place in those entities appeared to be adequate to comply with the previous AML regulatory requirements, given the relatively low-risk nature of their business. However, these entities will need to review and update their AML/CFT policies and procedures to

ensure they are consistent with the new regulatory requirements and the Banking Commission will then need to assess the adequacy of those arrangements.

### ***Ongoing supervision and monitoring – Recommendation 23***

#### *Application of Prudential Regulations to AML/CFT (c. 23.4):*

617. The AML/CFT framework for banks in RMI is integrated with the prudential supervision requirements as part of the *Banking Act*. Bank licensing includes fit and proper requirements which are subject to annual review at re-licensing, and bank supervision compliance and sanctions powers are applicable to all violations of the *Banking Act* and the regulations made thereunder, including for AML/CFT obligations.

618. Under section 134 (11) of the *Banking Act*, in February 2005, the Banking Commission used prudential powers for AML/CFT purposes via Advisory Notice (A-05) to advise of the proposed requirements for all banks and financial institutions operating in RMI to undergo an annual audit of their AML/CFT compliance program and internal controls, to be performed by a duly authorized external auditor. The Directive took effect immediately, after a two week consultation period, for banks. Other financial institutions were to be advised later as to the date in which the proposed directive would apply to them. The attachments set out a questionnaire to be completed annually about AML/CFT compliance arrangements and a checklist for auditors on AML/CFT compliance.

619. The Banking Commission has advised that banks are providing the Commission with copies of AML/CFT audits. However, the status of the advisory A-05 and associated requirements is unclear in respect of non-bank financial institutions and cash dealers, as the advisory appears to be based on section 134 of the *Banking Act* which only applies to licensed banks.

620. There are no prudential (non-AML/CFT) supervision or compliance obligations imposed on insurance intermediaries in RMI. The business of insurance intermediaries is not required to be subject to the prudential elements of the IAIS core principles. Prudential requirements and related AML/CFT obligations for insurers underwriting business for customers in RMI will be applied in their home jurisdiction.

621. As there are currently no foreign branches or subsidiaries of RMI financial institutions, the application of consolidated supervision for prudential and AML/CFT purposes has not yet arisen. The Banking Commission is considering an application for the locally chartered bank to establish an office in Hawaii to assist in direct clearing of U.S. dollar transactions and access to US Federal Funds market and the Banking Commission will need to consider whether any additional legislative and supervisory arrangements will be required to monitor and supervise the risks arising from such business on a consolidated basis.

#### *Monitoring and Supervision of Value Transfer/Exchange Services (c. 23.6):*

622. Onsite examinations appear to be the primary AML monitoring and supervision tool applied to money value transfer and exchange service providers. Only one MVT business was in existence until 2009, and it was last examined by the Banking Commissioner's office in 2006. More proactive and regular AML compliance engagement and information collection would assist in monitoring and supervising to ensure compliance with the new regulatory requirements and address the increasing risks in this sector as new participants are added to the supervisory net.

### ***Guidelines – R.25.1 (Guidance for financial institutions other than on STRs)***

623. The Banking Commission has up to August 2004, issued a range of guidelines to assist financial institutions and cash dealers in understanding their AML/CFT obligations, including:

- i. Guidelines on suspicious transactions, and Preparation Guidelines for Suspicious Activity Report Form;
- ii. Instructions and reporting form for Currency Transaction Report.

624. The Banking Commission has not yet issued detailed guidelines to assist financial institutions and cash dealers to effectively comply with the new requirements and risk based approach to CDD established under the revised *AML/CFT Regulations*. Greater guidance would significantly assist newly identified institutions to understand their compliance requirements. All existing guidance instruments (guidelines and advisory notices) are now out of date and will need to be revised to be consistent with the detailed new regulatory requirements.

### *Statistics and effectiveness (R.32)*

625. The Banking Commission has advised that the Commission undertook onsite AML/CFT compliance examinations in the last 5 years as follows:

**Table: AML/CFT supervisory On-site Examinations**

Year	Coverage
2006	4 (1 bank, 1 insurance intermediary, 1 money remitter, and 1 non-deposit taking lender)
2007	1 (bank)
2008	0
2009	0
2010 (to November 2010)	1 (bank)

### **3.10.2. Recommendations and Comments**

626. **Recommendation 29:** Adequate powers are available to the Banking Commission to monitor compliance, conduct onsite examinations and obtain necessary information to carry out AML/CFT supervision. The effectiveness of these powers is compromised by the absence of regular collection and monitoring of offsite AML/CFT compliance information and the lack of recent onsite examinations.

627. **Recommendation 17:** The Banking Commission has a reasonable range of proportionate and dissuasive sanctions available to be exercised over banks but no AML/CFT compliance sanctions have been imposed to date, on the basis that compliance deficiencies have been rectified once identified in on-site examinations. With respect to non-bank entities subject to AML/CFT requirements, the primary sanction available is civil money penalties, with no options available for other proportionate administrative sanctions such as administrative fines or compliance orders.

628. The RMI authorities should establish a wider range of sanctions, particularly for the non-bank entities, and consider increasing the maximum level of civil money penalties, having regard for relativity with the maximum penalties provided for similar offences and the breaches of sections 169 and 170, which are set out in s.169 (5) of the Act.

629. The Banking Commission should, after identifying AML/CFT compliance breaches, set out in writing to the offending institution reasonable but firm deadlines for rectification of compliance

breaches, and obtain written responses for the entities detailing actions taken, rather than possibly delaying follow-up of rectification until subsequent onsite examinations.

630. Non-compliance with required corrective action should then be followed up by formal sanctions as provided for under the *Banking Act* and Regulations.

631. **Recommendation 23:** The RMI authorities should provide in legislation for powers to prevent criminals or their associates from holding or being beneficial owners of a controlling interest in or being a senior manager or director of a non-bank financial institution or cash dealer.

632. The RMI should consider introducing fit and proper person requirements for all such persons.

633. The RMI authorities have advised that there is no intention to licence offshore banks under the *Banking Act*. The legislative framework provides in the Act for offshore banking but these powers are inadequate to meet international best practices for offshore bank licensing and supervision. To reduce the risk of negative international sentiment being focused on the potential for offshore banking in RMI to be used for ML and FT, the authorities should consider removing all references to offshore banks from the *Banking Act*. If there is sound justification to permit offshore banking at some future time, the authorities should then establish a robust separate offshore banking legislative framework consistent with international standards.

634. The Banking Commission should as soon as possible carry out targeted onsite compliance monitoring regarding the effectiveness of arrangements established by subject entities to implement the new detailed obligations set out in the revised *AML/CFT Regulations*.

635. The Banking Commission should consider implementing regular collection and off-site monitoring of AML/CFT compliance information, for example through annual reports by each subject entity, and requiring copies of annual internal or external audit reports on AML/CFT compliance and procedures from non-banks. These reports should supplement the compliance information derived from onsite examinations to monitor effectiveness of arrangements for compliance with new requirements. The status of the 2005 advisory A-05 on AML/CFT external audit requirements is unclear in respect of non-bank financial institutions and cash dealers. Any uncertainty regarding the Banking Commissioner's powers to obtain such compliance information and audit reports from non-bank entities should be removed by amendment to the *Banking Act* and regulations as necessary.

636. The Banking Commissioner has appropriate regulatory powers to issue formal notices which are enforceable pursuant to the *Banking Act* and Regulations. The Banking Commissioner should ensure the form, wording and timing of such notices are specific as to the powers being exercised. In the absence of correct legal form, such notices issued by the Banking Commissioner could be subject to challenge. For example, Advisory A-05 on AML audit requirements should be updated to confirm its application to banks only, under section 134(11) of the *Banking Act*; and Advisory A-10(c) which provides a temporary grace period (exemption) for all financial institutions and cash dealers from compliance with the new obligations of the revised *AML/CFT Regulations* until 22 October 2010 should specifically refer to being issued under the relevant exemption and exception powers (contained in section 8 of the Regulations).

637. The RMI authorities should consider establishing through legislation a register of financial service providers to ensure the Banking Commission has sufficient information to identify all parties that fall within the definition of financial institutions and cash dealers in RMI. At a minimum, all MVT and money exchange business should be subject to a mandatory registration requirement as

provided for in section 121(1) of the CTA. The registration framework should provide effective penalties for any entities carrying on such business that are not registered, and provide grounds for deregistration including for willful failure to comply with AML requirements or upon conviction for certain offences including crimes relating to fraud, dishonesty or ML and FT.

638. The Banking Commission should also consider establishing working arrangements with the Registrar of Corporations and the local atoll governments that issue business licences to assist the Banking Commission to identify all businesses in RMI that are chartered or licensed as businesses to provide any type of financial service that would be subject to the *Banking Act* and Regulations.

639. The Banking Commission should correct identified inadequacies in scope of entities covered and immediately exercise the powers to monitor compliance with and enforce AML/CFT requirements under the *Banking Act* for certain non-deposit taking lenders (including MIDB), remittance dealers and life insurance intermediaries that are not currently supervised for AML/CFT purposes.

640. The Banking Commission should consider whether additional legislative and supervisory arrangements will be required to effectively monitor and supervise on a consolidated basis the risks arising from the establishment of any foreign subsidiaries, branches or offices of RMI financial institutions.

641. The Banking Commission should immediately revise the AML examination procedures manual and all offsite supervision procedures and instructions for staff to incorporate the risk based approach to CDD and the broader range of compliance requirements set out in the revised *AML/CFT Regulations* and recent amendment to the *Banking Act*. The Banking Commissioner should also review banks' conditions of licence in respect of AML/CFT matters to ensure the obligations are comprehensive and consistent with the revised *AML/CFT Regulations*.

642. The RMI authorities should immediately pass the amendments to the *Banking Act* sections 166 and 167 as per the draft presented to the evaluation team (see also related recommendation under R.26).

643. The RMI authorities should prepare a national AML/CFT risk assessment using the APG national risk assessment framework or some other tool to identify the level and nature of AML/CFT risks and associated criminality in RMI, develop future risk indicators and contribute to the development of a comprehensive national strategy to effectively combat ML and FT.

644. **Recommendation 25:** The Banking Commission should issue detailed guidelines to assist financial institutions and cash dealers to effectively comply with the new requirements and risk based approach to CDD established under the revised *AML/CFT Regulations*. That should include criteria to be adopted in considering applications for the various approvals and exemption powers that the Banking Commissioner can exercise under the Regulations. Technical assistance from regional agencies may be appropriate to implement these recommendations as soon as possible.

645. **Recommendation 30: Integrity:** The Banking Commission should consider establishing a code of conduct for staff of the Banking Commission and FIU consistent with international best practice to enhance transparency regarding the expectations on staff regarding honesty, integrity and professionalism.

646. **Recommendation 30: Resources:** At least one additional technical staff position should be established as soon as possible in the Banking Commission to provide sufficient resources to

effectively conduct on and offsite AML supervision for all cash dealers and financial institutions and ensure compliance with the more detailed requirements of revised *AML/CFT Regulations*. The Banking Commissioner should draw up a work program to schedule AML/CFT onsite compliance examinations, and ensure all entities are examined at least once every four (4) years with more frequent examinations scheduled according to the risk the entity poses, particularly for banks. At least two (2) onsite AML/CFT examinations should be carried out every year to maintain supervisors' skills and experience and spread the workload evenly.

### 3.10.3. Compliance with Recommendations 17, 23, 25 & 29

	Rating	Summary of factors underlying rating
<b>R.17</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>Penalties for compliance breaches by non-bank financial institutions and cash dealers are not sufficiently proportionate or dissuasive.</li> <li>No effective use of formal sanctions powers by Banking Commission to date.</li> </ul>
<b>R.23</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>A number of entities operating as a non-deposit taking lender, money remittance service provider, or insurance intermediary appear to be covered by the AML/CFT legislative requirements but are not currently supervised for AML/CFT purposes.</li> <li>Effectiveness is undermined by the lack of onsite AML examinations since 2007, and inadequate information to carry out regular offsite AML compliance monitoring, particularly for non-bank financial institutions and cash dealers.</li> <li>The Banking Commission has not yet conducted monitoring or site examinations with respect to compliance with the recently introduced requirements of the revised <i>AML/CFT Regulations</i>.</li> <li>No legislation exists to prevent criminals or their associates from holding or being beneficial owners of a controlling interest in, or being a senior manager or director of a non-bank financial institution or cash dealer.</li> <li>No registration or licensing requirement is in place for money or value transfer service providers, or other non-bank financial institutions and cash dealers.</li> </ul>
<b>R.25</b>	<b>NC</b>	<ul style="list-style-type: none"> <li>Lack of comprehensive guidance to assist subject entities to comply with new AML/CFT regulatory requirements.</li> <li>Previously issued guidance material has not been updated to ensure it is consistent with the revised <i>AML/CFT Regulations</i>.</li> </ul>
<b>R.29</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>Lack of effectiveness of powers due to inadequate human resources in the Banking Commission.</li> </ul>

### 3.11. Money or Value Transfer Services (SR.VI)

#### 3.11.1. Description and Analysis

##### *Legal Framework:*

647. The *Banking Act* definition of financial institution includes, in section 102(n)(iv), any person who carries on a business of “money transmission services”. All providers are designated as financial institutions and subject to AML/CFT requirements. There is no separate category of money or value transfer services providers in the *Banking Act* or other laws.

648. The CTA, in section 120 (1) on “Measures to suppress financing of terrorism”, requires “any person, that provides a service for the transmission of money or value, including transmission through an alternative remittance system or informal money or value transfer system or network, or the agent of such person, shall be required to be licensed by the competent authorities of the Marshall Islands, and shall be subject to the disclosure requirements prescribed by the relevant authorities in relation to that type of business.” However, the RMI authorities have not yet implemented a licensing process under this provision.

649. The implementation of AML/CFT obligations in the formal regulated sector, which includes the banking sector and two international remittance providers are covered in the preceding sections. By way of background, one international remittance provider operates out of a bank and is licensed as part of its banking operations. The other is a stand-alone financial institution that is regulated by the Banking Commission.

650. The focus of this section is on the informal money/value transfer (MVT) operators or alternative remittance system operating in the RMI. The RMI has one or two informal providers not under the regulatory net. They are licensed by local government as businesses but not supervised for AML/CFT purposes by the Banking Commission as financial institutions.

651. According to financial institutions met during the on-site, the outflow of funds from RMI residents exceeds the inflow of funds from the small RMI diaspora based in the US. The explanation provided was that the Marshallese community based in the U.S was not as financially sound as Marshallese based in the RMI.

*Designation of Registration or Licensing Authority (c. VI.1):*

652. All MVT service providers, whether part of the formal or informal system are required to be licensed by a competent authority under section 120 (1) of the CTA. However, this requirement has not been implemented.

653. The Banking Commission indicated that it is in the process of identifying all informal providers and including them in a Registrar of providers. This approach seems to differ from the requirement of licensing, although the plan is to include these informal providers under the Banking Commission’s AML/CFT supervision program.

*Application of FATF Recommendations (c. VI.2): (applying R.4-11, 13-15 & 21-23, & SRI-IX)  
Monitoring of Value Transfer Service Operators (c. VI.3):*

654. There is neither application of FATF Recommendations nor any monitoring of informal MVT operators at this stage.

*List of Agents (c. VI.4):*

655. There is a requirement under the CTA Act, as mentioned, to maintain a list of agents. This is currently done for one international remittance provider, as it has two agents in the RMI. No other formal provider has agents in the RMI. There is no available information of informal service providers but given the size of the market, it is unlikely.

*Sanctions (applying c. 17.1-17.4 in R.17)(c. VI.5):*

656. The Banking Commission has the same sanction powers outlined under Recommendation 17. There are no plans to sanction the informal providers identified to date, only to include them under the supervisory umbrella.

*Additional Element—Applying Best Practices Paper for SR VI (c. VI.6):*

657. The RMI has indicated it is in the process of introducing a Registrar for MVT providers.

### 3.11.2. Recommendations and Comments

658. The informal MVT sector is relatively negligible. The formal MVT operators, namely the two banks and the international remittance providers are subject to existing AML/CFT obligations. In order to include the informal MVT providers under the supervisory framework, the RMI should:

- Implement the Register for MVT service providers.
- Identify informal MVT providers and subject them to existing AML/CFT obligations.

### 3.11.3. Compliance with Special Recommendation VI

	Rating	Summary of factors underlying rating
<b>SR.VI</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Lack of effective implementation of the CTA licensing requirements for MVT.</li> <li>• Informal MVT providers are not covered under existing AML/CFT obligations.</li> </ul>

#### 4. PREVENTIVE MEASURES—DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

##### 4.1. Customer Due Diligence and Record-keeping (R.12)

###### 4.1.1 Description and Analysis

*CDD Measures for DNFBPs in Set Circumstances (Applying c. 5.1-5.18 in R. 5 to DNFBP) (c. 12.1): (Applying Criteria under R. 6 & 8-11 to DNFBP) (c.12.2):*

659. The AML/CFT regulatory requirements in RMI are set out in the *Banking Act* and revised *AML/CFT Regulations* and apply to financial institutions and cash dealers, which includes the operator of any gambling house, casino or lottery, and a person who carries on a business dealing in bullion. No other categories of DNFBP are covered by these requirements.

660. No casinos, gambling businesses or lotteries are permitted in RMI, under the provision of the *Gambling and Recreation Prohibition Act 1998*, which states that no person, natural or corporate, shall engage in any form of gaming or gambling activities within the Republic, and no person, natural or corporate, shall possess, use, sell, or purchase, directly or indirectly, any gambling or gaming machines, appliances or devices used in the conduct of, or to promote gaming or gambling activities within the Republic. Exception is provided for activities by non-profit organizations that receive a permit from the local government for the gaming activities of bingo, raffles and cakewalks for the purpose of raising funds, and are solely in furtherance of the stated purposes of the non-profit organizations

661. Legal attorneys, accountants and TCSPs in RMI are not subject to AML/CFT requirements as required under Recommendation 12. There do not appear to be any real estate agents operating in RMI, and there are no AML/CFT requirements that would apply to that business when they are involved in transactions for a client concerning the buying and selling of real estate.

###### 4.1.2 Recommendations and Comments

662. The risks of AML/CFT through such businesses have been well established through international studies. While this sector remains unregulated it poses a potential AML/CFT risk for RMI.

663. The authorities should introduce legislative obligations on DNFBP to comply with the requirements of Recommendation 12 but implementation should be risk based.

###### 4.1.3. Compliance with Recommendation 12

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
<b>R.12</b>	<b>NC</b>	<ul style="list-style-type: none"> <li>No AML/CFT requirements are in place for lawyers and accountants who conduct financial transactions on behalf of customers, or TCSPs.</li> </ul>

##### 4.2. Monitoring Transactions and other Issues (R.16)

*(Applying R.13 to 15 & 21)*

###### 4.2.1 Description and Analysis

664. The STR reporting obligations in the *Banking Act* and revised *AML/CFT Regulations* only covers financial institutions and cash dealers, although as indicated previously, a cash dealer is defined to include “an operator of a gambling house, casino or lottery” and “a person who carries on a business dealing in bullion”. Therefore at present, there are no STR reporting obligations for DNFBP.

#### 4.2.2 Recommendations and Comments

665. The authorities should introduce legislative obligations on DNFBP to comply with the requirements of Recommendation 16 but implementation should be risk based.

#### 4.2.3 Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
<b>R.16</b>	NC	<ul style="list-style-type: none"> <li>No STR reporting obligations for DNFBP.</li> </ul>

### 4.3. Regulation, Supervision, and Monitoring (R.24-25)

#### 4.3.1. Description and Analysis

##### Recommendation 24 (Supervision of DNFBPs)

*Regulation and Supervision of Casinos (c. 24.1, 24.1.1, 24.1.2 & 24.1.3):*

666. Casinos are prohibited from operating in the RMI as explained previously.

*Monitoring Systems for Other DNFBPs (c. 24.2 & 24.2.1):*

667. The main DNFBP sector is the offshore company formation services sector. These are accountants, lawyers and other company service providers based in foreign jurisdictions providing services for the RMI’s offshore company registry. However, there is no direct supervision of such company formation service providers.

668. The Trust Company of the Marshall Islands, Inc. (TCMI) is the off-shore company Registrar. However, it does not deal directly with company formation service providers, as the actual registration services is provided by International Registries, Inc. (IRI) which is an affiliate company headquartered in Virginia (USA) with several affiliates and offices round the globe. The IRI performs some due diligence prior to accrediting company formation service providers as “qualified intermediaries”, including screening their names through commercially available databases and verifying that they are a licensed attorney, banker, accountant, or corporate formation specialist. There is no ongoing annual requirement to maintain the accredited status, although on each occasion a qualified intermediary submits an application of incorporation on behalf of a client, the details of the qualified intermediary are checked again through the data base used by IRI.

669. There is no monitoring system in place for other DNFBPs.

##### Recommendation 25 (Guidance for the DNFBP sectors)

*Guidelines for DNFBPs (applying c. 25.1):*

670. There has been no AML/CFT guidance provided to DNFBP.

#### **4.3.2. Recommendations and Comments**

671. The RMI should introduce an appropriate legal and supervisory framework for DNFBP with a prioritised and phased implementation based on a risk assessment, with a focus on enhancing supervision of company formation service providers based offshore, to monitor compliance with CDD, STR reporting and other AML/CFT measures recommended under R.12 and R.16.

#### **4.3.3. Compliance with Recommendations 24 & 25 (criteria 25.1, DNFBP)**

	<b>Rating</b>	<b>Summary of factors relevant to s.4.3 underlying overall rating</b>
<b>R.24</b>	NC	<ul style="list-style-type: none"> <li>There is no supervision and regulation of DNFBP.</li> </ul>
<b>R.25</b>	NC	<ul style="list-style-type: none"> <li>No guidance provided on AML/CFT for DNFBP.</li> </ul>

#### **4.4. Other Non-Financial Businesses and Professions—Modern-Secure Transaction Techniques (R.20)**

##### **4.4.1. Description and Analysis**

*Other Vulnerable DNFBPs (applying R. 5, 6, 8-11, 13-15, 17 & 21 c. 20.1):*

672. The *Banking Act*'s definition of financial institution includes “an operator of a gambling house, casino or lottery”. This is in excess of the requirement of the FATF to include casinos only, and include one of the examples listed by the FATF of other DNFBP i.e. gambling. However, as noted earlier, gambling is illegal in the RMI since the promulgation of the *Gambling and Recreation Prohibition Act 1998*.

673. There are no high value or luxury goods sold in the RMI. Most are purchased offshore and imported. The exemption is the trade in second hand marine or motor vehicles which considering the size and scope of the RMI's economy and the general socio economic conditions, could be considered luxury goods.

*Modernization of Conduct of Financial Transactions (c. 20.2):*

674. The RMI is essentially a cash based economy for retail transactions. Only one bank offers credit card services and there are only two ATMs in the RMI. The Banking Commission has not taken any measures to encourage the use of more modern and secure techniques for conducting financial transactions. However, given the population size it may not be profitable for financial institutions to introduce new products into the market.

675. Based on RMI statistics, there are on average 2,365 CTRs per annum from 2007-2009, which indicate that cash is used to purchase relatively high value products.

##### **4.4.2 Recommendations and Comments**

676. The RMI should encourage the introduction of modern and secure techniques for conducting transactions.

#### **4.4.3. Compliance with Recommendation 20**

	<b>Rating</b>	<b>Summary of factors underlying rating</b>
<b>R.20</b>	<b>PC</b>	<ul style="list-style-type: none"><li>• No measures have been taken to encourage the use of modern and secure techniques for conducting financial transactions.</li></ul>

## 5. LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANIZATIONS

### 5.1 Legal Persons – Access to beneficial ownership and control information (R. 33)

#### 5.1.1. Description and Analysis

##### *Legal Framework:*

677. Laws providing for the formation of legal persons in the RMI include the *Business Corporations Act (BCA)*, *Revised Partnership Act*, *Limited Partnership Act*, and *Limited Liability Company Act*. These statutes are collectively known as the *Associations Law*, and provide the legal framework for the establishment and operation of domestic and non-resident domestic corporations, partnerships, limited partnerships, limited liability companies, foreign maritime entities, and foreign corporations authorized to do business in the RMI.

678. Under the *Foreign Investment Business License (FIBL) Act*, the Minister of Finance is the designated Registrar of Foreign Investments (section 503A, FIBL).

679. At the time of the on-site, there were about 622 businesses, incorporated and unincorporated, registered with the resident domestic Registrar, including 84 companies with a FIBL licence. For the Registrar of non-resident domestic entities, TCMI, there are reported to be about 30,000 active entities, with additional 5,000-6,000 new registrations each year. About 70% of entity registrations are in the maritime sector and linked to the RMI ship registry.

##### *Measures to Prevent Unlawful Use of Legal Persons (c. 33.1):*

##### Corporations

680. Section 2(c)–(d) of the BCA defines a “corporation” or “domestic corporation” as “a corporation for profit formed under this Act, or existing on its effective date and theretofore formed under any other general statute or by any special act of the Republic or which has transferred to the Republic pursuant to Division 14 of this Act”. A “foreign corporation” means “a corporation for profit formed under laws of a foreign jurisdiction. “Authorized” when used with respect to a foreign corporation means having authority under Division 12 of this Act to do business in the Republic”.

681. Sections 2 (i)-(j) in the BCA, further differentiate and define resident corporations as “Doing Business in the RMI” and non-resident as “Not Doing Business in the RMI”. These covered both corporations and other legal entities.

682. The BCA Act is applicable to both resident and non-resident corporations. Overall, the provisions are essentially the same with some variations for certain provisions for non-residents e.g. non-resident corporations are not permitted to provide banking, insurance or trust services.

683. Incorporators, as defined in section 25 of the BCA, can be “any person, partnership, association or corporation, singly or jointly with others, and without regard to his or their residence, domicile, or jurisdiction of incorporation, may incorporate or organize a corporation under this Act.”

684. For directors, Section 49 of the BCA specifies that “...directors need not be residents of the RMI or shareholders of the corporation...Non-resident corporations may appoint or elect directors which are corporations.”

685. All resident domestic and non-resident corporations are required to file their articles of incorporation for registration purposes (section 28, BCA). The more significant contents of which are summarized as follows:

- (a) the name of the corporation;*
- (b) the duration of the corporation if other than perpetual;*
- (c) the purpose or purposes for which the corporation is organized.*
- (d) the registered address of the corporation in the Republic and the name and address of its registered agent;*
- (e) the aggregate number of shares which the corporation shall have authority to issue;*

*x x x*

- (h) if bearer shares are authorized to be issued as provided in section 42 of this Act, the manner in which any required notice shall be given to shareholders of bearer shares;*

*x x x*

- (j) if the initial directors are to be named in the articles of incorporation, the names and addresses of the persons who are to serve as directors until the first annual meeting of the shareholders or until their successors shall be elected and qualified;*
- (k) the name and address of each incorporator:*

686. The registration requirements for non-resident and resident corporations are the same. The BCA (or other Acts under the *Association Law*) does not require the filing of the names of any director, officer, shareholder or beneficial owner. This is done only on a voluntary basis. The only requirement is the name and address of each incorporator, but as provided in the statutes, could be another legal person and not the real beneficial owner. Further, there are no mandatory requirements for corporations or company formation service providers to collect beneficial ownership information.

687. There is also no requirement in the BCA to file annual reports or to notify the Registrar of transfer of share ownership or changes in directors. There is a requirement to notify the Registrar of any amendment to the articles of incorporation, of a merger or consolidation where any two or more corporations consolidate into a new corporation, and of the dissolution of an entity.

688. There is a requirement under section 80 for all RMI corporations to maintain records of registered shareholders and a record of all bearer certificates issued, including the number, class and date of issuance. Resident domestic corporations must maintain this information either at the office of the corporation or at the office of its agent and registrar in the RMI. The BCA is silent on where records of registered shareholders of non-resident corporations are held.

#### Foreign Investment Business Licences

689. There are additional requirements for non-citizens wanting to establish a resident business in the RMI. Under the FIBL Act, every non-citizen required to obtain a foreign investment business licence shall submit an application to the Registrar. A non-citizen is defined to include both a non-citizen natural person and any legal entity in which a non-citizen owns an equity interest. The application for a foreign investment business licence shall contain the following information:

- (a) the name of the applicant's business;*

- (b) the applicant's principal place of business in the Republic and its authorized representative for purposes of the application;*
- (c) the purpose, scope, and objectives of the business activities to be conducted by the applicant;*
- (d) the proposed form of the business organization, including the ownership and management structure;*
- (e) the names, addresses, and citizenship of the initial owners and managers;*
- (f) proposals for ownership and management by citizens of the Republic;*
- (g) proposals to give employment preferences to citizens of the Republic and to train citizens of the Republic for positions in management and at other levels;*
- (h) anticipated capital contributions, revenue and expenditure for the first three (3) years of operation; and*
- (i) any other information the Cabinet deems necessary or appropriate.*

690. In addition to the above requirements under the FIBL Act, and in case the applicant for the licence is a foreign corporate entity, the FIBL Act requires the disclosure of the names, addresses and passport numbers of all the legal and beneficial shareholders of the proposed business together with the same details of directors, key, management and expatriate personnel (Regulation 505(1), item no. 7, Foreign Investment Business Application). However, there is no definition provided in the Regulation of "beneficial shareholders", no sanction for a false declaration, and no procedure in place to verify the authenticity of information provided in an FIBL application.

#### Partnership and Limited Partnership

There are two forms of partnerships in the RMI: resident and non-resident. Both types of partnerships are required to be registered under the Revised Partnership Act. Once registered, a partnership is considered a legal entity as provided in section 20 of the Act. Any person, as defined in Article 1 (14) of the Revised Partnership Act, can file to register a partnership. A person is defined to mean, " a natural person, partnership, limited partnership, trust, estate, limited liability company, association, corporation, custodian, nominee or any other individual or entity in its own or any representative capacity, in each case, whether domestic or foreign." The provisions concerning beneficial ownership, nominee arrangements and record keeping are similar with the BCA.

#### Non Profit and Cooperatives

691. Information on non-profit entities and cooperatives are addressed under the next section on NPOs. In brief, the regulatory and supervisory framework is similar to resident corporations.

#### Registrars

692. Pursuant to section 4 of the (BCA), and in similar worded sections in other Acts under the *Association Law*, the RMI has two Registrars of Corporations: a Registrar responsible for resident domestic and authorized foreign corporations, limited liability companies and partnerships; and a Registrar responsible for non-resident domestic corporations, partnerships, limited partnerships, limited liability companies, and foreign maritime entities.

##### (i) Resident Domestic (Doing Business in the RMI)

693. As Registrar of Corporations for resident domestic entities, the Attorney General is responsible for the filing and maintenance of all instruments required or permitted to be filed by resident entities under the BCA. According to the AG's office, they maintain an alphabetical index

(including on a spreadsheet) of all the names of all existing entities registered under the BCA pursuant to section 27. Under section 80 of the BCA, resident and non-resident domestic corporations are required to maintain internal records of the corporation, including books of accounts, minutes, and records of shareholders. The assessment team noted in the course of the interview that recent personnel movements within the OAG had affected the updating of these records. As of the time of the on-site, there was only one person handling the Registrar of Corporations for resident domestic entities.

694. The Registrar contacts the police to undertake a criminal background check of nominated directors only. There is no requirement to check whether the nominated directors or incorporators are acting in a nominee capacity, which as indicated, is permissible under the BCA and other Acts in the *Association Law*.

695. For applicants that are subject to the requirements under the FIBL Act, authorities disclosed that they do background and verification checks of all applicants by requesting, through a formal letter, the Police Commissioner to do a criminal background check. The effectiveness of this process for a FIBL licence might be questionable given, as noted under Recommendation 27 of this report, the RMI Police has not paid its Interpol fees and only one request was submitted to Interpol in the last 12 months with no response.

(ii) Non-resident (Not Doing Business in the RMI)

696. The TCMI is the Registrar responsible for non-resident legal persons i.e. corporations, partnerships, and foreign maritime entities. TCMI is a private company registered in the RMI. Registration of non-resident domestic entities is administered in part through International Registries, Inc. (IRI), a private company and an affiliate of TCMI, headquartered in Virginia, with 19 subsidiaries and branches globally in key markets such as: Baltimore, Dalian, Dubai, Ft. Lauderdale, Geneva, Hamburg, Hong Kong, Houston, Istanbul, London, Mumbai, New York, Piraeus, Roosendaal, Seoul, Shanghai, Singapore, Tokyo, and Zurich.

697. The Registrar (TCMI) does not deal directly with an applicant for incorporation. The registration process for non-resident corporations and partnerships involves qualified intermediaries (i.e. company formation service providers), such as accredited and licensed attorneys, accountants, or corporate formation specialists based around the globe. Only TCMI accredited intermediaries may submit applications to TCMI on behalf of applicants, either natural or legal persons.

698. The TCMI expects the qualified intermediaries to perform customer due diligence on their clients. TCMI officials have stated that, as an additional measure, if the names of directors, officers, or shareholders are made known to the Registrar, these individuals are also checked through World Check, which collects nationally and internationally maintained lists of specially designated legal or natural persons known or suspected of participation in, but not limited to, terrorism, terrorism financing, terrorism facilitation, narco-trafficking, or financial crimes. However, this is a practice rather than explicitly provided in RMI statute or regulation.

699. The formation and publicly filed documents of non-resident domestic corporations and partnerships are maintained by TCMI in a centralized computer database, with hard copies of documents held in the TCMI building in the RMI.

*Access to Information on Beneficial Owners of Legal Persons (c. 33.2):*

700. There are no specific powers in the BCA for the two Registrars of Incorporation (i.e. for resident domestic and non-resident) to investigate or access information held by entities formed under the Act. However, the BCA does not preclude the use of law enforcement powers to access information as described under section 2.5-2.6 of this report.

701. The key deficiency in relation to information access is that information held by both Registrars may not contain accurate and current information on beneficial and legal ownership, except possibly under the FIBL, as there is neither a mandatory requirement to provide such information at the registration stage, nor is there an on-going requirement to inform the Registrars of any changes. Further, if the company share registry is held outside of the RMI (potentially in the case of non-resident corporations or foreign corporations owning a resident corporation), timely access by RMI authorities may be difficult and subject to a mutual legal assistance process.

702. The available registration records of domestic corporations held by the OAG, including those with a FIBL are available to competent authorities upon request, and while the records are not publicly available, the Registrar will respond to request for information from the public, as long as a valid reason is submitted. However, the actual registration papers are not provided, only information to confirm the existence of a registered entity, and details of directors etc.

703. The information held by TCM is available upon request. Additionally, the Registrar (TCMI) works closely with the DFIU, the OAG, and the Ministry of Foreign Affairs. If a request is received from the DFIU regarding any allegations of malfeasance on the part of an RMI non-resident domestic entity, TCMI checks the records of the entity and provides all available information, as necessary, to the appropriate authorities.

*Prevention of Misuse of Bearer Shares (c. 33.3):*

704. Sections 28 and 42 of the BCA authorize a corporation to issue shares which may be in registered or bearer form. Resident domestic corporations, however, are not allowed to issue shares in bearer form. However, no additional safeguards are in place to prevent misuse of bearer shares.

*Additional Element—Access to Information on Beneficial Owners of Legal Persons by Financial Institutions)(c. 33.4):*

705. According to RMI authorities, records kept by the Registrar of resident domestic entities are classified as public documents and are available to the public upon the filing of a formal request. Most requests the AG receives are for verification purposes made by would-be creditors of a registered corporation. Both Registrars do not maintain an official website and online inquiry is not possible.

### **5.1.2. Recommendations and Comments**

706. The OAG lacks sufficient human resources, thereby hindering the efficient performance of its functions as Registrar of Corporations. Moreover, key personnel in the AG's office lack the necessary training to undertake their duties properly.

707. It is recommended that the OAG be provided with additional human resources and appropriate training to perform their functions.

708. It is also recommended the RMI should take the following measures:

- Make disclosure of beneficial ownership a mandatory requirement for both resident and non-resident corporations.
- Prevent the misuse of bearer shares and include appropriate sanctions in case of none compliance.
- Ensure accurate and timely information on beneficial ownership is available to law enforcement authorities.

### 5.1.3. Compliance with Recommendations 33

	Rating	Summary of factors underlying rating
<b>R.33</b>	NC	<ul style="list-style-type: none"> <li>• Except under the FIBL Act, there are no measures or mechanisms to verify, inquire and determine beneficial ownership.</li> <li>• Lack of timely access to accurate information on beneficial ownership.</li> <li>• There are no measures in place to ensure that bearer shares are not misused.</li> </ul>

## 5.2. Legal Arrangements—Access to Beneficial Ownership and Control Information (R.34)

### 5.2.1 Description and Analysis

#### *Legal Framework:*

709. The *Trust Act of 1994* and the *Trust Companies Act of 1994* govern the formation of trusts.

710. Formation of trusts can only be performed by and is solely at the discretion of the Marshall Islands Trust Company (“MITC”), who has authority to accept or deny any application. Under the *Trust Companies Act*, the Commissioner of Banking has been designated Commissioner of Trust Companies. MITC is an inactive company. Additionally, since its formation, the policy of MITC has been not to accept any applications for trusts, nor has it ever accepted any applications for trusts and there are no trustee companies licensed by the Commissioner of Trusts engaging in business within the RMI.

711. While there may be, in fact, no existing trust in the RMI formed by the MITC as of the on-site, trusts are nonetheless recognized in the RMI. The law on trusts is still valid and existing albeit unutilized. It provides specific recognition to RMI Court’s jurisdiction over foreign trust in the RM under section 148 of the Trust Law which states the Courts has jurisdiction where, “(b) a trustee of a foreign trust is resident in the Marshall Islands (c) any trust property of a foreign trust is situated in the Marshall Islands and (d) administration of any trust property of a foreign trust is carried on in the Marshall Islands”. The Associations Law also refers to “trust” in various provisions.

#### *Measures to Prevent Unlawful Use of Legal Arrangements (c. 34.1):*

712. There are no measures in place considering that the MITC has been inactive and the law was never enforced nor utilized.

#### *Access to Information on Beneficial Owners of Legal Arrangements (c. 34.2):*

713. Even if the law was enforced, there is neither provision nor requirement under section 206, (1) and (2) of the TCA (Application for Licence of a Domestic and Foreign Trust Company) that would allow inquiry or access to information on beneficial ownership.

### 5.2.2. Recommendations and Comments

714. As stated above, the TCA was never enforced but remains in the RMI statute books. RMI may consider repealing the TCA or amend it and incorporate the deficiencies under c. 34.1 and 34.2.

### 5.2.3. Compliance with Recommendations 34

	Rating	Summary of factors underlying rating
<b>R.34</b>	NC	<ul style="list-style-type: none"> <li>• There are no measures in place to prevent unlawful use of legal arrangements.</li> <li>• No provision allowing access to information on beneficial ownership.</li> </ul>

## 5.3. Non-Profit Organizations (SR.VIII)

### 5.3.1. Description and Analysis

715. The RMI has a relatively small non-profit organization (NPO) sector. The NPO sector can be categorized as follows: (i) Ecclesiastical/Religious Groups; (ii) Special Purpose Organizations Groups, and (iii) Grass Roots Community Groups. There are about 100 NPOs registered formally in RMI. Most are domestic NPOs, although there are a few foreign NPOs. Some domestic NPOs are connected internationally through funding provided by international donors, i.e. European Union, Australia and Japan. Community based organizations such as women's groups are common, although not always registered with the appropriate authorities.

716. There is an umbrella NPO organization, The Marshall Islands Council of NGOs (MICNGOS). It hosted its first ever National Conference in August 2010. The three day workshop covered a range of topics, including legal issues, financial and project reporting and project management.

#### *Legal Framework:*

717. The Registrar of Corporations in the OAG is responsible for the registration and filing of NPOs in the RMI. The following statutes and regulations govern the operations of incorporated and unincorporated NPOs in the RMI.

- *Non-Profit Corporations Act*
- *Associations Law (Business Corporations Act, Revised Partnership Act, Limited Partnership, Limited Liability Company Act, Unincorporated Associations Act)*
- *Cooperatives Act*
- *Counter Terrorism Act*

718. In section 302 of the *Non Profit Corporation Act*, a “non-profit corporation” means a resident domestic corporation of which no part of the income or profit is distributable to its members, directors, or officers. A non-profit corporation may be formed in accordance with existing

requirements, and rules and regulations promulgated by the Register of Corporations, in accordance with section 9 of the *Business Corporations Act* and *Limited Liability Company Act*.

719. Under the *Cooperatives Act*, in section 204, cooperative associations are also deemed “nonprofit,” inasmuch as they are not organized to make a profit for themselves or for their members, but only for their members as producers and/or procurers of cooperative products. Five or more persons may form a cooperative. Besides requirements specific to cooperatives, other requirements under the *Corporations Act* apply, including formation.

720. NPOs may also form as an unincorporated association in Part V - *Unincorporated Associations Act*. In section 209, an unincorporated association is defined as, “a body of individuals acting together for the prosecution of a common enterprise without a corporate charter, but expressed in its bylaws regulating its conduct, expressing its purpose and governing the relations of its members among themselves and to it, in the absence of statute.” There is a requirement for members to execute, sign and file an association certificate with the Register of Incorporation.

721. There is an overarching requirement under the CTA Act that states, “(3) No corporation, business, enterprise, partnership, association, or entity, shall be granted charitable or non-profit status in the Marshall Islands where there are reasonable grounds to believe that any funds solicited, collected, held, used, or owned by such corporation, business, enterprise, partnership, association, or entity, may be diverted to a terrorist or a terrorist organization.”

*Review of Adequacy of Laws & Regulations of NPOs (c. VIII.1):*

722. In 2006, the RMI conducted and submitted a sectoral review of its NPO sector to the APG. As part of this review process, two NPO Bills to enhance NPO regulation and supervision were submitted to the Nitijela for approval. However, they were not passed due to opposition from NGO groups. The two Bills were based on NGO laws in another jurisdiction – which among other requirements, included a requirement of a minimum of 20 members. However, it is not clear whether the draft NPO laws incorporated the requirements of SR.VIII.

723. There is a plan to introduce an NGO law in the future. The recent National conference of NGOs discussed the need to enhance the legal and governance framework for NPOs.

*Outreach to the NPO Sector to Protect it from Terrorist Financing Abuse (c. VIII.2):*

724. No competent authority has conducted outreach on FT risks to the NPO sector. The Law Society of the Marshall Islands has conducted education awareness raising of current legal requirements in relation to registration and reporting in order to encourage community groups to register formally. MIGNOS has conducted other awareness raising events but none were on FT risks in the NPO sector.

*Supervision or Monitoring of NPOs that Account for Significant Share of the Sector’s Resources or International Activities (c. VIII.3):*

725. There is no separate or additional monitoring of NPOs beyond the ongoing registration requirements with the Registrar of Incorporations; ongoing requirements pertain only to exception reporting e.g. filing any changes on article of associations. The only annual requirement is the payment of annual registration fees. There is no system in place to monitor non-compliance with annual fee payments or with exception reporting.

726. Domestic NPOs with funding from international donors are subject to donor funding and reporting requirements. These sometimes include audited reports, but in general audited reports of NPOs are not common given their size.

*Information maintained by NPOs and availability to the public thereof (c. VIII.3.1):*

727. The Registrar has discretionary powers in terms of dissemination of information. Registration documents and any variations submitted, while not available electronically, are available to the public on a request basis, as long as valid reasons are provided e.g. verifying the authenticity of an NPO. The extent of information provided depends on the nature and reasons behind the request.

728. Registration information includes the purpose of the NPO and the name and address of each incorporator but not necessarily information on the board of directors, senior management or the “mind and control” of the NPO.

729. NPOs are not required to make publicly available annual reports or audited statements.

*Measures in place to sanction violations of oversight rules by NPOs (c. VIII.3.2):*

730. There is only one sanction available under the *Corporations Act*. The High Court and Registrar can dissolve an association under the *Corporations Act*. Dissolution is available when there are internal problems or when the association fails to appoint a register agent, or pay its annual dues or carry out unlawful business, including providing insurance, trust or banking services :

*§103 the holders of one-half of all outstanding shares of a corporation entitled to vote in an election of directors may adopt at the meeting a resolution and institute a special proceeding in the High Court of the Republic for dissolution on one or more of the following grounds:*

*x x x*

*§104. Dissolution on failure to pay annual registration fee or appoint or maintain registered agent.*

*(1) Procedure for dissolution. On failure of a corporation to pay the annual registration fee or to maintain a registered agent for a period of one (1) year, the appropriate Registrar of Corporations shall cause a notification to be sent to the corporation through its last recorded registered agent that its articles of incorporation will be revoked unless within ninety (90) days of the date of the notice, payment of the annual registration fee has been received or a registered agent has been appointed, as the case may be. Furthermore, if any corporation abuses or misuses its corporate powers, privileges or franchises, including, but not limited to, participating in activities in violation of section 3(5) of this Act, the registered agent in its sole discretion shall have the power to resign as registered agent of such corporation. In either case, the Registrar of Corporations shall issue a proclamation declaring that the articles of incorporation have been revoked and the corporation dissolved as of the date stated in the proclamation....*

731. The provisions of the *Association Laws* are applicable to NPOs registered under the *NPO Act* and the *Cooperatives Act*. The *NPO Act* includes under section 104, “Dissolution of unincorporated associations by the High Court because of fraud in its management.”

732. The Registrar advised there has been no NPO dissolved in the last five years either by the High Court or Registrar.

*Licensing or registration of NPOs and availability of this information (c. VIII.3.3):*

733. The process of registering an incorporated NPO with the Registrar of Corporations is similar to profit making entities. There are some variations. For unincorporated associations, they are not required to submit Articles of Incorporation and By-laws, but they are required to execute and file the association's certificate (i.e. information on the association) and submit an application to the Registrar for approval. There is an additional requirement for an unincorporated organization to make its application known publicly with a notice in a newspaper or through some other public forum.

734. There is no background check required under the *NPO Act* or in the *Associations Law*. The registration documents are not passed, automatically, to the Revenue and Taxation Division (co-located in the same building); however, payment of the required fee to the Revenue and Taxation Division with receipt attached is required before the registration process can be completed.

735. In 2008, the Office of the Registrar of Corporation received 43 non-profit corporation registered and only 18 new for-profit corporations being registered, making it a total of 61 corporations registered. The Office has seen a surge in incorporation, especially non-profit organizations in 2009 and 2010, although no detailed statistics are available. This might be due to the taxation benefit of registration and the awareness raising program undertaken by MIGNOS.

736. The authorities have acknowledged that there are some NPOs operating based only on local government permits.

737. The actual registration documents and amendments held by the Registrar are available upon request to other competent authorities, including the Domestic Financial Intelligence Unit; Department of Public Safety; and Division of Customs, Revenue, Taxation and Treasury.

*Maintenance of records by NPOs, and availability to appropriate authorities (c. VIII. 3.4):*

738. Under section 80 of the *Corporations Act*, corporations are required to maintained any "records maintained by a corporation in the regular course of its business, including its stock ledger, books of account, and minute books, ... including further indicated that the actual registration papers are made available to other government agencies upon requests, including the Bureau of Public Safety and Revenue and Taxation." The Corporations Act is silent on the minimum period that such records are required to be kept.

739. There is no specific mention of record keeping requirements in the *Non-Profit Corporations Act and Unincorporated Associations Act*.

740. There are further powers available to competent authorities under section 84 to petition the High Court to direct the corporation to provide the information requested, if the corporation refuses to provide such records.

*Measures to ensure effective investigation and gathering of information (c. VIII.4):*

741. There is no special mechanism in place for the investigation of the NPO sector. The process as described in section 2 of the reports applies in the event of an investigation.

742. There is also no separate coordination mechanism for NPO matters. If needed, the Attorney General, as the Registrar of NPOs and a member of the AML/CFT Committee, can raise policy and operational concerns with other members of the AML/CFT Committee.

743. The authorities noted that there has never been an investigation of NPO in recent years, or any record of fraud or breaches of the law in the last five years.

*Responding to international requests regarding NPOs - points of contacts and procedures (c. VIII.5):*

744. The Registrar of Corporation is the contact point for international information exchange.

### 5.3.2. Recommendations and Comments

745. The NPO sector in the RMI is relatively small, and made up of mostly domestic NPOs, with some receiving donor funding from bilateral and multilateral donors, including the European Union and Australia. The following measures are proposed to enhance the supervisory and governance framework of the NPO sector in the RMI:

- The competent authorities should review the current draft NGO law and other laws governing the NPO sector, and incorporate, as necessary, the requirements of the FATF SR.VIII in either the proposed NGO law or existing laws, in consultation with the NPO Sector.
- The Registrar of Incorporation should maintain a separate database of NPOs registered to enhance transparency, improve supervision and facilitate information dissemination of the sector.
- The competent authorities should develop and implement a program to further enhance the transparency and accountability of the NPO sector, including assessing FT risk, and raising awareness of potential vulnerabilities in the sector, both FT and other criminal activities.

### 5.3.3. Compliance with Special Recommendation VIII

	Rating	Summary of factors underlying rating
<b>SR.VIII</b>	<b>NC</b>	<ul style="list-style-type: none"> <li>• Review of NPO sector not complete.</li> <li>• No outreach undertaken on FT risks.</li> <li>• Lack of oversight and monitoring of NPOs.</li> <li>• Lack of NPO transparency requirements.</li> <li>• Lack of available sanctions.</li> <li>• Registration requirements lack fit and proper test.</li> <li>• Lack of record keeping requirements.</li> </ul>

## 6. NATIONAL AND INTERNATIONAL CO-OPERATION

### 6.1. National Co-Operation and Coordination (R.31)

#### 6.1.1 Description and Analysis

*Legal Framework:*

*Mechanisms for Domestic Cooperation and Coordination in AML/CFT (c. 31.1):*

746. The Banking Commissioner/DFIU Head is the lead agency for AML/CFT implementation and chairs the AML/CFT Committee which comprises the DFIU Head, the Police Commissioner, the Assistant Secretary for Customs and a representative of the Attorney General. This Committee serves two functions: to discuss AML/CFT policy issues and to serve as the FIU Committee.

747. AML/CFT meetings are held quarterly; however on occasion meetings are held in between the quarterly meetings to address urgent working matters that arise during the course of any of the committee member's responsibilities. There are also meetings held to discuss operational issues but these are called as needed. No formal minutes are kept and follow-up is via email.

748. There was a recent focus on the mutual evaluation, as expected in the months preceding the on-site. An awareness raising workshop was conducted in January 2010 with industry stakeholders on the scheduled ME and stakeholders' role. Finally, the Committee's work has included the four AML/CFT related Bills submitted to the Nitijela in October 2010.

749. There is a Counter Terrorism Working Group consisting of the Attorney General, Banking Commissioner, TCMi and Immigration. The Group has not met for the last two years.

*Additional Element - Mechanisms for Consultation Between Competent Authorities and Regulated Institutions (c. 31.2):*

750. There are no formal mechanism for consultation between competent authorities and regulated institutions. There is neither a bankers association nor a financial sector industry association. Moreover, it is the practice for industry to be consulted after a new act has been passed by the Nitijela. This seems to be the case in regards to the amendments to the *Banking Act* to include STR reporting on FT and also the revised *AML/CFT Regulations*.

*Statistics (applying R.32):*

751. No detailed statistics or records are kept of national coordination meetings.

#### 6.1.2. Recommendations and Comments

752. The RMI is a relatively small jurisdiction and meetings are easily arranged and information shared. There should, however, be more formal recording of actions arising from both policy and operational meetings.

753. The Committee should oversee the conduct of a national AML/CFT risk assessment and develop a strategy to implement the recommendations contained in this mutual evaluation report.

### 6.1.3. Compliance with Recommendation 31

	Rating	Summary of factors underlying rating
<b>R.31</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• There is a lack of structured approach to AML/CFT coordination.</li> <li>• Policy level coordination mechanisms are not being used to effectively achieve key AML/CFT outcomes.</li> </ul>

## 6.2. The Conventions and UN Special Resolutions (R.35 & SR.I)

### 6.2.1. Description and Analysis

#### *Ratification of UN Instruments*

754. RMI acceded to the UN Convention for the Suppression of the Financing of Terrorism (1999) on 27 January 2003, and to the Vienna Convention and Palermo Conventions on 10 November 2010, within the 8 week period after the on-site.

#### *Implementation of UN Instruments*

755. Most of the Palermo's provisions are found in the ML provisions of the *Banking Act* and *Proceeds of Crime Act*, along with the noted deficiencies identified under paragraph 2.1.2 of this report.

756. To implement the FT Convention, RMI enacted the *Counter Terrorism Act* of 2002, which criminalized FT (with some deficiencies noted under 2.2 of this report) and the following punishable acts under the above-mentioned instruments and protocols:

- Weapons of Mass Destruction Offenses (s125)
- Internationally Protected Persons Offenses (s126)
- Hostage Taking (s127)
- Terrorist Bombing (s128)
- Plastic Explosives (s129)
- Safety of Civil Aviation Offenses(s130)
- Maritime Offenses (Safety of Maritime Navigation and Fixed Platform) (s135)
- Nuclear Material Offenses (s136).

#### *Implementation of UN SCRs relating to terrorist financing*

757. As noted in the discussions 2.4.1, the CTA has significant deficiencies regarding the freeze of terrorist funds within the context of UNSCRs 1267 and 1373.

### 6.2.2. Recommendations and Comments

758. Deficiencies in the existing law based on the Conventions should be addressed.

759. The noted deficiencies in the implementation of UNSCR 1267 and 1373 should be addressed particularly the freezing and designation mechanisms.

### 6.2.3 Compliance with Recommendation 35 and Special Recommendation I

	Rating	Summary of factors underlying rating
<b>R.35</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>Deficiencies in <i>Banking Act</i> on the ML offence.</li> </ul>
<b>SR.I</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>Effective measures to fully implement UNSCR 1267 and 1373 have not been put into place.</li> <li>There are no procedures for the designation and delisting of persons or entities within the context of UNSCR 1373.</li> </ul>

## 6.3. Mutual Legal Assistance (R.36-38, SR.V)

### 6.3.1. Description and Analysis

#### *Legal Framework:*

760. Mutual Legal Assistance in RMI is primarily governed by the *Mutual Legal Assistance in Criminal Matters Act* (“MACMA”) and the *Proceeds of Crime Act* (POCA).

#### *Widest Possible Range of Mutual Assistance (c. 36.1):*

761. All requests for international assistance are made by and through the Attorney General who may grant, refuse or postpone any action on the request under the conditions provided in section 410 (MACMA). Requests for assistance may include requests for: i) evidence gathering orders or search warrant (section 411); ii) transfers of detained persons (sections 412 & 413); iii) restraining orders (section 415); iv) enforcement of foreign confiscation or restraining orders (section 416); and v) locating proceeds of crime (section 417). These include, therefore, the widest possible range of mutual assistance for serious offence. However, the deficiencies highlighted in the ML and FT offence would limit the scope, depending on the nature of any MLA request.

762. Under section 411 of the MACMA, RMI may provide assistance to a foreign request by obtaining evidence by way of an application for a search warrant or evidence gathering order. An evidence-gathering order under section 411 of the MACMA,

*(a) shall provide for the manner in which the evidence is to be obtained in order to give proper effect to the foreign request, unless such manner is prohibited under the law of the RMI, and in particular, may require any person named therein to:*

- (i) make a record from data or make a copy of a record;*
- (ii) attend court to give evidence on oath or otherwise until excused;*
- (iii) produce to the High Court or to any person designated by the Court, anything, including any document, or copy thereof, or*

*(b) may include such terms and conditions, as the High Court considers desirable, including those relating to the interests of the person named therein or of third parties.*

763. “Proceeds of crime” whether under the MACMA (section 405 (n)) or under the POCA (section 205 (k)) means *“fruits of a crime, or any property derived or realized directly or indirectly from a serious offense and includes, on a proportional basis, property into which any property derived or realized directly from the offense was later successively converted, transformed or intermingled, as well as income, capital or other economic gains derived or realized from such property at any time since the offense”*. The definition includes “tainted property” or property used in, or in connection with, the commission of a serious offence (section 205 (p), POCA).

764. Pursuant to section 257 of the POCA,

*“Where a foreign country requests assistance with the location or seizure of property suspected to be tainted property in respect of an offense within its jurisdiction, the provisions of section 252 (Search warrants in relation to tainted property), 253 (Application for search warrants by telephone or other means of communication), and 254 (Searches in emergencies) apply, with the necessary changes in points of detail, provided that the Attorney General has, under section 408 of the Mutual Assistance In Criminal Matters Act, 2002, authorized the giving of assistance to the foreign country.”*

765. Further, under section 261 of the POCA,

*“where a foreign country requests assistance to locate or seize property suspected of being tainted property in respect of an offense ... the provisions of section 258 (production orders) shall apply to the request, with the necessary changes in points of detail.”*

766. Whenever the foreign request pertains to the location or seizure of suspected tainted property, an application for production order is made pursuant to section 258 of the POCA. An authorized officer may apply *ex parte* in writing to the judge for a production order against a person whom the officer has probable cause to believe is in possession or control of (a) a document relevant to identifying, locating or quantifying property of the defendant, or to identifying or locating a document necessary for the transfer of property of the defendant; or (b) a document relevant to identifying, locating or quantifying tainted property in relation to the offence, or to identifying or locating a document necessary for the transfer of tainted property in relation to the offence.

767. Foreign requests for RMI restraining orders as well as enforcement of foreign confiscation orders are allowed under sections 415 and 416 of the MACMA. Moreover, the Attorney General is authorized to assist a foreign country in locating property believed to be proceeds of a serious crime committed in the requesting country. The Attorney General may authorize the making of any application to the High Court, for the purpose of acquiring the information sought by the foreign country (section 417, MACMA).

768. “Tainted property” means (i) property used in, or in connection with, the commission of a serious offence; or (ii) proceeds of crime (section 205 (p)), POCA. It does not cover instrumentalities intended to be laundered or assets of corresponding value.

769. The lack of criminalization of a number of categories of predicate offences would impede MLA under the MACMA in relation to those predicate offences.

*Provision of Assistance in Timely, Constructive and Effective Manner (c. 36.1.1):*

770. While the MACMA does not provide for clear timeframes in which MACMA requests have to be handled, the authorities stated that in practice mutual legal assistance requests are being dealt

with within about a week. No statistics or case studies were provided to the assessors to demonstrate that MLA is provided in a timely and effective manner.

*No Unreasonable or Unduly Restrictive Conditions on Mutual Assistance (c. 36.2):*

771. Section 404 provides that the MACMA applies to the RMI and to any foreign State that has an agreement with or enters into a reciprocal agreement on assistance in criminal matters with the RMI. One such agreement is RMI-US *Agreement on Extradition, Mutual Assistance in Law Enforcement Matters and Penal Sanction*, concluded in April 2003 pursuant to section 175 of *The Amended Compact of Free Association*. The other agreement is the tri-lateral extradition treaty of RMI, Palau and the Federated States of Micronesia. RMI has no other formal arrangements with other jurisdictions on mutual legal assistance.

Section 410 of the MACMA provides the conditions for the grant or denial of an MLA request:

*The Attorney-General may, in respect of any request from a foreign State for international assistance in any investigation commenced or proceeding instituted in that State relating to a serious offense:*

- (a) grant the request, in whole or in part, on such terms and conditions as the Attorney-General thinks fit;*
- (b) refuse the request, in whole or in part, on the ground that, in the opinion of the Attorney-General, to grant the request would be likely to prejudice the sovereignty, security or other essential or public interest of the RMI or would result in manifest unfairness or a denial of human rights, or it is otherwise appropriate in all circumstances of the case, that the assistance requested should not be granted, in whole or in part; or*
- (c) after consulting with the competent authority of the foreign State, postpone the request, in whole or in part, on the ground that granting the request immediately would be likely to prejudice the conduct of an investigation or proceeding in the RMI.*

772. Section 410 (b) above was taken from Article 21 (b) of the Palermo Convention. It was modified to include other grounds for refusal to grant requests for assistance namely: i) manifest unfairness; ii) denial of human rights; and, iii) the denial is appropriate under the circumstances. The fact that an offence may also involve fiscal matters is not a ground for the denial of a request for assistance under the MACMA.

773. The form and contents of a foreign request for mutual legal assistance is provided under section 409 (1) (MACMA). Non-compliance with section 409 is not a ground for denying a request for assistance. A request may nonetheless be granted if the same is found to be necessary after consultation (section 409 (2) MACMA).

*Efficiency of Processes (c. 36.3):*

774. There are no clear and efficient processes in place for the execution of mutual legal assistance requests in a timely way and without undue delay. The authorities stated that requests received would be dealt with immediately upon receipt and that a response would be sent back to the requesting country within a week. However, due to the fact that only one request has ever been received, albeit

not AML/CFT related, no documentation could be provided to show that in practice, mutual legal assistance requests are being dealt with efficiently and without undue delay.

*Provision of Assistance Regardless of Possible Involvement of Fiscal Matters (c. 36.4):*

775. MLA requests involving fiscal matters is not one of the grounds under section 410 (b), MACMA, where the Attorney General is allowed to deny the request.

*Provision of Assistance Regardless of Existence of Secrecy and Confidentiality Laws (c. 36.5):*

776. The RMI has not addressed this issue. Note, however, that secrecy and confidentiality are not among the explicit grounds for refusing a request for assistance.

*Availability of Powers of Competent Authorities (applying R.28, c. 36.6):*

777. This is covered by sections 257 (in relation to sections 252 to 254) and 261 (in relation to section 258) of the POCA and under section 411 of the MACMA where competent authorities may apply for a search warrant, evidence gathering order or production order.

778. Section 252 authorizes the conduct of a search on persons or premises or to seize property found in the conduct of such search. Section 258, on the other hand, authorizes the production of relevant documents material to identifying, locating or transferring tainted property.

*Avoiding Conflicts of Jurisdiction (c. 36.7):*

779. The RMI has not addressed this issue. However, under section 104 (4) of the CTA, it is provided that “*where a person is suspected to have engaged in terrorism and the alleged offender is present in the Marshall Islands, in a case where the Marshall Islands has jurisdiction, and the alleged offender is not extradited to a foreign country that has established jurisdiction over the offense or the alleged offender, the Attorney-General shall whether or not the offense was committed in the Marshall Islands, have authority to prosecute the person in accordance with any law that is for the time being in force in the Marshall Islands.*”

## **SRV**

*International Cooperation under SR V (applying c. 36.1-36.6 in R. 36, c. V.1):*

780. Section 115 (2) of the CTA provides that any MLA provided under the CTA shall be carried out pursuant to and in accordance with the MACMA.

781. Requests for assistance under the MACMA may include requests for: i) evidence gathering orders or search warrant (section 411); ii) transfers of detained persons (sections 412 & 413); iii) restraining orders (section 415); iv) enforcement of foreign confiscation or restraining orders (section 416); and v) locating proceeds of crime (section 417).

782. Aside from the MACMA, it would appear that the provisions of the POCA, specifically sections 257 and 261 would similarly be applicable considering that FT and other violations under the CTA would constitute “serious offenses” under the POCA. This would mean, therefore, that the remedies and provisions for search warrants, evidence gathering orders and production orders would similarly be available to authorities in order to provide assistance involving terrorist and FT-related international request for legal assistance.

783. The MLA discussions under 6.3.1 are equally applicable to SR V. The same is true, however, with regard to the deficiencies noted above: i) no for clear timeframes in which MACMA requests have to be handled; and ii) no clear and efficient processes in place for the execution of mutual legal assistance requests in a timely way and without undue delay.

*Additional Element under SR V (applying c. 36.7 & 36.8 in R.36, c. V.6):*

784. Regarding the issue of determining the best venue for prosecution, section 104 (4) of the CTA provides “where a person is suspected to have engaged in terrorism and the alleged offender is present in the Marshall Islands, in a case where the Marshall Islands has jurisdiction, and the alleged offender is not extradited to a foreign country that has established jurisdiction over the offense or the alleged offender, the Attorney-General shall whether or not the offense was committed in the Marshall Islands, have authority to prosecute the person in accordance with any law that is for the time being in force in the Marshall Islands”

### **Recommendation 37**

*Dual Criminality and Mutual Assistance (c. 37.1 & 37.2):*

785. Dual Criminality is observed in the grant of mutual assistance under the MACMA. The provisions of the MACMA limits MLA to ‘serious offense’, which, under section 405 (q) of the MACMA is defined as follows:

(q) “serious offense” means an offense against a provision of:

(i) any law of the RMI, which is a criminal offense punishable by imprisonment for a term of more than one year;

(ii) a law of a foreign country, in relation to acts or omissions, which had they occurred in the RMI, would have constituted a criminal offense punishable by imprisonment for a term of more than one year;

786. Section 405 (q)(ii) is comprehensive enough that would allow RMI authorities to provide assistance using the “same conduct” approach to MLA. For example, under Article III of the RMI and US “Agreement on Extradition, Mutual Assistance in Law Enforcement Matters and Penal Sanction,”, it states “that this condition shall not be interpreted so as to require that the offense described in the laws of both Governments be identical in those matters which do not affect the nature of the crime”.

*International Cooperation under SR V (applying c. 37.1-37.2 in R. 37, c. V.2):*

787. Dual criminality is similarly observed in MLA requests under the CTA considering that the MACMA is made applicable pursuant to section 115 (2) of the CTA. Consequently, the restrictive application of the MACMA also applies to terrorism and FT related MLA requests made under the CTA. (Please see discussion under Rec. 37).

### **Recommendation 38**

*Timeliness to Requests for Provisional Measures including Confiscation (c. 38.1):*

788. Giving effect to foreign requests for RMI restraining orders as well as enforcement of foreign confiscation orders are allowed under sections 415 and 416 of the MACMA. Moreover, the Attorney General is authorized to assist a foreign country in locating property believed to be proceeds of a serious crime committed in the requesting country. The Attorney General may authorize the making of any application to the High Court, for the purpose of acquiring the information sought by the foreign country (section 417, MACMA).

789. “Proceeds of crime” under section 405 (n) of the MACMA means “*fruits of a crime, or any property derived or realized directly or indirectly from a serious offense and includes, on a proportional basis, property into which any property derived or realized directly from the offense was later successively converted, transformed or intermingled, as well as income, capital or other economic gains derived or realized from such property at any time since the offense*”. The definition does not cover instrumentalities intended for use in the commission of ML and FT nor of property of corresponding value.

790. There are no clear and efficient processes that will provide for a timely response to MLA requests.

*Property of Corresponding Value (c. 38.2):*

791. The definition of “tainted property” under the POCA and “proceeds of crime” under the MACMA does not include property of corresponding value. Therefore there is no scope for the RMI to respond to such request.

*Coordination of Seizure and Confiscation Actions (c. 38.3):*

792. This is governed by sections 415-417 of the MACMA. As stated earlier, the provisions of the MACMA would only apply in respect to a foreign State that has an arrangement with or enters into a reciprocal agreement on assistance on criminal matters with the RMI (section 404, MACMA).

*International Cooperation under SR V (applying c. 38.1-38.3 in R. 38, c. V.3):*

793. FT-related requests for legal assistance made under the CTA are carried out utilizing the provisions of the MACMA, specifically sections 415-417 thereof. Under the latter provisions, RMI can provide assistance with regard to a) requests for RMI restraining orders (section 415); b) enforcement of foreign confiscation or restraining orders (sec. 416) and c) assists in locating property believed to be proceeds of a serious crime. However, the definition of “proceeds of crime” under section 405 (n) of the MACMA does not cover instrumentalities intended for FT nor of property of corresponding value.

*Asset Forfeiture Fund (c. 38.4):*

794. The RMI authorities indicated that they intend to establish such a fund. However, there is neither plan nor concrete action at this stage towards this stated intent.

*Sharing of Confiscated Assets (c. 38.5):*

795. Under section 418 of the MACMA, “*the Attorney- General may enter into an arrangement with the competent authorities of a foreign country, in respect of money laundering and proceeds of crime, for the reciprocal sharing with that country of such part of any property realized:*

*(a) in the foreign country, as a result of action taken by the Attorney-General pursuant to section 407(4); or*

*(b) in the RMI, as a result of action taken in the RMI pursuant to section 416 (1), as the Attorney-General thinks fit.”*

*Additional Element under SR V (applying c. 38.4-38.6 in R. 38, c V.7):*

796. As described above, section 418 of the MACMA appears to be sufficiently comprehensive as to allow asset sharing arrangements that involve FT-related funds.

*Statistics (applying R.32):*

797. There are no available AML/CFT-related statistics as there has been no request made to RMI as of the time of the onsite. There has been one MLA request on a health related matter but not AML/CFT related. This request was submitted through diplomatic channels and was referred to the Ministry of Health for action.

### **6.3.2. Recommendations and Comments**

798. RMI should enhance the offence of ML to ensure that MLA can be provided in relation to proceeds from the widest range of predicate offences.

799. While there are available provisions and remedies that allow RMI to respond to an MLA request, there are noted deficiencies that would hinder RMI’s ability to provide assistance. These include the absence of clear timeframes and processes that would allow timely and speedy responses, the definition and coverage of the property that may be the subject of the request, and the limitation on the MACMA’s application.

800. RMI should consider reviewing and updating the provisions of the MACMA and its partner legislations, e.g. the POCA, and provide regulations that:

#### **Recommendation 36**

- Comprehensively criminalise all categories of designated offences to ensure MLA provisions under MACMA can be applied to the widest range of proceeds of crime.
- Indicate reasonable time periods within which requests for legal assistance can be acted upon.
- Amend the MACMA so the application of MLA is not conditional upon formal and bilateral agreements or arrangements with a foreign State being made.
- Develop clear and efficient procedures for the execution of MLA requests.
- Develop procedures to provide mechanisms to provide for the best venue for ML prosecutions.

#### **Recommendation 37**

- Amend the MACMA to allow for the delivery of mutual legal assistance on less intrusive and non compulsory measures.

**Recommendation 38**

- Include a provision in the MACMA for equivalent value seizure and confiscation of assets.
- Establish a mechanism for feedbacks and follow-ups.

**SR V**

- Indicate reasonable time periods within which requests for legal assistance can be acted upon.

**6.3.3. Compliance with Recommendations 36 to 38 and Special Recommendation V**

	Rating	Summary of factors relevant to s.6.3 underlying overall rating
<b>R.36</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Scope of coverage of the ML offence in the RMI undermines effectiveness of the MLA framework.</li> <li>• The MACMA is restrictive in the sense that it only applies to cases where formal and bilateral agreements or arrangements with a foreign State have been made.</li> <li>• The MACMA does not provide for clear timeframes within which MLA requests are to be handled.</li> <li>• There are no clear and efficient processes in place for the execution of MLA requests without undue delay.</li> <li>• No mechanism to determine the best venue for ML prosecutions.</li> <li>• Effectiveness cannot be established.</li> </ul>
<b>R.37</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• Dual criminality limits the ability to render assistance.</li> </ul>
<b>R.38</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>• There are no clear and efficient processes to provide a timely response to requests.</li> <li>• No clear provision for property of corresponding value.</li> </ul>
<b>SR.V</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• No clear timeframes and guidance for the expedient processing of MLA.</li> <li>• The MACMA is restrictive in the sense that it only applies to cases where formal and bilateral agreements or arrangements with a foreign State have been made.</li> <li>• Ability to render assistance is limited by dual criminality.</li> <li>• Effectiveness cannot be established.</li> </ul>

## 6.4. Extradition (R.37, 39, SR.V)

### 6.4.1. Description and Analysis

#### *Extradition*

801. The *Criminal Extradition Act (CEA)* sets out the procedures for extradition. Under section 203, the Cabinet has the authority to have arrested and delivered up to the executive authority of another government any person charged with “*treason, felony or other crime, who has fled from justice and is found in the Republic*”.

802. The *CEA* provides rules for the extradition of persons from a foreign country to RMI (section 206) and surrender of persons to a foreign state upon request of the latter (sections 207 and 208, *CEA*).

#### *Money Laundering and terrorist financing as Extraditable Offences (c. 39.1):*

803. The CTA specifically provides that terrorism offences are extraditable offences (section 114). No similar provision exists for ML under the *Banking Act*. Given the broad wording of the *CEA* only requiring that the person to be extradited has been charged with a crime, ML is deemed extraditable under the *CEA*.

#### *Extradition of Nationals (c. 39.2):*

804. According to the authorities, RMI does not extradite its own nationals. The *CEA* makes reference to “any person” as the subject of extradition. However, it is not specified in the Act, whether the reference to “any person” includes its own nationals, and neither is there a provision whereby a foreign jurisdiction seeking extradition of an RMI national can submit its case to the competent RMI authorities for the purpose of prosecution.

However, in the RMI and the US *Agreement on Extradition, Mutual Assistance in Law Enforcement Matters and Penal Sanction*, RMI nationals can be extradited to the U.S. This is provided under Article I: Obligation to Extradite, which states, “*Government of the United States shall extradite to the Republic of the Marshall Islands, and the Government of the Republic of the Marshall Islands shall extradite to the United States, subject to the provisions and conditions described in this Agreement, any person found in their respective jurisdictions against whom the requesting Government is proceeding for an offense or who is wanted by that Government for the enforcement of a sentence.*”

#### *Cooperation for Prosecution of Nationals (applying c. 39.2(b), c. 39.3):*

805. There is no provision under the *CEA* that would authorize the domestic prosecution for ML of an RMI national as an alternative to extradition. In respect of FT however, section 4(4) of the CTA provides that where a person is suspected to have engaged in terrorism and is present in the RMI, in a case where the RMI has jurisdiction, and the alleged offender is not extradited to the foreign country that has established jurisdiction over the offence or alleged offender, the AG shall, whether or not the offence was committed in the RMI, have authority to prosecute the person in accordance with the laws of the RMI. This provision may be interpreted to also include reference to an RMI national given that the definition of “person” is wide enough to be interpreted in this manner.

*Dual Criminality and Mutual Assistance (c. 37.1 & 37.2):*

While not specifically provided under the CEA, authorities maintain that the extradition provisions of the CEA apply the dual criminality principle.

*Efficiency of Extradition Process (c. 39.4):*

806. There are no procedures that provide clear timeframes for processing extradition requests.

*Additional Element (R.39)—Existence of Simplified Procedures relating to Extradition (c. 39.5):*

807. The RMI has not as yet adopted a simplified process.

*SRV (V.4)*

808. Terrorism offences are extraditable offences under section 114 of the CTA. Authorities stated that RMI does not extradite its own nationals.

809. Under section 4(4) of the CTA, however, it is provided that “where a person is suspected to have engaged in terrorism and is present in the RMI, in a case where the RMI has jurisdiction, and the alleged offender is not extradited to the foreign country that has established jurisdiction over the offense or alleged offender, the AG shall, whether or not the offense was committed in the RMI, have authority to prosecute the person in accordance with the laws of the RMI”. It is unclear whether the term “any person” includes an RMI national considering that statement by Authorities against extradition of RMI nationals.

810. There are no procedures that provide clear timeframes for processing extradition requests.

*Additional Element under SR V (applying c. 39.5 in R. 39, c V.8):*

811. The RMI has not as yet adopted extradition procedures.

*Statistics (applying R.32):*

812. No statistics on extradition were available at the time of the on-site.

**6.4.2. Recommendations and Comments**

813. RMI should enhance the offence of ML to ensure that extradition is available in relation to laundering from the widest range of predicate offences.

814. RMI should consider revising and updating its extradition law to include provisions for clear timeframes and processes that would enable a timely response to any extradition request, and make clear whether RMI nationals may be extradited, and if not, provide for domestic prosecution in lieu of extradition.

**6.4.3. Compliance with Recommendations 37 & 39, and Special Recommendation V**

	Rating	Summary of factors relevant to s.6.4 underlying overall rating
<b>R.39</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Doubts exist as to whether RMI nationals can be extradited.</li> <li>• There is no provision authorizing the domestic prosecution of an RMI national who has not been extradited.</li> <li>• No procedures that provide clear timeframes for processing extradition</li> </ul>

		requests.
<b>R.37</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Dual criminality limits the ability to render assistance with regard to extradition.</li> </ul>
<b>SR.V</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• No clear timeframes and guidelines for the expedient processing of extradition requests.</li> <li>• Doubts exist as to whether nationals can be extradited.</li> <li>• Effectiveness cannot be established.</li> </ul>

## 6.5. Other Forms of International Co-Operation (R.40 & SR.V)

### 6.5.1. Description and Analysis

#### *Widest Range of International Cooperation*

815. Relevant legislations such as the *Banking Act* and CTA provide the legal basis for information exchange outside of the MLA process. Section 167 (j) explicitly provide the Banking Commissioner with, “...the authority and ability to exchange information between international administrative authorities”, and in section 167 (k), “...to facilitate and assist international administrative authorities in conducting proceeds of crime, money laundering, and or the financing of terrorism investigations.”

816. The CTA in section 116 also explicitly allows for intelligence sharing by the Attorney General and other law enforcement authorities and officers designated by the former to, “to share and disclose intelligence information relating to terrorism, terrorist organizations, transnational crime, illicit drugs, money laundering, illegal arms-trafficking...and provide early warnings of such matters to the competent law enforcement authorities”. Section 116 goes on to outline the various categories of “any foreign country”. These include specifically any foreign State that is a member of the Pacific Islands Forum; (c) the US, in accordance with the duties and responsibilities of the RMI under the Compact of Free Association with the US; and (d) any other foreign State that is a member of the United Nations. As stated, section 116 captures broader transnational crime matters, including ML and crime in general.

817. Further, section 175 of the Revised Compact of Free Association provides for a broad range of law enforcement measures between the RMI, the US and other compact states. This is further articulated in the *Agreement on Extradition, Mutual Assistance in Law Enforcement Matters and Penal Sanction*, which covers also non MLA cooperation.

#### *Provision of Assistance in Timely, Constructive and Effective Manner*

818. There is regular cooperation between the Police (DPS), including the CID, with foreign law enforcement agencies, particularly the Australian Federal Police as outlined under Recommendations 27 and 28. There were no detailed statistics provided on information exchanged.

819. The DPS also has access to traditional law enforcement databases and obtains investigative assistance through the South Pacific Islands Criminal Intelligence Network (SPICIN), INTERPOL, and the US National Crime Information Center (NCIC) However, as highlighted earlier, DPS cannot access INTERPOL information as its fees are overdue.

820. The RMI is a member of the Oceania Customs Organization (OCO). In addition, RMI Customs works together with other Customs in the Pacific and Oceania region, including the World Customs Organization.

821. The DFIU may have access to information from FIUs in foreign jurisdictions through its membership of the Egmont Group of FIUs. Statistics on information exchange is provided under Recommendation 26. In practice, the DFIU has been more a recipient of information requests, rather than proactively requesting or disseminating information.

822. The Banking Commission has exchanged supervisory information on one occasion— in 2009 with a European country. This involved the Banking Commission confirming the identification information of a company registered in the RMI.

823. TCMI has responded to foreign requests for verification of company registration and other information, including on company formation intermediaries. As noted, however, in Recommendation 33, there are significant gaps in terms of information held on beneficial owners and/or the controlling mind (s) behind a corporate entity.

#### *Clear and Effective Gateways for Exchange of Information*

824. The Transnational Crime Unit (TCU) within the DPS deals with all international requests for information, including with Interpol. It has one dedicated Interpol liaison officer.

825. The Banking Commissioner, as head of both the Banking Commission and DFIU, is the gateway for the exchange of financial intelligence.

826. The OAG is also a designated gateway for information exchange on terrorism related and other transnational crime matters. The Registrar of Corporations in the OAG is responsible for information exchange on corporations operating in the RMI. But the gateway for the exchange of information for the Registrar (TCMI) of non-resident corporations seems to be through multiple avenues, and not always directly by the TCMI.

827. On FT threats specifically, section 118 (2)(a) of the CTA deals with establishing communication channels to allow for rapid exchange of information concerning all aspects of terrorism and terrorist organizations. This includes exchanging information on cross border entry and exit information.

#### *Spontaneous Exchange of Information*

828. As indicated in section 2.5 of this report, the legal powers of information exchange contained in section 167 of the *Banking Act* and section 116 of the CTA do not preclude the spontaneous exchange of information. In fact, under section 118 of the CTA, the RMI is tasked to, “...cooperate in the prevention of terrorism by exchanging information to provide early warning of possible terrorism.”

#### *Making Inquiries on Behalf of Foreign Counterparts*

829. Section 167(k) of the *Banking Act* provides the Banking Commissioner with the authority and ability to facilitate and assist international administrative authorities in conducting proceeds of crime, ML and/or financing of terrorism investigations. As noted under Recommendation 26, the Banking

Commissioner, in its dual role also as DFIU head, has exercised these powers in response to financial intelligence requests.

830. Section 118 (2) (C) of the CTA provides for conducting inquiries with respect to terrorists and members of terrorist organizations, including on FT.

*Conducting of Investigations on Behalf of Foreign Counterparts*

831. The CTA in section 116 authorizes the Attorney General to conduct investigations on behalf of foreign counterparts. Other competent authorities are authorized to conduct investigations on behalf of foreign counterparts, subject to approval and where permitted by domestic law. As noted, the provisions of section 116 include ML and any transnational crime.

*No Unreasonable or Unduly Restrictive Conditions on Exchange of Information*

832. The *Banking Act* and CTA provisions for exchange of information do not contain disproportionate or unduly restrictive conditions.

*Provision of Assistance Regardless of Possible Involvement of Fiscal Matters*

833. There is no explicit requirement providing or excluding the provision of assistance because of possible involvement of fiscal matters.

834. The RMI is a member of the OECD's Global Forum on Transparency and Exchange of Information. It was originally listed as uncooperative and was removed in 2007 after committing to a program to improve transparency.

835. The RMI has signed Tax Information Exchange Agreements (TIEAs) with the USA, Australia and Kingdom of the Netherlands. A further two TIEAs (with New Zealand and Ireland) are close to being signed. Negotiations are currently underway with other countries to secure a minimum of twelve TIEAs, in order to comply with the OECD requirements.

836. RMI is also a member of the All Islands Tax Administrations Association (AITAA) and the Pacific Islands Tax Administrations Association (PITAA).

*Provision of Assistance Regardless of Existence of Secrecy and Confidentiality Laws*

837. There is nothing in the CTA or *Banking Act* that would limit the intelligence or information available under relevant sections of both Acts referred to previously.

*Safeguards in Use of Exchanged Information (c. 40.9):*

838. Pursuant to the *Banking Act* Part XIII – Money Laundering Section 167(1) (m) and Part XI – General Section 154 (2), the Banking Commissioner and every officer and employee working under the Commissioner adheres to the secrecy of all banking information.

839. Section 550 of the *Public Safety Act* provides for confidentiality provisions for officers of the DPS, including police officers. Section 555 (a) provides for discharge or suspension, "... if an officer divulges any confidential information to anyone without prior approval of the Director, unless such disclosure is absolutely necessary under the circumstance". Criminal sanctions for unauthorized disclosure are provided in section 557 of the same Act.

*Additional Element—Exchange of Information with Non-Counterparts*

840. The wording of the relative sections in the *Banking Act* and CTA are sufficiently broad to allow for information exchange with non-counterparts.

*Additional Element—Provision of Information to FIU by Other Competent Authorities pursuant to request from Foreign FIU (c. 40.11)*

841. The RMI authorities advised that the DFIU has received requests for non-financial intelligence specific information, principally in relation to companies registered by the TCMI and has responded to these requests by obtaining such information in the first instance from TCMI.

*Statistics (applying R.32):*

842. The actual number of information exchanged is limited. It is difficult to assess the effectiveness and efficiency of other forms of international cooperation, suffice to note that there is a legal framework for such information exchange.

### 6.5.2. Recommendations and Comments

843. The RMI has the legal framework for the exchange of information outside of the MLA process. Given the size of the jurisdiction, there has been limited scope for information exchange. The efficacy of the process for such exchanges is harder to assess, although they seem to function well enough given the limited demand placed upon the current arrangements.

844. The RMI should explore options to enhance its framework for the exchange of information on non-resident corporations.

### 6.5.3. Compliance with Recommendation 40 and Special Recommendation V

	Rating	Summary of factors relative to s.6.5 underlying overall rating
<b>R.40</b>	<b>LC</b>	<ul style="list-style-type: none"> <li>The effectiveness and efficiency of the current legal and administrative framework is difficult to determine due to the lack of statistical data across all relevant competent authorities.</li> </ul>
<b>SR.V</b>	<b>PC</b>	<ul style="list-style-type: none"> <li><i>This is a composite rating</i></li> </ul>

## 7. OTHER ISSUES

### 7.1. Resources and Statistics

845. There is an overall lack of resources to effectively implement the requirements of the AML/CFT regime, particularly the additional requirements under the newly amended *AML/CFT Regulations 2010* and the *Cross-Border Declaration Act 2010*. While it is understandable in a small jurisdiction for government officials to assume more than one post, the nature of certain work functions is better separated, at least at the operational levels, if not at the management level.

846. Additional staffing resources at the operational level, would for example, enable some staff in the Banking Commission and DFIU to specialize in FIU functions and/or AML supervision functions, and other staff to focus on prudential and/or AML/CFT supervisory functions.

847. There also needs to be additional resources devoted to ML laundering investigation as noted previously in this report.

	Rating	Summary of factors underlying rating
<b>R.30</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• Lack of DFIU dedicated resources and specialized financial intelligence expertise.</li> <li>• Lack of expertise and dedicated resources to undertake financial investigation/s of ML/FT and proceeds of crime.</li> <li>• Lack of staff resources in Banking Commission/DFIU to conduct timely onsite and offsite AML supervision and monitor and enforce compliance of subject entities with detailed requirements of revised AML regulations.</li> <li>• Lack of training, awareness and expertise in AML/CFT.</li> </ul>
<b>R.32</b>	<b>PC</b>	<ul style="list-style-type: none"> <li>• There is no structured approach to collecting and maintaining AML/CFT related statistics.</li> </ul>

### 7.2. Other relevant AML/CFT Measures or Issues

848. The assessment team observed the RMI has used international technical assistance and training in an effective manner. The RMI has implemented amendments to laws, regulations and procedures based on international technical advice.

849. The assessment team also observed, in some instances, that some officials are not fully aware of the details contained in their laws and/or regulations. This situation is due to numerous factors, not unique to this jurisdiction. One of the reasons might be that local officials, because of various reasons, have not been involved in the minute details of drafting legal instruments and other documents, given that external international advisers have undertaken the drafting.

#### 7.2.1 Recommended Action

850. International technical advice would be more effective if line agencies are actively involved in the drafting of laws, regulations, other enforceable means or guidelines.

**Table 1. Ratings of Compliance with FATF Recommendations**

<b>Forty Recommendations</b>	<b>Rating</b>	<b>Summary of factors underlying rating<sup>6</sup></b>
<b>Legal systems</b>		
1. ML offence	<b>PC</b>	<ul style="list-style-type: none"> <li>• The definition of ML is not fully in accord with the Vienna and Palermo Conventions.</li> <li>• The definition of “serious offense” does not cover the entire FATF designated list of offences.</li> <li>• Offences such as piracy of products, human trafficking and migrant smuggling, market manipulation and insider trading, smuggling and certain environmental crimes are not included.</li> <li>• Doubts exists as to whether self-laundering is allowed.</li> <li>• Lack of effective implementation.</li> </ul>
2. ML offence—mental element and corporate liability	<b>LC</b>	<ul style="list-style-type: none"> <li>• The scope of criminal liability for legal persons is limited to bodies corporate and does not include the full range of legal persons as defined in the methodology.</li> <li>• Lack of effective implementation.</li> </ul>
3. Confiscation and provisional measures	<b>LC</b>	<ul style="list-style-type: none"> <li>• The term “tainted property” does not cover instrumentalities intended for use in the commission of any ML, FT or other predicate offences, and property of corresponding value.</li> <li>• Lack of effective implementation.</li> </ul>
<b>Preventive measures</b>		
4. Secrecy laws consistent with the Recommendations	<b>C</b>	<ul style="list-style-type: none"> <li>• The recommendation is fully observed.</li> </ul>
5. Customer due diligence	<b>PC</b>	<ul style="list-style-type: none"> <li>• CDD obligations under the revised AML/CFT regulations have not yet been implemented by a number of entities meeting the definition of financial institution or cash dealer.</li> <li>• Effectiveness of arrangements to comply with the detailed CDD obligations of the revised <i>AML/CFT Regulations</i> has not yet been verified by the Banking Commission through compliance monitoring.</li> <li>• Financial institutions and cash dealers do not have adequate policies and procedures to determine the natural persons who ultimately control customers who are legal persons.</li> </ul>
6. Politically exposed persons	<b>LC</b>	<ul style="list-style-type: none"> <li>• Effectiveness of arrangements to comply with obligations under the revised <i>AML/CFT Regulations</i> has not yet been verified through compliance monitoring.</li> </ul>

<sup>6</sup> These factors are only required to be set out when the rating is less than Compliant.

7. Correspondent banking	PC	<ul style="list-style-type: none"> <li>No requirement for senior management authorization of correspondent bank accounts.</li> <li>No requirement for both parties to correspondent banking relationships to document their respective AML/CFT responsibilities.</li> </ul>
8. New technologies & non face-to-face business	LC	<ul style="list-style-type: none"> <li>Effectiveness of arrangements to comply with obligations under the revised <i>AML/CFT Regulations</i> has not yet been verified through compliance monitoring.</li> </ul>
9. Third parties and introducers	C	<ul style="list-style-type: none"> <li>The recommendation is fully observed.</li> </ul>
10. Record-keeping	LC	<ul style="list-style-type: none"> <li>Lack of recent compliance monitoring limits ability to assess effectiveness.</li> </ul>
11. Unusual transactions	LC	<ul style="list-style-type: none"> <li>Detailed obligations under revised AML Regulations not fully implemented by some non-banks and cash dealers.</li> </ul>
12. DNFBP–R.5, 6, 8–11	NC	<ul style="list-style-type: none"> <li>No AML/CFT requirements are in place for lawyers and accountants who conduct financial transactions on behalf of customers, or TCSPs.</li> </ul>
13. Suspicious transaction reporting	PC	<ul style="list-style-type: none"> <li>STR reporting does not cover all predicate offences.</li> <li>STR filing on tax matters or on suspected proceeds of other crimes defined under RMI laws are not specifically provided for in the <i>Banking Act</i> or <i>AML/CFT Regulations</i>.</li> <li>The lack of STR reporting from non-banking entities indicates weakness in effectiveness of implementation.</li> </ul>
14. Protection & no tipping-off	LC	<ul style="list-style-type: none"> <li>No explicit provision in section 170 (4) of the <i>Banking Act</i> to prohibit tipping off in the period after a suspicion has been formed and before a STR has been prepared or submitted.</li> </ul>
15. Internal controls, compliance & audit	LC	<ul style="list-style-type: none"> <li>Some NBFIs and cash dealers have not fully implemented the requirements of the revised <i>AML/CFT Regulations</i>.</li> </ul>
16. DNFBP–R.13–15 & 21	NC	<ul style="list-style-type: none"> <li>No STR reporting obligations for DNFBP.</li> </ul>
17. Sanctions	PC	<ul style="list-style-type: none"> <li>Penalties for compliance breaches by non-bank financial institutions and cash dealers are not sufficiently proportionate or dissuasive.</li> <li>No effective use of formal sanctions powers by Banking Commission to date.</li> </ul>
18. Shell banks	C	<ul style="list-style-type: none"> <li>The recommendation is fully observed.</li> </ul>
19. Other forms of reporting	C	<ul style="list-style-type: none"> <li>The recommendation is fully observed.</li> </ul>
20. Other DNFBP & secure transaction techniques	PC	<ul style="list-style-type: none"> <li>No measures have been taken to encourage the use of modern and secure techniques for conducting financial transactions.</li> </ul>
21. Special attention for higher risk	NC	<ul style="list-style-type: none"> <li>There are no regulations in place to require special attention to</li> </ul>

countries		<p>business relations and transactions with high risk countries.</p> <ul style="list-style-type: none"> <li>• There are no regulations in place to require financial institutions to examine and document the background of transactions which have no apparent economic or visible lawful purpose.</li> <li>• There is no specific statute or regulation that allows for issuance or implementation of countermeasures.</li> </ul>
22. Foreign branches & subsidiaries	C	<ul style="list-style-type: none"> <li>• The recommendation is fully observed.</li> </ul>
23. Regulation, supervision and monitoring	PC	<ul style="list-style-type: none"> <li>• A number of entities operating as a non-deposit taking lender, money remittance service provider, or insurance intermediary appear to be covered by the AML/CFT legislative requirements but are not currently supervised for AML/CFT purposes.</li> <li>• Effectiveness is undermined by the lack of onsite AML examinations since 2007, and inadequate information to carry out regular offsite AML compliance monitoring, particularly for non-bank financial institutions and cash dealers.</li> <li>• The Banking Commission has not yet conducted monitoring or site examinations with respect to compliance with the recently introduced requirements of the revised <i>AML/CFT Regulations</i>.</li> <li>• No legislation exists to prevent criminals or their associates from holding or being beneficial owners of a controlling interest in, or being a senior manager or director of a non-bank financial institution or cash dealer.</li> <li>• No registration or licensing requirement is in place for money or value transfer service providers, or other non-bank financial institutions and cash dealers.</li> </ul>
24. DNFBP—regulation, supervision and monitoring	NC	<ul style="list-style-type: none"> <li>• There is no supervision and regulation of DNFBP.</li> </ul>
25. Guidelines & Feedback	NC	<ul style="list-style-type: none"> <li>• There are no formalized processes and procedures to provide adequate and appropriate feedback to financial institutions and cash dealers on STRs filed.</li> <li>• Guidelines issued are outdated.</li> <li>• Feedback is not provided on a regular basis to reporting entities.</li> <li>• Lack of comprehensive guidance to assist subject entities to comply with new AML/CFT regulatory requirements.</li> <li>• Previously issued guidance material has not been updated to ensure it is consistent with the revised <i>AML/CFT Regulations</i>.</li> <li>• No guidance provided on AML/CFT for DNFBP.</li> </ul>
<b>Institutional and other measures</b>		
26. The FIU	PC	<ul style="list-style-type: none"> <li>• Deficiencies in the STR analysis, screening and prioritization process.</li> <li>• No clear legal authority to obtain information from LEAs to</li> </ul>

		<p>assist in the analysis of the STRs.</p> <ul style="list-style-type: none"> <li>• Lack of sector specific STR guidance.</li> <li>• No publicly available FIU annual report, including statistics.</li> <li>• No back up of data is performed.</li> </ul>
27. Law enforcement authorities	PC	<ul style="list-style-type: none"> <li>• Predicate offence investigations are pursued at the expense of ML investigations.</li> <li>• Lack of implementation of available ML investigation powers.</li> </ul>
28. Powers of competent authorities	PC	<ul style="list-style-type: none"> <li>• Certain powers not explicitly provided in legislation.</li> <li>• Effectiveness of police powers has not been tested in relation to ML and FT.</li> </ul>
29. Supervisors	LC	<ul style="list-style-type: none"> <li>• Lack of effectiveness of powers due to inadequate human resources in the Banking Commission.</li> </ul>
30. Resources, integrity, and training	PC	<ul style="list-style-type: none"> <li>• Lack of DFIU dedicated resources and specialized financial intelligence expertise</li> <li>• Implementation is impeded by the lack of financial investigative expertise.</li> <li>• Lack of expertise and dedicated resources to undertake financial investigation/s of ML/FT and proceeds of crime.</li> <li>• Lack of training, awareness and expertise in AML/CFT.</li> </ul>
31. National co-operation	PC	<ul style="list-style-type: none"> <li>• There is a lack of structured approach to AML/CFT coordination.</li> <li>• Policy level coordination mechanisms are not being used to effectively achieve key AML/CFT outcomes.</li> </ul>
32. Statistics	PC	<ul style="list-style-type: none"> <li>• There is no structured approach to collecting and maintaining AML/CFT related statistics.</li> </ul>
33. Legal persons–beneficial owners	NC	<ul style="list-style-type: none"> <li>• Except under the FIBL Act, there are no measures or mechanisms to verify, inquire and determine beneficial ownership.</li> <li>• There are no measures in place to ensure that bearer shares are not misused.</li> </ul>
34. Legal arrangements – beneficial owners	NC	<ul style="list-style-type: none"> <li>• There are no measures in place to prevent unlawful use of legal arrangements.</li> <li>• Lack of timely access to accurate information on beneficial ownership.</li> <li>• No provision allowing access to information on beneficial ownership.</li> </ul>
<b>International Cooperation</b>		
35. Conventions	LC	<ul style="list-style-type: none"> <li>• Deficiencies in <i>Banking Act</i> on the ML offence.</li> </ul>
36. Mutual legal assistance (MLA)	PC	<ul style="list-style-type: none"> <li>• Scope of coverage of the ML offence in the RMI undermines effectiveness of the MLA framework.</li> <li>• The MACMA is restrictive in the sense that it only applies to cases where formal and bilateral agreements or arrangements</li> </ul>

		<p>with a foreign State have been made.</p> <ul style="list-style-type: none"> <li>• The MACMA does not provide for clear timeframes within which MLA requests are to be handled.</li> <li>• There are no clear and efficient processes in place for the execution of MLA requests without undue delay.</li> <li>• No mechanism to determine the best venue for ML prosecutions.</li> <li>• Effectiveness cannot be established.</li> </ul>
37. Dual criminality	LC	<ul style="list-style-type: none"> <li>• Dual criminality limits the ability to render assistance.</li> </ul>
38. MLA on confiscation and freezing	LC	<ul style="list-style-type: none"> <li>• There are no clear and efficient processes to provide a timely response to requests.</li> <li>• No clear provision for property of corresponding value.</li> </ul>
39. Extradition	PC	<ul style="list-style-type: none"> <li>• Doubts exist as to whether RMI nationals can be extradited.</li> <li>• There is no provision authorizing the domestic prosecution of an RMI national who has not been extradited.</li> <li>• No procedures that provide clear timeframes for processing extradition requests.</li> </ul>
40. Other forms of co-operation	LC	<ul style="list-style-type: none"> <li>• The effectiveness and efficiency of the current legal and administrative framework is difficult to determine due to the lack of statistical data across all relevant competent authorities.</li> </ul>
<b>Nine Special Recommendations</b>		
SR.I Implement UN instruments	PC	<ul style="list-style-type: none"> <li>• Effective measures to fully implement UNSCR 1267 and 1373 have not been put into place.</li> <li>• There are no procedures for the designation and delisting of persons or entities within the context of UNSCR 1373.</li> </ul>
SR.II Criminalize terrorist financing	LC	<ul style="list-style-type: none"> <li>• The definition of “attempts” is not fully consistent with the FT.</li> <li>• While offences meet all the essential criteria of SR II, there is as yet no basis to evaluate the effectiveness of the implementation.</li> </ul>
SR.III Freeze and confiscate terrorist assets	PC	<ul style="list-style-type: none"> <li>• The absence of specific procedure and timeframes to demonstrate freezing “without delay” in relation to the requirements of UNSCR 1267.</li> <li>• Total period permissible for freezing funds detailed under CTA is 2 years.</li> <li>• There are no procedures for the designation and delisting of persons or entities within the context of UNSCR 1373.</li> <li>• No effective communication systems or guidelines to subject persons.</li> <li>• No publicly known procedures for delisting and unfreezing.</li> </ul>
SR.IV Suspicious transaction reporting	LC	<ul style="list-style-type: none"> <li>• Unable to confirm effectiveness due to recent implementation of mandatory reporting requirements.</li> </ul>
SR.V International cooperation	PC	<ul style="list-style-type: none"> <li>• No clear timeframes and guidance for the expedient processing of MLA.</li> </ul>

		<ul style="list-style-type: none"> <li>• The MACMA is restrictive in the sense that it only applies to cases where formal and bilateral agreements or arrangements with a foreign State have been made.</li> <li>• Ability to render assistance is limited by dual criminality.</li> <li>• Effectiveness cannot be established.</li> </ul>
SR.VI AML/CFT requirements for money/value transfer services	PC	<ul style="list-style-type: none"> <li>• Lack of effective implementation of the CTA licensing requirements for MVT.</li> <li>• Informal MVT providers are not covered under existing AML/CFT obligations.</li> </ul>
SR.VII Wire transfer rules	LC	<ul style="list-style-type: none"> <li>• The Banking Commissioner's powers to authorize a de-minimis threshold of US\$3,000 are not consistent with SRVII.</li> <li>• Effectiveness of arrangements to comply with wire transfer obligations under the revised <i>AML/CFT Regulations</i> has not yet been verified through compliance monitoring.</li> </ul>
SR.VIII Nonprofit organizations	NC	<ul style="list-style-type: none"> <li>• NPO Sector Review not completed.</li> <li>• No outreach undertaken on FT risks.</li> <li>• Lack of oversight and monitoring of NPOs.</li> <li>• Lack of NPO transparency requirements.</li> <li>• Lack of available sanctions.</li> <li>• Registration requirements lack fit and proper test.</li> <li>• Lack of record keeping requirements.</li> </ul>
<ul style="list-style-type: none"> <li>• SR.IX Cash Border Declaration &amp; Disclosure</li> </ul>	NC	<ul style="list-style-type: none"> <li>• CDA does not define natural and legal persons.</li> <li>• CDA does not clearly cover legal persons.</li> <li>• Inwards RMI Customs declaration does include a definition of 'currency' to include bearer negotiable instruments and precious metals and stones; and warning for failure to declare and/or false declaration.</li> <li>• No outwards currency declaration form available as required in the CDA.</li> <li>• Not clear if the RMI Customs has access to the UNSCR1267 list.</li> <li>• CDA does not provide for data to be retained for use by authorities.</li> <li>• No legal basis to forward information to the DFIU/or for DFIU to access the information.</li> <li>• No legal basis for the DFIU to receive or access cross border information.</li> <li>• No broad nor proportionate sanctions available.</li> <li>• No adequate procedures to safeguard information.</li> <li>• Lack of formalized information sharing arrangements.</li> <li>• No clear implementation of the declaration system.</li> </ul>

**Table 2. Recommended Action Plan to Improve the AML/CFT System**

<b>FATF Recommendations</b>	<b>40+9</b>	<b>Recommended Action (in order of priority within each section)</b>
<b>2. Legal System and Related Institutional Measures</b>		
Criminalization of Money Laundering (R.1, 2, & 32)		<ul style="list-style-type: none"> <li>Amend the <i>Banking Act</i> to (a) remove the reference to “render assistance” in Section 1 (b); and (b) specifically cover “self-laundering”.</li> <li>Include comprehensive offences against each designated category of predicate offences, including by: <ul style="list-style-type: none"> <li>enacting legislation that would criminalize piracy of products, human trafficking, migrant smuggling, insider trading and market manipulation with penalties that would qualify them to be predicate offences to ML; and</li> <li>amending the existing customs and environmental law by providing for penalties that would qualify them to be serious offences and thus be predicate offences to ML.</li> </ul> </li> <li>The authorities should develop a strategy to build expertise and undertake ML investigation and prosecution, with an initial focus on simpler cases of potential ML, proceeds of crime and taxation related violations (see related recommendation under R.27).</li> </ul> <p><b>Recommendation 2</b></p> <ul style="list-style-type: none"> <li>Amend the definition of legal persons to include the full range as defined in the methodology.</li> </ul>
Criminalization of Terrorist Financing (SR.II & R.32)		<ul style="list-style-type: none"> <li>It is recommended that the RMI conduct a FT risk assessment as part of a national AML/CFT assessment, and amend the definition of “attempts” to be consistent with the FT Convention.</li> </ul>
Confiscation, freezing, and seizing of proceeds of crime (R.3 & 32)		<ul style="list-style-type: none"> <li>Amend both the POCA, and <i>Banking Act</i> to ensure that “tainted property” covers instrumentalities intended for use in the commission of any ML, FT or other predicate offences and is the same in both Acts.</li> <li>Ensure that provisional measures and confiscation applies to property of corresponding value.</li> </ul>
Freezing of funds used for terrorist financing (SR.III & R.32)		<ul style="list-style-type: none"> <li>Adopt specific procedure, timeframes and ensure sanctions for non-compliance, through the promulgation of regulations pursuant to the CTA, to enable freezing “without delay” in relation to the requirements of UNSCR 1267.</li> <li>Adopt specific procedures for the designation and delisting of persons or entities within the context of UNSCR 1373.</li> <li>Implement an effective mechanism or communication systems or guidelines to subject persons.</li> <li>Provide for publicly known procedures for delisting and unfreezing.</li> <li>Develop and implement procedures to monitor compliance by the</li> </ul>

	RMI government.
The Financial Intelligence Unit and its functions (R.26, 30 & 32)	<ul style="list-style-type: none"> <li>• Ratify as soon as possible the <i>Banking Act Amendment 2010</i> Bill, including the new section 167, which will address current deficiencies and further improve the operations of the DFIU. The Bill should include a clear provision for the DFIU to access information from other competent authorities, and vice versa.</li> <li>• Review the STR analysis SOP to ensure all relevant information (including UNSCR 1267 and other lists) is considered in the screening, prioritization and analysis process.</li> <li>• Develop and implement sector specific STR guidance and feedback for financial institutions and cash dealers.</li> <li>• Publish a DFIU annual report to include statistics, typologies and trends. A sanitized version of the annual report should be publicly available.</li> <li>• Develop SOP to ensure all FIU data is backed-up on a regular basis and stored in an off-site secure location</li> <li>• Provide a separate budget for the DFIU, and dedicate one full time staff member to DFIU and AML/CFT functions (see recommendation also for FATF Recommendation 23 and 30).</li> <li>• Develop or enhance SOPs to ensure all information requested or received between the DFIU and competent authorities (i.e. CID), or reporting entities, are officially recorded by all competent authorities, whether receiving or requesting, for audit and statistical purposes.</li> </ul>
Law enforcement, prosecution and other competent authorities (R.27, 28, 30 & 32)	<ul style="list-style-type: none"> <li>• Provide additional training to develop sufficient expertise in ML, proceeds of crime and financial investigations for the DFIU, DPS, judicial and prosecutorial agencies.</li> <li>• Develop a plan to build expertise in investigations, with an initial focus on simpler cases of potential ML, proceeds of crime and taxation related violations.</li> <li>• Ensure there are sufficient funds from the national budget to guarantee ongoing access to the Interpol system. At the time of the mutual evaluation the fee had not been paid and there remained one outstanding request for information.</li> </ul>
Cross Border Declaration or disclosure (SR IX)	<ul style="list-style-type: none"> <li>• Amend the CDA to include the declaration of currency and bearer negotiable instrument for the postal system and containerized cargo.</li> <li>• Amend the CDA to explicitly include both natural and legal persons.</li> <li>• Revise the current inward declaration form to include the definition of currency, and sanctions for failure to declare currency and for false declaration.</li> <li>• Implement a departure declaration system to compliment the inwards declaration system in line with the CDA.</li> <li>• Implement as a system which retains the information and</li> </ul>

	<p>identification data in instances where currency declared in excess of US\$10,000.</p> <ul style="list-style-type: none"> <li>• Provide the legal basis for customs to share information with the DFIU, and formalise processes and procedures for the sharing and transferring of information among Customs, the DFIU, Immigration and other relevant agencies in the form of a MOU.</li> <li>• Provide for a range of proportionate and dissuasive sanctions, including for false declaration.</li> <li>• Implement procedures for the proper use and safeguarding of information reported or recorded.</li> <li>• Upgrade the current manual system to a computerized database.</li> </ul>
<b>3. Preventive Measures–Financial Institutions</b>	
Customer due diligence, including enhanced or reduced measures (R.5–8)	<ul style="list-style-type: none"> <li>• <b>Recommendation 5.</b> The RMI authorities should take further steps to ensure all entities meeting the definition of non-bank financial institution or cash dealer are aware of their CDD compliance obligations. The authorities should undertake outreach regarding the new obligations, issue comprehensive guidance on risk based CDD and the detailed obligations under the Regulations, and subsequently obtain off-site compliance monitoring information or conduct on-site reviews to confirm that the full range of the new obligations are fully implemented.</li> <li>• The authorities should ensure that financial institutions and cash dealers have a proper understanding of the need to take reasonable measures to determine the ownership and control structure, and the ultimate natural person(s) who control customers that are legal persons, and have implemented adequate policies and procedures in accordance with section 3C of the revised <i>AML/CFT Regulations</i>.</li> <li>• The definition of “beneficial owner” in the revised <i>AML/CFT Regulations</i> should be amended to be consistent with FATF Recommendations, i.e. “the natural person who ultimately owns or controls the customer and/or the person on whose behalf a transaction is being conducted”.</li> <li>• <b>Recommendation 6.</b> consider signing, ratifying and fully implementing the UN Convention on Corruption, including the obligation to apply FATF Recommendation 6 to domestic PEPs.</li> <li>• <b>Recommendation 7.</b> The revised <i>AML/CFT Regulations</i> (section. 3N) should be amended to require senior management approval before establishing new correspondent relationships and to require both correspondent and respondent institutions to agree and record their respective AML/CFT responsibilities.</li> <li>• <b>Recommendation 8.</b> With respect to the requirements to prevent misuse of new technological developments, the Banking Commission should provide guidance on, and review the implementation of arrangements established for mobile banking facilities and other new technology innovations to ensure the associated AML/CFT risks are mitigated effectively.</li> </ul>

Third parties and introduced business (R.9)	<i>The recommendation is fully observed.</i>
Financial institution secrecy or confidentiality (R.4)	<i>The recommendation is fully observed.</i>
Record keeping and wire transfer rules (R.10 & SR.VII)	<ul style="list-style-type: none"> <li>The RMI authorities should amend section 3M.9 of the revised <i>AML/CFT Regulations</i> to be consistent with SR.VII, reducing the available exemption to US\$1,000, and permitting it to apply to the cross border originator information requirements of section 3M.3 and the verification of originator information requirements of section 3M.1 only. Until the Regulations are amended accordingly, the Banking Commission should not approve a de-minimis wire transfer threshold that does not comply with SR.VII. Current financial institution practice is satisfactory without any exemption which suggests that no such threshold exemption is necessary.</li> </ul>
Monitoring of transactions and relationships (R.11 & 21)	<ul style="list-style-type: none"> <li><b>Recommendation 11:</b> the Banking Commission should address the minor scope and implementation issues associated with the Commission's incomplete coverage of all non bank financial institution and cash dealers as defined under the <i>Banking Act</i>.</li> <li><b>Recommendation 21:</b> The Banking Commissioner should seek to amend the <i>Banking Act</i> or <i>AML/CFT Regulations</i> to meet the requirements of this Recommendation.</li> </ul>
Suspicious transaction reports and other reporting (R.13, 14, 19, 25, & SR.IV)	<p><b>Recommendation 13</b></p> <ul style="list-style-type: none"> <li>The remaining FATF predicate offences, once incorporated into an amended <i>Banking Act</i>, should be reflected in the revised <i>AML/CFT Regulations</i>, and in further guidance to financial institutions and cash dealers.</li> <li>Tax matters and other suspicious transactions related to any criminal act should be clarified in the revised <i>AML/CFT Regulations</i> to remove any doubt or confusion caused by the current wording.</li> <li>Undertake measures to enhance compliance with STR reporting requirements with non bank financial institutions and cash dealers.</li> </ul> <p><b>Recommendation 14</b></p> <ul style="list-style-type: none"> <li>Amend section 170 (4) of the <i>Banking Act</i> to prohibit tipping off in the period after a suspicion has been formed and before a STR has been prepared or submitted.</li> </ul> <p><b>Recommendation 25</b></p> <ul style="list-style-type: none"> <li>The Banking Commission/DFIU should establish internal guidelines and procedures to provide consistent, timely, and appropriate feedback to financial institutions and cash dealers on STR reporting to enhance the effectiveness of the reporting regime.</li> <li>The <i>Banking Act</i> and/or regulations should be amended to include specific provisions that protect the identity or maintain the</li> </ul>

	confidentiality of person(s) reporting STRs to the DFIU.
Internal controls, compliance, audit and foreign branches (R.15 & 22)	<ul style="list-style-type: none"> <li>• The Banking Commission should provide sector specific guidance on AML/CFT internal procedures for non-bank financial institutions (see Recommendation 25) and conduct regular examinations to assess compliance (see Recommendation 23).</li> </ul>
Shell banks (R.18)	<i>The recommendation is fully observed.</i>
The supervisory and oversight system—competent authorities and SROs Role, functions, duties and powers (including sanctions) (R.23, 30, 29, 17, 25, & 32)	<ul style="list-style-type: none"> <li>• <b>Recommendation 29:</b> Conduct onsite examinations and obtain necessary information to carry out AML/CFT supervision.</li> <li>• <b>Recommendation 17:</b> Establish a wider range of sanctions, particularly for the non-bank entities, and consider increasing the maximum level of civil money penalties, having regard for relativity with the maximum penalties provided for similar offences and the breaches of sections 169 and 170, which are set out in s.169 (5) of the Act.</li> <li>• The Banking Commission should, after identifying AML/CFT compliance breaches, set out in writing to the offending institution reasonable but firm deadlines for rectification of compliance breaches, and obtain written responses for the entities detailing actions taken, rather than possibly delaying follow-up of rectification until subsequent onsite examinations.</li> <li>• Non-compliance with required corrective action should then be followed up by formal sanctions as provided for under the <i>Banking Act</i> and Regulations.</li> <li>• <b>Recommendation 23:</b> The RMI authorities should provide in legislation for powers to prevent criminals or their associates from holding or being beneficial owners of a controlling interest in or being a senior manager or director of a non-bank financial institution or cash dealer.</li> <li>• The RMI should consider introducing fit and proper person requirements for all such persons.</li> <li>• To reduce the risk of negative international sentiment being focused on the potential for offshore banking in RMI to be used for ML and FT, the authorities should consider removing all references to offshore banks from the <i>Banking Act</i>. If there is sound justification to permit offshore banking at some future time, the authorities should then establish a robust separate offshore banking legislative framework consistent with international standards.</li> <li>• The Banking Commission should as soon as possible carry out targeted onsite compliance monitoring regarding the effectiveness of arrangements established by subject entities to implement the new detailed obligations set out in the revised <i>AML/CFT Regulations</i>.</li> <li>• The Banking Commission should consider implementing regular collection and off-site monitoring of AML/CFT compliance</li> </ul>

	<p>information, for example through annual reports by each subject entity, and requiring copies of annual internal or external audit reports on AML/CFT compliance and procedures from non-banks. These reports should supplement the compliance information derived from onsite examinations to monitor effectiveness of arrangements for compliance with new requirements. The status of the 2005 advisory A-05 on AML/CFT external audit requirements is unclear in respect of non-bank financial institutions and cash dealers. Any uncertainty regarding the Banking Commissioner's powers to obtain such compliance information and audit reports from non-bank entities should be removed by amendment to the <i>Banking Act</i> and regulations as necessary.</p> <ul style="list-style-type: none"> <li>• Advisory A-05 on AML audit requirements should be updated to confirm its application to banks only, under section 134(11) of the <i>Banking Act</i>; and Advisory A-10(c) which provides a temporary grace period (exemption) for all financial institutions and cash dealers from compliance with the new obligations of the revised <i>AML/CFT Regulations</i> until 22 October 2010 should specifically refer to being issued under the relevant exemption and exception powers (contained in section 8 of the Regulations).</li> <li>• The RMI authorities should consider establishing through legislation a register of financial service providers to ensure the Banking Commission has sufficient information to identify all parties that fall within the definition of financial institutions and cash dealers in RMI. At a minimum, all MVT and money exchange business should be subject to a mandatory registration requirement as provided for in section 121(1) of the CTA. The registration framework should provide effective penalties for any entities carrying on such business that are not registered, and provide grounds for deregistration including for willful failure to comply with AML requirements or upon conviction for certain offences including crimes relating to fraud, dishonesty or ML and FT.</li> <li>• The Banking Commission should also consider establishing working arrangements with the Registrar of Corporations and the local atoll governments that issue business licences to assist the Banking Commission to identify all businesses in RMI that are chartered or licensed as businesses to provide any type of financial service that would be subject to the <i>Banking Act</i> and Regulations.</li> <li>• The Banking Commission should correct identified inadequacies in scope of entities covered and immediately exercise the powers to monitor compliance with and enforce AML/CFT requirements under the <i>Banking Act</i> for certain non-deposit taking lenders (including MIDB), remittance dealers and life insurance intermediaries that are not currently supervised for AML/CFT purposes.</li> <li>• The Banking Commission should consider whether additional</li> </ul>
--	---

	<p>legislative and supervisory arrangements will be required to effectively monitor and supervise on a consolidated basis the risks arising from the establishment of any foreign subsidiaries, branches or offices of RMI financial institutions.</p> <ul style="list-style-type: none"> <li>• The Banking Commission should immediately revise the AML examination procedures manual and all offsite supervision procedures and instructions for staff to incorporate the risk based approach to CDD and the broader range of compliance requirements set out in the revised <i>AML/CFT Regulations</i> and recent amendment to the <i>Banking Act</i>. The Banking Commissioner should also review banks' conditions of licence in respect of AML/CFT matters to ensure the obligations are comprehensive and consistent with the revised <i>AML/CFT Regulations</i>.</li> <li>• The RMI authorities should immediately pass the amendments to the <i>Banking Act</i> sections 166 and 167 as per the draft presented to the evaluation team (see also related recommendation under R.26).</li> <li>• The RMI authorities should prepare a national AML/CFT risk assessment using the APG national risk assessment framework or some other tool to identify the level and nature of AML/CFT risks and associated criminality in RMI, develop future risk indicators and contribute to the development of a comprehensive national strategy to effectively combat ML and FT.</li> <li>• <b>Recommendation 25:</b> The Banking Commission should issue detailed guidelines to assist financial institutions and cash dealers to effectively comply with the new requirements and risk based approach to CDD established under the revised <i>AML/CFT Regulations</i>. That should include criteria to be adopted in considering applications for the various approvals and exemption powers that the Banking Commissioner can exercise under the Regulations. Technical assistance from regional agencies may be appropriate to implement these recommendations as soon as possible.</li> <li>• <b>Recommendation 30: Integrity.</b> The Banking Commission should consider establishing a code of conduct for staff of the Banking Commission and FIU consistent with international best practice to enhance transparency regarding the expectations on staff regarding honesty, integrity and professionalism.</li> <li>• <b>Recommendation 30: Resources.</b> At least one additional technical staff position should be established as soon as possible in the Banking Commission to provide sufficient resources to effectively conduct on and offsite AML supervision for all cash dealers and financial institutions and ensure compliance with the more detailed requirements of revised <i>AML/CFT Regulations</i>. The Banking Commissioner should draw up a work program to schedule AML/CFT onsite compliance examinations, and ensure all entities are examined at least once every four (4) years with more frequent examinations scheduled according to the risk the</li> </ul>
--	---

	entity poses, particularly for banks. At least two (2) onsite AML/CFT examinations should be carried out every year to maintain supervisors' skills and experience and spread the workload evenly.
Money value transfer services (SR.VI)	<ul style="list-style-type: none"> <li>• Implement the Register for MVT service providers.</li> <li>• Identify informal MVT providers and subject them to existing AML/CFT obligations.</li> </ul>
<b>4.Preventive Measures–Nonfinancial Businesses and Professions</b>	
Customer due diligence and record-keeping (R.12)	<ul style="list-style-type: none"> <li>• The authorities should introduce legislative obligations on DNFBP to comply with the requirements of Recommendation 12 but implementation should be risk based.</li> </ul>
Suspicious transaction reporting (R.16)	<ul style="list-style-type: none"> <li>• The authorities should introduce legislative obligations on DNFBP to comply with the requirements of Recommendation 16 but implementation should be risk based.</li> </ul>
Regulation, supervision, monitoring, and sanctions (R.17, 24, & 25)	<ul style="list-style-type: none"> <li>• The RMI should introduce an appropriate legal and supervisory framework for DNFBP with a prioritised and phased implementation based on a risk assessment, with a focus on enhancing supervision of company formation service providers based offshore, to monitor compliance with CDD, STR reporting and other AML/CFT measures recommended under R.12 and R.16.</li> </ul>
Other designated non-financial businesses and professions (R.20)	<ul style="list-style-type: none"> <li>• The RMI should encourage the introduction of modern and secure techniques for conducting transactions.</li> </ul>
<b>5. Legal Persons and Arrangements &amp; Non Profit Organizations</b>	
Legal Persons–Access to beneficial ownership and control information (R.33)	<ul style="list-style-type: none"> <li>• It is recommended that the OAG be provided with additional human resources and appropriate training to perform their functions.</li> <li>• Make disclosure of beneficial ownership a mandatory requirement for both resident and non-resident corporations.</li> <li>• Prevent the misuse of bearer shares and include appropriate sanctions in case of none compliance.</li> <li>• Ensure accurate and timely information on beneficial ownership is available to law enforcement authorities.</li> </ul>
Legal Arrangements–Access to beneficial ownership and control information (R.34)	<ul style="list-style-type: none"> <li>• RMI may consider repealing the TCA or amend it and incorporate the deficiencies under c. 34.1 and 34.2.</li> </ul>
Nonprofit organizations (SR.VIII)	<ul style="list-style-type: none"> <li>• The competent authorities should review the current draft NGO law and other laws governing the NPO sector, and incorporate, as necessary, the requirements of the FATF SR.VIII in either the proposed NGO law or existing laws, in consultation with the NPO Sector.</li> <li>• The Registrar of Incorporation should maintain a separate</li> </ul>

	<p>database of NPOs registered to enhance transparency, improve supervision and facilitate information dissemination of the sector.</p> <ul style="list-style-type: none"> <li>• The competent authorities should develop and implement a program to further enhance the transparency and accountability of the NPO sector, including assessing FT risk, and raising awareness of potential vulnerabilities in the sector, both FT and other criminal activities.</li> </ul>
<b>6. National and International Cooperation</b>	
National cooperation and coordination (R.31 & 32)	<ul style="list-style-type: none"> <li>• There should, however, be more formal recording of actions arising from both policy and operational meetings.</li> <li>• The Committee should oversee the conduct of a national AML/CFT risk assessment and develop a strategy to implement the recommendations contained in this mutual evaluation report.</li> </ul>
The Conventions and UN Special Resolutions (R.35 & SR.I)	<ul style="list-style-type: none"> <li>• Deficiencies in the existing law based on the Conventions should be addressed.</li> <li>• The noted deficiencies in the implementation of UNSCR 1267 and 1373 should be addressed particularly the freezing and designation mechanism.</li> </ul>
Mutual Legal Assistance (R.36, 37, 38, SR.V & 32)	<p>RMI should consider reviewing and updating the provisions of the MACMA and its partner legislations, e.g. the POCA, and provide regulations that:</p> <p><b>Recommendation 36</b></p> <ul style="list-style-type: none"> <li>• Comprehensively criminalise all categories of designated offences to ensure MLA provisions under MACMA can be applied to the widest range of proceeds of crime.</li> <li>• Indicate reasonable time periods within which requests for legal assistance can be acted upon.</li> <li>• Amend the MACMA so the application of MLA is not conditional upon formal and bilateral agreements or arrangements with a foreign State have been made.</li> <li>• Develop clear and efficient procedures for the execution of MLA requests.</li> <li>• Develop procedures to provide mechanisms to provide for the best venue for ML prosecutions.</li> </ul> <p><b>Recommendation 37</b></p> <ul style="list-style-type: none"> <li>• Amend the MACMA to allow for the delivery of mutual legal assistance on less intrusive and non compulsory measures.</li> </ul> <p><b>Recommendation 38</b></p> <ul style="list-style-type: none"> <li>• Include a provision in the MACMA for equivalent value seizure and confiscation of assets.</li> <li>• Establish a mechanism for feedbacks and follow-ups.</li> </ul> <p><b>SR V</b></p> <ul style="list-style-type: none"> <li>• Indicate reasonable time periods within which requests for legal</li> </ul>

	assistance can be acted upon.
Extradition (R. 39, 37, SR.V & R.32)	<ul style="list-style-type: none"> <li>• RMI should enhance the offence of ML to ensure that extradition is available in relation to laundering from the widest range of predicate offences.</li> <li>• RMI should consider revising and updating its extradition law to include provisions for clear timeframes and processes that would enable a timely response to any extradition request, and make clear whether RMI nationals may be extradited, and if not, provide for domestic prosecution lieu of extradition.</li> </ul>
Other Forms of Cooperation (R. 40, SR.V & R.32)	<ul style="list-style-type: none"> <li>• The RMI should explore options to enhance its framework for the exchange of information on non-resident corporations.</li> </ul>
<b>7. Other Issues</b>	
Other relevant AML/CFT measures or issues	<ul style="list-style-type: none"> <li>• International technical advice would be more effective if line agencies are actively involved in the drafting of laws, regulations, other enforceable means or guidelines.</li> </ul>

## **Annex 1. Authorities' Response to the Assessment**



### **Republic of the Marshall Islands Banking Commission**

P.O. Box 1408 ~ Majuro ~ Marshall Islands ~ 96960  
Phone No. (692) 625-6310 ~ Fax No. (692) 625-6309 ~ Email Address: bankcomm@ntamar.net

Response by the Republic of the Marshall Islands  
14<sup>th</sup> Annual APG Meeting  
Kochi, India

Delivered by Ann Marie S. Muller, Banking Commissioner

### **INTRODUCTION**

Co-Chairs, APG Secretariat, Distinguished Delegates, ladies & gentlemen....Yokwe

At the outset, let me first of all take this opportunity to offer the Republic of the Marshall Islands' deepest appreciation and 'kommol tata' to the Government of India for the warm hospitality and assistance for this conference. I also wish to offer the RMI's gratitude to the APG Secretariat for all their hard work in the arrangements for this meeting.

Secondly, I wish to thank the APG Evaluation Team –

- Mr. Lindsay Chan of the APG Secretariat
- Mr. Arnold Frane of the Anti-Money Laundering Council Secretariat of the Philippines
- Mr. Peter Dench of the Reserve Bank of New Zealand
- Guangand Semdiu Decherong of the Republic of Palau Financial Institution Commission
- Gai Lambourne of Australian Transaction Reports & Analysis Centre

for visiting our humble shores and for the comprehensive report on the Evaluation of the Marshall Islands that has just been presented to us this afternoon.

Allow me to introduce the other members of the Marshall Islands Delegation:

- Mr. Laurence Edwards – Assistant Attorney General
- Mr. James Myazoe & Ms. Meredith Kirby, Deputy Registrars

The draft Mutual Evaluation Report (MER) that is before the Plenary has been extensively discussed between the Evaluation Team and the Republic of the Marshall Islands, and the RMI looks forward to addressing the recommendations proposed by the Evaluation Team as a basis for formulating an Action Plan towards compliance with 40 + 9 FATF Recommendations.

### **GENERAL COMMENTS**

The Republic of the Marshall Islands became a member of the APG in June 2002 and undertook the commitments as a member of the Asia Pacific Group and as a member of the international community in the global effort to eradicate money laundering and the financing of terrorism. The RMI is mindful of its international obligations and continues to work towards enhancing its AML/CFT framework towards compliance to the international standards.

Despite being a Small Island Developing State, constrained with limited resources, both in capacity and capability, as noted in the draft MER, the RMI has committed substantial resources towards its AML/CFT framework. In addition, we will be meeting with the Donors and Providers in the margins of this annual conference for technical assistance to further strengthen and implement our AML/CFT system. Despite our constraints, the Republic of the Marshall Islands remains fully committed and will continue to support the work of the APG in the global fight against money laundering and the financing of terrorism.

On this note, I wish to update the Plenary on some recent developments which are not incorporated in the draft MER.

On March 18, 2011, the Marshall Islands Nitijela (Parliament) enacted P.L.2011-51 - Proceeds of Crime (Amendment) Act, 2011. The Proceeds of Crime Act Amendment addresses the shortcomings cited by the Evaluation Team. Additionally, the Marshall Islands Cabinet has approved two other key legislative amendments – namely the Banking Amendment Bill and the Mutual Legal Assistance Bill, which are currently pending before the Nitijela.

The Attorney General's office is currently pursuing 7 fraud investigations as part of a wider probe into suspected malfeasance by private and government actors. In response to this ongoing investigation, the Auditor General's office has established a hotline for the public to report suspected incidents of misconduct.

And lastly, on April 21, 2011, the Marshall Islands Cabinet thru C.M. 046(2011) approved for the accession of the RMI to the UN Convention Against Corruption (UNCAC), which is also now pending before the Nitijela.

### **CONCLUSION**

In conclusion, RMI once again reaffirms its commitment as a member of the Asia Pacific Group on Money Laundering. I take this opportunity to thank the donors who are present at this meeting for the assistance provided over the years and look forward to our meaningful discussion this week.

The RMI plans on working closely with the APG Secretariat in the upcoming months in the development of a post-MER Implementation Action Plan, including attendance at the upcoming workshop in Sydney, Australia, and looks forward to reporting back to the Plenary over the next two years.

Kommol tata.

**Annex 2. Details of All Bodies Met During the On-Site Visit**

***Public Sector:***

1. Attorney General
2. Banking Commissioner/Head of Domestic Financial Intelligence Unit (DFIU)
3. Chief of Police
4. Secretary of Foreign Affairs
5. Deputy Registrars – non-resident entities
6. Banking Commission
7. Division of Customs, Revenue, Taxation, & Treasury
8. Domestic Financial Intelligence Unit
9. Department of Public Safety
10. Ministry of Foreign Affairs
11. Office of the Attorney General
12. Registrar of Corporations- Office of the Attorney General (Resident Registrar)
13. Registrar of Corporations (Non-Resident Registrar)

***Private Sector/Non-Government***

14. Two commercial banks
15. Non-bank financial institutions
16. International remittance company
17. Insurance company
18. Accountants and lawyers
19. MICNGOS
20. Jewellery and handicraft stores
21. Land ownership expert

### **Annex 3. List of All Laws, Regulations, and Other Material Received**

#### **Key legislation provided:**

1. Administration Procedures Act
2. Banking Act
3. Business Corporations Act
4. Compact of Free Associations
5. Counter Terrorism Act
6. Criminal Code
7. Criminal Procedures Act
8. Ethics in Government Act
9. Evidence Act
10. Exchange of Information Act
11. Extradition Act
12. Foreign Evidence Act
13. Foreign Investment Business License Act
14. Gaming & Recreation Prohibition Act
15. Import Duties and Licenses Act
16. Legal Profession Act
17. Licensing Act
18. Limited Liability Companies Act
19. Limited Partnerships Act
20. Maritime Administration Act
21. Non-Profit Corporations Act
22. Notaries Public Act
23. Other Forms of Associations Acts
24. Parole Board Act
25. PL 2009-20 - Banking Amendment Act
26. PL 2009-29 - Currency Declaration Act
27. Proceeds of Crimes Act
28. Prostitution Act
29. Public Safety Act
30. Revised Partnership Act
31. Tax Information System Act
32. Treason and Sedition Act
33. Trust Act
34. Trust Companies Act

#### **Key regulations provided:**

1. Revised Anti-Money Laundering Regulations 2002, as issued in May 2010
2. Advisory A-05 – Notification of requirement for annual audit for AML/CFT compliance
3. Advisory A-10 (a) – Notification of the requirement for STRs in relation to FT
4. Advisory A-10 (c) issued by the Banking Commission on 23 September 2010, on the revised *AML/CFT Regulations* that were passed in May 2010.

**Annex 4. Copies of Key Laws, Regulations, and Other Measures****NITIJELA OF THE REPUBLIC OF THE MARSHALL ISLANDS****30th CONSTITUTIONAL REGULAR SESSION, 2009****BILL NO.: 38**P.L. 2009 - 20**AN ACT**

to amend Section 167 of the Banking Act, in order to enable the Banking Commissioner to report to the relevant authorities, transactions that may involve “financing of terrorism”, (in addition to transactions involving proceeds of crimes) and for related matters; to amend Section 170 of the Banking Act to require financial institutions to report suspicious transactions related to terrorist financing.

**ENACTED BY THE NITIJELA OF THE REPUBLIC OF THE MARSHALL ISLANDS:****Section 1. Short Title.**

This Act may be cited as the Banking (Amendment) Act, 2009.

**Section 2. Amendments.**

(1) Section 167 of the Banking Act is hereby amended to read as follows:

**§167. Commissioner’s authority in prohibiting money laundering activity**

(1) The Commissioner:

- (a) shall receive, analyze, and disseminate reports of transactions issued by financial institutions or cash dealers pursuant to Section 170 and Section 170A of this Act;
- (b) shall send any such report to the appropriate law enforcement authorities, if there are reasonable grounds to suspect that the transaction is suspicious;
- (c) may enter the premises of any financial institution or cash dealer during ordinary business hours to inspect any record and ask any question relating to such record, make notes and take copies of the whole or any part of the record;

BILL NO.:38

P.L. 2009-20

- 1 (d) shall send to the appropriate law enforcement authorities, any information derived  
2 from an inspection carried out pursuant to Subsection (1) (c) of this Section, if it  
3 gives the Commissioner reasonable grounds to suspect that a transaction involves  
4 money laundering, proceeds of a crime, and or the financing of terrorism;  
5 (e) may instruct any financial institution or cash dealer to take such steps as may be  
6 appropriate to facilitate any investigation anticipated by the Commissioner;  
7 (f) may compile statistics and records, disseminate information within the Republic  
8 of the Marshall Islands or elsewhere, make recommendations arising out of any  
9 information received; issue guidelines to financial institutions and advise the  
10 appropriate officials;  
11 (g) shall create training requirements and provide such training for any financial  
12 institution with respect to transaction record-keeping and reporting obligations  
13 provided for in this Act;  
14 (h) may consult with any relevant person, institution or organization for the purpose  
15 of exercising its powers or duties under Subsections (1) (e), (f), (g) or (1) of this  
16 Section;  
17 (i) shall have the authority to request additional information from financial  
18 institutions and cash dealers where the Commissioner has reasonable grounds to  
19 believe that such information is essential in discovering money laundering activity,  
20 proceeds of crime, and or the financing of terrorism;

**Annex 4. Copies of Key Laws, Regulations, and Other Measures**

BILL NO.:38

P.L. 2009 - 20

- 1 (j) shall have the authority and ability to exchange information between international  
 2 administrative authorities;
- 3 (k) shall have the authority and ability to facilitate and assist international  
 4 administrative authorities in conducting proceeds of crime, money laundering, and or  
 5 the financing of terrorism investigations;
- 6 (l) shall have the authority and ability to apply for a warrant to enter any premises  
 7 belonging to or in the possession or control of a financial institution, cash dealer or  
 8 any officer or employee thereof, and to search the premises and remove any  
 9 documents, materials, or other things therein for the purposes of preventing money  
 10 laundering activity, the financing of terrorism, or tracing the proceeds of crime, as so  
 11 ordered by the High Court and specified in the warrant other than as authorized in  
 12 Subsection (c) and (i) above;
- 13 (m) shall have the authority and ability to obtain information under this Section  
 14 notwithstanding any secrecy or other restrictions on disclosure of information  
 15 imposed by this Act; and
- 16 (n) shall conduct, in association with law enforcement authorities, investigations  
 17 into the proceeds of crime, money laundering, and or the financing of terrorism,  
 18 only where the Commissioner has reasonable grounds to suspect the proceeds of  
 19 crime, money laundering activity, and or the financing of terrorism, is occurring.
- 20 (2) Section 170 of the Banking Act is hereby amended by inserting the following after Section 170(4)

BILL NO.:38

P.L. 2009 - 20**§170A Reporting of suspicious transactions and activities related to terrorist financing**

- (1) Financial institutions and cash dealers must report any transaction, attempted transaction or other activity where they suspect or have reasonable grounds to suspect that the transaction, attempted transaction or other activity may be related to terrorism, terrorist acts, a terrorist organization, an individual terrorist, terrorist property or financing of terrorism.
- (2) All suspicious transactions, attempted transactions and other activities that may be related to terrorism, terrorist acts, a terrorist organization, an individual terrorist, terrorist property or financing of terrorism must be reported regardless of the amount involved in the transaction, attempted transaction or activity.
- (3) Such suspicion must be reported in writing to the Commissioner as soon as reasonably practicable and, in any event, within three days of the forming of such suspicion.
- (4) A financial institution or cash dealer, its employees, officers or directors who willfully violates the requirements of this section commits an offence punishable by a fine of not more than \$2,000,000 or imprisonment for not more than twenty (20) years, or both.
- (5) Where a person is employed by a financial institution or cash dealer and his or her employer has an established procedure for the reporting of suspicious, transactions, attempted transactions, or other activities, it is a defense for him to prove that he reported his suspicion in accordance with that procedure.
- (6) For the purposes of this section the “financing of terrorism” shall have the same meaning as “financing of terrorism” in §120 Title 15 –Anti-Terrorism Laws 2002.

BILL NO.:38

P.L. 2009-201 Section 3. **Effective Date.**

2 This Act shall take effect on the date of certification in accordance with the Constitution  
 3 of the Republic of the Marshall Islands and Rules of Procedures of the Nitijela.

4

5 **CERTIFICATE**6 **I hereby certify:**

7

8 (1) That Nitijela Bill No: 38 was passed by the Nitijela of the Republic of the Marshall  
 9 Islands on the 13<sup>th</sup> day of May, 2009; and

10 (2) That I am satisfied that Nitijela Bill No.: 38 was passed in accordance with the relevant  
 11 provisions of the Constitution of the Republic of the Marshall Islands and the Rules  
 12 of Procedures of the Nitijela.

13

14 I hereby place my signature before the Clerk this 5<sup>th</sup> day of June, 2009.

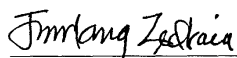
15

16

**Attest:**

17

18



19

**Hon. Jurelang Zedkaia**

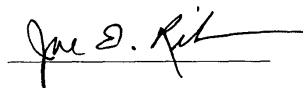
20

Speaker

21

Nitijela of the Marshall Islands

22

**Joe E. Riklon**

Clerk

Nitijela of the Marshall Islands

## THE BANKING ACT

*(note: the following contains part xiii –Money Laundering - of the Banking Act. Other parts of the Banking Act have not been included)*

### **PART XIII - MONEY LAUNDERING**

- §166. Offenses and Penalties
- §167. Authority of the Commissioner
- §168. Verification of customer Id.
- §169. Requirement to maintain Records
- §170. Report Suspicious Transactions
- §171. Seizure of suspicious currency
- §172. Application for Confiscation Order
- §173. Notice of Application
- §174. Confiscation Order upon Conviction
- §175. Effect of Order
- §176. Payment instead of Confiscation
- §177. Procedure for fines
- §178. Suspicious transaction - Immunity
- §179. Good faith - Immunity
- §180. Currency Transaction Reports
- §181. Assessment of Civil penalties
- §182. Effective Date

---

### **PART XIII – ANTI – MONEY LAUNDERING OFFENSES**

#### **§166. Money laundering offenses and penalties.**

#### **PART XIII – ANTI – MONEY LAUNDERING OFFENSES**

#### **§166. Money laundering offenses and penalties.**

- (1) A person commits the offense of money laundering if the person:
  - (a) acquires, possesses or uses property, knowing or having reason to believe that the property is the proceeds of crime;
  - (b) knowing or having reason to believe that such property is the proceeds of crime, renders Assistance to another person for:
    - (i) the conversion or transfer of property, with the aim of concealing or disguising the illicit origin of that property, or of aiding any person involved in the commission of the offense to evade the legal consequences thereof; and
    - (ii) concealing or disguising the true nature, origin, location, disposition, movement or ownership of the property.
- (2) Where a person is convicted of any of the offenses specified in Subsection (1), in the case of a natural person, such person shall be liable to imprisonment for a term of imprisonment not exceeding twenty (20) years or a fine not exceeding \$2,000,000, or both, and in the case of a body corporate five (5) times such a fine or double the amount of money involved in the offense scheme, which ever is greater.

#### **§167. Commissioner's authority in prohibiting money laundering activity.**

- (1) The Commissioner:
  - (a) shall receive reports of transactions issued by financial institutions or cash dealers pursuant to Section 170 of this Act;
  - (b) shall send any such report to the appropriate law enforcement authorities, if there are reasonable grounds to suspect that the transaction is suspicious;
  - (c) may enter the premises of any financial institution or cash dealer during ordinary business hours to inspect any record and ask any question relating to such record, make notes and take copies of the whole or any part of the record;

- (d) shall send to the appropriate law enforcement authorities, any information derived from an inspection carried out pursuant to Subsection (1) (c) of this Section, if it gives the Commissioner reasonable grounds to suspect that a transaction involves proceeds of a crime;
- (e) may instruct any financial institution or cash dealer to take such steps as may be appropriate to facilitate any investigation anticipated by the Commissioner;
- (f) may compile statistics and records, disseminate information within the Republic of the Marshall Islands or elsewhere, make recommendations arising out of any information received; issue guidelines to financial institutions and advise the appropriate officials;
- (g) shall create training requirements and provide such training for any financial institution with respect to transaction record-keeping and reporting obligations provided for in this Act;
- (h) may consult with any relevant person, institution or organization for the purpose of exercising its powers or duties under Subsections (1) (e), (f), (g) or (1) of this Section;
- (i) shall have the authority to request additional information from financial institutions and cash dealers where the Commissioner has reasonable ground to believe that such information is essential in discovering money laundering activity;
- (j) shall have the authority and ability to exchange information between international administrative authorities;
- (k) shall have the authority and ability to facilitate and assist international administrative authorities in conducting money laundering investigations;
- (l) shall have the authority and ability to apply for a warrant to enter any premises belonging to or in the possession or control of a financial institution, cash dealer or any officer or employee thereof, and to search the premises and remove any documents, materials, or other things therein for the purposes of preventing money laundering activity, as so ordered by the High Court and specified in the warrant other than as authorized in Subsection (c) and (i) above;
- (m) shall have the authority and ability to obtain information under this Section notwithstanding any secrecy or other restrictions on disclosure of information imposed by this Act; and
- (n) shall conduct, in association with law enforcement authorities, investigations into money laundering only where the Commissioner has reasonable grounds to suspect money laundering activity is occurring.

**§168. Financial institutions and cash dealers to verify customers identity.**

- (1) A financial institution or cash dealer shall maintain accounts in the name of the account holder. They shall not open or keep anonymous accounts or accounts which are in fictitious or incorrect names.
- (2) A financial institution or cash dealer shall record and verify the identity, representative capacity, domicile, legal capacity, occupation or business purpose of persons, as well as other identifying information on those persons, whether they be occasional or usual clients, through the use of documents providing convincing evidence of their legal existence and the powers of their legal representative, or any other official or private documents, especially when opening new accounts or passbooks, entering into fiduciary transactions, renting of safe deposit boxes, or performing cash transactions over an amount pursuant to the requirement outlined in paragraph 1 of Section 170 (1) of the Act.
- (3) If it appears to a financial institution or cash dealer that an applicant requesting it to enter into any transaction, whether or not in the course of a continuing business relationship, is acting on behalf of another person, the institution or cash dealer shall take reasonable measure to establish the true identity of any person on whose behalf or for whose ultimate benefit the applicant may be acting in the proposed transaction, whether as trustee, nominee, agent or otherwise.
- (4) Nothing in this Section shall require the production of any evidence of identity where:
  - (a) the applicant is itself a financial institution or a cash dealer to which this Act applies; or
  - (b) there is a transaction or a series of transactions taking place in which the applicant has already produced satisfactory evidence of identity. (subsection (2) and paragraph (4) (b) amended by P.L. 2002-59)

**§169. Financial institutions and cash dealers to establish and maintain customer records.**

- (1) Every financial institution or cash dealer shall retain records for all transactions. These records shall be kept in a readily recoverable form.

- (2) Financial institutions and cash dealers shall maintain records on customer identification, account files and business correspondence for six (6) years after the account has been closed, and all records necessary to reconstruct financial transactions for six (6) years after the conclusion of the transactions.
- (3) Records regarding financial transactions shall contain particulars sufficient to identify the following:
- (a) name, address and occupation (or where appropriate business or principal activity) of each person;
  - (i) conducting the transaction; or
  - (ii) if known, on whose behalf the transaction is being conducted as well as the method used by the financial institution or cash dealer to verify the identity of each such person;
  - (b) nature and date of the transaction;
  - (c) type and amount of currency involved;
  - (d) the type and identifying number of any account with the financial institution or cash dealer involved in the transaction;
  - (e) if the transaction involves a negotiable instrument other than currency, the name of the drawer of the instrument, the name of the institution on which it was drawn, the name of the payee (if any), the amount and date of the instrument, the number (if any) of the instrument and details of any endorsements appearing on the instrument;
  - (f) the name and address of the financial institution or cash dealer, and of the officer, employee or agent of the financial institution or cash dealer who prepared the report;
  - (g) multiple transaction which, altogether, exceed ten thousand dollars, shall be treated as single transaction if they are undertaken by or on behalf of any one person during any twenty-four hour period. In such a case, when a financial institution or cash dealer, its employees, officers or agents have knowledge of these transactions, they shall record these transactions.
- (4) Record required under Subsection (1) shall be kept by the financial institution for a period of at least six (6) years from the date the relevant business or transaction was completed.
- (5) A financial institution or cash dealer, its employees, officers or directors, wilfully violating the requirement of Section 169 or 170 commits an offense punishable by a fine of not more than \$2,000,000 or imprisonment for not more than twenty (20) years, or both. (P.L. 2002-59)

**§170. Financial institutions and cash dealers to report suspicious transactions.**

- (1) Financial institutions and cash dealers shall, within 3 days of the transaction, report to the Commissioner all suspicious transactions, including but not limited to those which are ten thousand dollars (\$10,000) or more or multiple transactions which, altogether, exceed ten thousand dollars (\$10,000) if they are undertaken by or on behalf of any one person during any twenty-four hour period or, complex or unusual transactions, whether completed or not, and all unusual patterns of transactions, and otherwise significant but periodic transactions, which have no apparent economic or lawful purpose. The Commissioner may provide additional information or criteria to be used in identifying suspicious transactions under this subsection.
- (2) A financial institution or cash dealer which has reported a suspicious transaction in accordance with this Section shall, if requested to do so by the Commissioner or Attorney-General, give such further information as it has in relation to the transaction.
- (3) The Commissioner, Attorney-General, financial institutions and cash dealers shall maintain reports required by this Section for a period of fifteen (15) years.
- (4) Financial institutions and cash dealers, its employees, officers or directors, shall not notify any person or entity other than the Commissioner or Attorney-General, a court of competent jurisdiction upon process issued, or other person as may be authorized by law, of the information, record, or report that has been prepared, or otherwise referred or furnished to the Commissioner, Attorney-General or court of competent jurisdiction, or other lawfully authorized person. Any person or financial institution or cash dealer who improperly discloses such information commits an offense, punishable by a fine of not more than \$2,000,000.00 or imprisonment for not more than 20 years, or both.

**§171. Seizure and detention of suspicious imports or exports of currency.**

- (1) The Commissioner or Attorney-General may seize and, in accordance with this Section detain, any currency which is being imported into or exported from the Republic of the Marshall Islands, if:
  - (a) he or she has reasonable grounds for suspecting that it is:
    - (i) property derived from a serious offense; or
    - (ii) intended by any person for use in the commission of a serious offense.
- (2) Currency detained under Subsection (1) of this Section shall not be detained for more than twenty-four (24) hours after seizure, unless a judge orders its continued detention for a period not exceeding three (3) months from the date of seizure, upon being satisfied that:
  - (a) there are reasonable grounds for the suspicion referred to in Subsection (1) (a) of this Section; and (b) its continued detention is justified while:
    - (i) its origin or derivation is further investigated; or
    - (ii) consideration is given to the institution in the Republic of the Marshall Islands or elsewhere of criminal proceedings against any person for an offense with which the currency is connected.
- (3) A judge may subsequently order continued detention of the currency if satisfied of the matters mentioned in Subsection (2) of this Section, but the total period of detention shall not exceed two (2) years from the date of the order made under that Subsection.
- (4) Subject to Subsection (5) of this Section, currency detained under this Section may be released in whole or in part to the person on whose behalf it was imported or exported:
  - (a) by order of a judge that its continued detention is no longer justified, upon application by or on behalf of that person and after considering any views of the Attorney- General to the contrary; or (b) by the Commissioner and Attorney-General, if satisfied that its continued detention is no longer justified.
- (5) No currency detained under this Section shall be released where:
  - (a) an application is made under Section 172 of this Act for the purpose of:
    - (i) the confiscation of the whole or any part of the currency; or
    - (ii) its restraint pending determination of its liability to confiscation; or
  - (b) proceedings are instituted in the Republic of the Marshall Islands or elsewhere against any person for an offense with which the currency is connected, unless and until the proceedings relating to the relevant application or the proceedings for the offense have been concluded.

**§172. Application for confiscation order.**

- (1) Where a person is convicted of a serious offense, the Commissioner or Attorney-General may, not later than six (6) months after the conviction, apply to the High Court for the following order:
  - (a) a confiscation order against property that is tainted property in respect of the offense.
- (2) An application under Subsection (1) may be made in respect of one or more than one offense.
- (3) Where an application under this Section is finally determined, no further application for a confiscation order may be made in respect of the offense for which the person was convicted without the leave of the High Court. The High Court shall not give such leave unless it is satisfied that:
  - (a) the property to which the new application relates was identified after the previous application was determined;
  - (b) necessary evidence became available after the previous application was determined; or
  - (c) it is in the interest of justice that the new application be made.

**§173. Notice of application.**

- (1) Where the Commissioner or Attorney-General applies for a confiscation order against property in respect of the person's conviction of a serious offense:
  - (a) the Commissioner or Attorney-General must give no less than fourteen (14) days written notice of the application to the person and to any other person who the Commissioner or Attorney-General has reason to believe may have an interest in the property;
  - (b) the person and any other person who claims an interest in the property may appear and adduce evidence at the hearing of the application; and
  - (c) the High Court may, at any time before the final determination of the application, direct the Commissioner or Attorney-General to:

- (i) give notice of the application to any person who, in the opinion of the High Court, appears to have an interest in the property;
- (ii) publish in a newspaper published and circulating in the Marshall Islands, a notice of the application.

**174. Confiscation order on conviction.**

- (1) Where upon application by the Commissioner or Attorney-General, the High Court is satisfied that property is tainted property in respect of a serious offense of which a person has been convicted, or a person charged who dies or absconds, the High Court may order that specified property be confiscated.
- (2) In determining whether property is tainted property the High Court may infer, in the absence of evidence to the contrary:
  - (a) that the property was used in or in connection with the commission of the offense if it was in the person's possession at the time of, or immediately after the commission of the offense for which the person was convicted; and
  - (b) that the property was derived, obtained or realized as a result of the commission of the offense if it was acquired by the person before, during or within a reasonable time after the period of the commission of the offense of which the person was convicted, and the High Court is satisfied that the income of that person from sources unrelated to criminal activity of that person cannot reasonably account for the acquisition of that property.
- (3) Where the High Court orders that property, other than money, be confiscated, the High Court shall specify in the order the amount that it considers to be the value of the property at the time when the order is made.
- (4) In considering whether a confiscation order should be made under Subsection (1) of this Section, the High Court shall have regard to:
  - (a) the rights and interests, if any, of third party owners of the property, provided the third party establishes no unlawful involvement or benefit from the transaction in which the person convicted was involved;
  - (b) the gravity of the offense concerned;
  - (c) any hardship that may reasonably be expected to be caused to any victim or third party by the operation of the order, provided the victim or third party establishes no unlawful involvement or benefit from the transaction in which the person convicted was involved; and
  - (d) the use that is ordinarily made of the property, or the use to which the property was intended to be put.
- (5) Where the High Court makes a confiscation order, the High Court may give such directions as are necessary or convenient for giving effect to the order.

**§175. Effect of confiscation order.**

- (1) Subject to Subsection (2) of this Section, where a Court makes a confiscation order against any property, the property vests absolutely in the Republic of the Marshall Islands by virtue of the order.
- (2) Where property ordered to be confiscated is registered property:
  - (a) the property vests in the Republic of the Marshall Islands in equity, but does not vest in the Republic of the Marshall Islands at law until the applicable registration requirements have been complied with;
  - (b) the Republic of the Marshall Islands is entitled to be registered as owner of the property;
  - (c) the Commissioner or Attorney-General has power on behalf of the Republic of the Marshall Islands to do or authorize the doing of anything necessary or convenient to obtain the registration of the Republic of the Marshall Islands as owner, including the execution of any instrument to be executed by a person transferring an interest in property of that kind.
- (3) Where the High Court makes a confiscation order against property:
  - (a) the property shall not, except with the leave of the High Court and in accordance with any directions of the High Court, be disposed of, or otherwise dealt with, by or on behalf of the Republic of the Marshall Islands before the relevant appeal date; and
  - (b) if, after the relevant appeal date, the order has not been discharged, the property may be disposed of and the proceeds applied or otherwise dealt with in accordance with the direction of the Commissioner and Attorney-General.

**§176. Payment instead of a confiscation order.**

(1) Where the High Court is satisfied that a confiscation order should be made in respect of the property of a person convicted of a serious offense, but that the property or any part thereof or interest therein cannot be made subject to such an order and, in particular:

- (a) cannot, on the exercise of due diligence be located;
- (b) has been transferred to a third party in circumstances which do not give rise to a reasonable inference that the title or interest was transferred for the purpose of avoiding the confiscation of the property;
- (c) is located outside of the Marshall Islands;
- (d) has been substantially diminished in value or rendered worthless; or
- (e) has been commingled with other property that cannot be divided without difficulty the High Court may, instead of ordering the property or part thereof or interest therein to be confiscated, order the person to pay to the Marshall Islands an amount equal to the value of the property, part or interest.

**§177. Application of procedure for enforcing fines.**

(1) Where the High Court orders a person to pay an amount under Section 176, that amount shall be treated as if it were a fine imposed upon him or her in respect of a conviction for a serious offense, and the High Court shall:

- (a) Where a person is convicted of any of the offenses specified in Subsection (1), in the case of a natural person, such person shall be liable to imprisonment for a term of imprisonment not exceeding twenty (20) years or a fine not exceeding \$2,000,000, or both, and in the case of a body corporate five (5) times such a fine or double the amount of money involved in the offense scheme, whichever is greater.
- (b) direct that the term of imprisonment imposed pursuant to Subsection (a) be served consecutively to any other form of imprisonment imposed on that person, or that the person is then serving.

**§178. Immunity where suspicious transaction reported.**

No action, suit or other proceedings shall lie against any financial institution or cash dealer, or any officer, employee or other representative of the institution acting in the ordinary course of the person's employment or representation, in relation to any action taken in good faith by that institution or person pursuant to this Act.

**§179. Immunity where official powers or functions exercised in good faith.**

No suit, prosecution or other legal proceedings shall lie against the Government, or any officer or other person in respect of anything done by or on behalf of that person, with due diligence and in good faith, in the exercise of any power or the performance of any function under this Act or any rule of order made thereunder. (P.L. 2000-20)

**§180. Currency Transaction Reports**

The Commissioner of Banking may prescribe a regulation that requires a financial institution or cash dealer involved in a transaction for the payment, receipt or transfer of currency to file a report on the transaction with the Commissioner's office and collect and maintain supporting documentation pertaining to such transaction. The requirements for when a currency transaction report must be filed may include, but are not limited to, a currency transaction that exceeds \$10,000 or involves multiple transactions, taken by or on behalf of a single person within a 24 hour period and, when aggregated, exceeds \$10,000. The Commissioner of Banking may also prescribe under the regulation the right to exempt certain transactions, including a class of transactions, from the filing requirement by the use and maintenance of an exemption registry by financial institutions and cash dealers. The Commissioner has the authority to revoke any exemption granted under the regulation. (P.L. 2002-59)

**§181. Assessment of Civil Money Penalties**

(1) In addition to any criminal penalties or fines authorized by Part XIII of the Banking Act, 1987, each financial institution and cash dealer, and any partner, director, officer, employee, or person participating in the conduct of the affairs of the financial institution or cash dealer who violates any provision of Part XIII, or any regulation promulgated by the Banking Commissioner implementing any provision of Part XIII shall be liable for a civil money penalty of not more than \$10,000 per violation.

(2) Collection: The Banking Commissioner shall refer all violations under subsection (1) above to the office of the Attorney-General for enforcement proceedings in the High Court of the Republic of the Marshall Islands; and (a) all monies collected under the authority of this paragraph shall be deposited into the Treasury of the Republic.

(3) The resignation, termination of employment or termination of participation in the affairs of any partner, director, officer, employee, or person participating in the conduct of the affairs of a financial institution or cash dealer shall not affect the jurisdiction of the court to issue judgement against such person or entity within six years of their resignation, termination of employment or termination of participation in the affairs of the financial institution or cash dealer.

(4) The Banking Commissioner may prescribe regulations establishing criteria and procedures not inconsistent with these provisions as may be necessary to carry out the provisions of this Part XIII.

(P.L. 2002-59)(sections 66 to 82 re-numbered to conform with style and format of the Code. Subsection (4) herein was incorrectly numbered as (5) in P.L. 2002-59)

**§182. Effective Date**

This Act shall take effect in accordance with Article VI, Section 21 of the Constitution. (Sections 166 -183 re-numbered to accommodate new provisions and to conform to new Code format P.L. 2002-59(Rev2003)

## **Anti-Money Laundering Regulations, 2002**

### **BANKING ACT**

The Banking Commissioner pursuant to Section 181 of the Banking Act, 17 MIRC, Chapter 1, as amended, hereby makes Regulations in respect to matters related to Anti-Money Laundering and Countering the Financing of Terrorism. .

#### **Section 1. Persons associated with or who control financial institutions and cash dealers.**

- (a) Each financial institution and cash dealer shall identify, obtain the requisite information, retain records and file with the Banking Commissioner reports regarding persons affiliated with or who own or control the financial institution and cash dealer to the extent and in the manner required by this Section 1.
- (b) Definitions. For the purposes of these Regulations:
  - (1) Act - means the Banking Act, 17 MIRC, Chapter 1;
  - (2) Acting in concert – means knowing participation in a joint activity or parallel action towards a common goal of acquiring control of a financial institution or cash dealer, whether or not pursuant to an express agreement;
  - (3) Attorney-General - means the Attorney-General appointed pursuant to the Constitution of the Republic of the Marshall Islands;
  - (4) Banking Commissioner - means the Banking Commissioner appointed under the Act;
  - (5) Batch transfers – means a transfer comprised of a number of individual wire transfers that are being sent to the same financial institutions, but may/may not be ultimately intended for different persons;
  - (6) Beneficial owners – means the beneficiary as defined in the Trust Act, 50 MIRC, Chapter 1;
  - (7) Control – means:
    - (i) the power, directly or indirectly, to direct the management or policies of a financial institution or cash dealer; or
    - (ii) to vote 10% or more of any class of voting shares of a financial institution or cash dealer;
  - (8) Cross-border transfer - means any wire transfer where the originator and beneficiary institutions are located in different jurisdictions. This also refers to any chain of wire transfers that has at least one cross-border element;
  - (9) Domestic transfers - means any transfer where the originator and beneficiary institutions are located in the same jurisdiction. This refers to any chain of wire transfers that takes place entirely within the borders of a single jurisdiction, even though the system used to effect the wire transfer may be located in another jurisdiction;
  - (10) “Financial institution and cash dealer” means the financial institution and cash dealer as defined in the Act;
  - (11) Identify – means to ascertain the full name, address, nationality occupation/business or principal activity;
  - (12) Institution affiliated party – means any director, officer, employee or person who:
    - (i) owns or controls a financial institution or cash dealer, or
    - (ii) participates in the conduct of the affairs of a financial institution or cash dealer;
  - (13) Intermediary - means a person relied on by a financial institution or cash dealer to perform some of the elements of the CDD process or to introduce business to the financial institution or cash dealer;
  - (14) Legal arrangement - refers to express trusts or other similar arrangements, i.e. fiducie, treuhand and fideicomiso;

- (15) Legal persons - refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property;
- (16) Politically exposed person - means any person who is or has been entrusted with a prominent public function in a foreign country, including, but not limited to Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned companies, and important political party officials. Family members and close associates who have business relationships with such persons are also included herein;
- (17) Settlor - means the settlor as defined in the Trust Act, 50 MIRC, Chapter 1;
- (18) Shell Bank – means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision;
- (19) Trustee - means a person performing functions under Part II of the Trusts Act, 50 MIRC, Chapter 1;
- (20) Wire transfers - means any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and beneficiary may be the same person.
- (c) Recordkeeping. Each financial institution and cash dealer shall
- (1) adopt a methodology by which it will identify all persons who, acting alone or in concert with one or more persons, owned or controlled the financial institution or cash dealer at any time during the immediately preceding calendar year;
  - (2) adopt a methodology by which it will ascertain whether any institution affiliated party has been convicted of any offense involving dishonesty, breach of trust or money laundering; and
  - (3) record the information gathered pursuant to this subsection (c) (1) and (2) in a report no later than thirty (30) days following the end of the year.
- (d) The compliance officer, as designated by each financial institution or cash dealer pursuant to Section 2 (Internal Policies, Procedures, Policies, and Training), shall certify that the information collected and retained by the financial institution or cash dealer pursuant to subsection (c)(3) is true and accurate.
- (e) Reporting – ownership/control reports.
- (1) Information regarding ownership and control of financial institutions and cash dealers shall be reported by completing an Ownership/Control Report form (OCR) pursuant to the OCR's instructions, and collecting and maintaining supporting documentation as required by paragraph (c) of this Section 1.
  - (2) The OCR shall be filed with the Banking Commissioner, as indicated in the instructions to the OCR.
  - (3) The OCR shall be filed annually, no later than by February 1.
- (f) Retention of Reports. Each financial institution or cash dealer shall retain a copy of all reports together with any supporting documentation required by this Section 1 for a period of six (6) years from the date the report is filed with the Banking Commissioner.

## **Section 2. Internal Policies, Procedures, Controls and Training**

### **Section 2A: Internal Policies, Procedures, Controls, and Training**

2A.1 Financial institutions and cash dealers must adopt and implement internal policies, procedures, and controls to ensure compliance with these Regulations.

2A.2 Financial institutions and cash dealers must designate a compliance officer at the management level. The compliance officer and other appropriate staff should have timely access to customer identification data and customer due diligence (CDD) information, transaction records, and any other relevant information. The compliance officer should have the authority to act independently and to report to senior management above the compliance officer's next reporting level or the board of directors or equivalent body.

2A.3 Financial institutions and cash dealers should acquaint themselves with relevant information on the prevention of money laundering and terrorist financing.

2A.4 Financial institutions and cash dealers must maintain an adequately resourced and internal or independent audit function to test compliance (including sample testing) with these policies, procedures, and controls.

2A.5 Financial institutions and cash dealers must establish ongoing employee training to ensure that employees are kept informed of new developments, including information on current money laundering and terrorist financing techniques, methods and trends; and that there is a clear explanation of all aspects of money laundering and terrorist financing laws and obligations, and in particular, requirements concerning CDD and suspicious activity reporting.

2A.6 Financial institutions and cash dealers must establish screening procedures to ensure appropriate standards when hiring employees.

2A.7 Financial institutions and cash dealers must have a centralized system for maintaining records of the information on the identity of customers, principal beneficiaries, authorized agents, beneficial owners, suspicious transactions and transactions exceeding \$10,000 or its equivalent in a foreign currency.

### **Section 3. Risk-Based Customer Due Diligence (CDD)**

#### **Section 3A: Definition of Risk-based Customer Due Diligence**

##### **3A.1 CDD includes:**

- a. identification of customers, including beneficial owners of the formal customer;
- b. gathering of information on customers to create a customer profile;
- c. application of acceptance policies to new customers;
- d. maintenance of customer information on an ongoing basis;
- e. monitoring of customer transactions; and
- f. rules on wire transfers and correspondent banking.

3A.2 CDD must be applied on a risk basis, which must include enhanced CDD for higher risk customers and "politically exposed persons" and may include simplified CDD for lower risk customers.

3A.3 CDD must be applied to existing customers on the basis of materiality and risk, and CDD must be conducted on such existing relationships at material times.

3A.4 CDD must be applied to any existing customers that have anonymous accounts or accounts in fictitious names.

#### **Section 3B: Identification of Customers**

3B.1 Financial institutions and cash dealers may not keep anonymous accounts or accounts in obviously fictitious names.

3B.2 Financial institutions and cash dealers must ensure that they know the true identity of their customers. Customers include persons who are (or who seek to be):

- a. in a business relationship (“business relationship”);
- b. engaged in one or more occasional transactions when the total value of the transactions exceeds \$10,000 (“threshold occasional transaction”);
- c. carrying out wire transfers as provided in Section 3M (“wire transfer”); and
- d. engaged in any business or transaction in any instance where there is a suspicion that the person is involved in money laundering or terrorist financing (“suspicious activity”) with the financial institution and cash dealer.

3B.3 In order to ensure proper customer identification, the financial institution and cash dealer must identify and verify the identity of the customer at any time that:

- a. the person applies for a business relationship;
- b. the person seeks to engage in a threshold occasional transaction;
- c. the person seeks to carry out a wire transfer;
- d. the person engages in a suspicious activity; and
- e. where doubts have arisen as to the veracity or adequacy of previously obtained identification data on the person.

3B.4 For customers who are physical persons, the financial institution and cash dealer must verify identity required using reliable, independent source documents, data, or information as provided for in Schedule 1 of these Regulations.

3B.5 For customers who are legal persons or legal arrangements, the financial institution and cash dealer must obtain and verify:

- a. the customer’s name and legal form, including by obtaining proof of incorporation or similar evidence of establishment or existence (such as a trust instrument);
- b. the names and addresses of members of the customer’s controlling body (such as directors or trustees);
- c. legal provisions that set out the power to bind the customer;
- d. legal provisions that authorize persons to act on behalf of the customer; and
- e. the identity of the physical person purporting to act on behalf of the customer, using source documents as provided in Section 3B.4.

3B.6 Legible file copies must be made and retained of the relevant identification data, account files, and business correspondence for at least six years following the termination of an account or business relationship (or longer if requested by the Banking Commissioner).

3B.7 Financial institutions and cash dealers must ensure that all customer and transaction records are available on a timely basis to the Banking Commissioner upon request.

#### Section 3C: Determination of Beneficial Owner of the Customer

3C.1 The financial institution and cash dealer must take reasonable measures to determine if a customer is acting on behalf of one or more beneficial owners. If so, the financial institution and cash dealer should take reasonable steps to verify the identity of the beneficial owner by using relevant information or data obtained from a reliable source such that the financial institution and cash dealer is satisfied that it knows the identity of the beneficial owner.

Financial institutions and cash dealers must obtain information on the intended purpose and intended nature of the business relationship.

3C.2 For life and other investment-linked insurance, the beneficiary under the policy must be identified

and verified.

3C.3 For public companies (or other legal persons or legal arrangements) quoted on an exchange regulated by the Banking Commission, and certain non-resident public companies subject to adequate regulatory disclosure requirements and quoted on a foreign exchange approved for this purpose by the Banking Commission that is subject to adequate supervision in a jurisdiction that is implementing effectively the FATF 40 and FATF 9 Special Recommendations, no further identification is necessary. In determining if there has been effective implementation in the jurisdiction, financial institutions and cash dealers should take into account the information available on whether these countries adequately apply the FATF 40 and FATF 9 Special Recommendations, including by examining the reports and reviews prepared by the Financial Action Task Force, International Monetary Fund, and World Bank publications.

3C.4 For other customers that are legal persons or legal arrangements, the financial institution and cash dealer must take reasonable measures to understand the ownership and control structure of the customer, including the ultimate natural person(s) who owns or controls a legal person, including natural persons with a controlling interest as described in this Section.

3C.5 With respect to companies, limited partnerships, or similar arrangements, identification should be made of each natural person that:

- a. owns directly or indirectly 10 percent or more of the vote or value of an equity interest in; and
- b. exercises management of

the company, limited partnership or similar arrangement.

3C.6 With respect to a trust or similar arrangements, identification should be made of the settlor(s), trustee(s), and beneficiaries whose vested interest is 10 percent or more of the value of the trust corpus.

3C.7 In determining indirect ownership of equity interests,

- a. an equity interest held by a company, limited partnership, or similar arrangement and by a trust should be considered as being owned proportionately by its shareholders, partners, or vested beneficiaries; and
- b. an equity interest held by a family member should be considered as also being owned, in its entirety, by each family member (family members include brothers, sisters, whether by the whole or half blood, spouse, ancestors, and lineal descendants).

3C.8 Legible file copies must be made and retained of the relevant identification data, account files and business correspondence for at least six years following the termination of an account or business relationship (or longer if requested by the Banking Commissioner ).

3C.9 Financial institutions and cash dealers must ensure that all customer and transaction records are available on a timely basis to the Commissioner of Banking upon request.

#### Section 3D: Delayed Verification

3D.1 Financial institutions and cash dealers may apply to the Banking Commission for authorization to delay completion of the customer identification process in Section 3B.3 a. and 3B.3 b. And Section 3C. Permission will be granted by the Banking Commission only if the financial institution and cash dealer presents a procedure that complies with this Section.

3D.2 Financial institutions and cash dealers may delay verification only if: verification occurs as soon afterwards as reasonably practical, the delay is essential to not interrupt the normal course of business, and the money laundering and terrorist financing risks are effectively managed.

Examples of situations where it may be essential not to interrupt the course of the normal conduct of business can be found in Appendix 1 Part A of these Regulations.

3D.3 Procedures to manage risk concerning delayed customer identification should include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed, and enhanced monitoring of large and complex transactions being carried out outside of the expected norms for that type of relationship.

#### Section 3E: Establishment of Customer Profile

3E.1 A financial institution and cash dealer must create a profile for each customer of sufficient detail to enable it to implement the CDD requirements of these Regulations. The customer profile should be based upon sufficient knowledge of the customer, including the customer's proposed business with the financial institution and cash dealer, and where necessary, the source of customer funds.

#### Section 3F: Reliance on Intermediaries

3F.1 Financial institutions and cash dealers may apply to the Banking Commission for authorization to rely on intermediaries such as trust and company service providers to perform the duties in Section 3B and 3C of this Regulation. Permission will be granted by the Banking Commission only if the financial institution and cash dealer presents a plan of internal policies and practices that comply with this Section.

3F.2 Financial institution and cash dealers may rely upon intermediaries that are also financial institutions and cash dealers (other entities that are subject to supervision by the Banking Commission under this Regulation).

3F.3 Financial institution and cash dealers may rely upon non-resident intermediaries if the financial institution and cash dealer is satisfied that the third party is adequately regulated and supervised and has measures in place to comply with the CDD requirements in this Regulation.

Financial institutions and cash dealers must be satisfied that a non-resident intermediary is subject to money laundering and terrorist financing policies comparable with the FATF 40 and FATF 9 Special Recommendations. They must be satisfied that the non-resident intermediary is subject to licensing and supervision to enforce those policies, and has not been subject to any material disciplinary action that calls into question its execution of those policies. Financial institutions and cash dealers must ensure that non-resident intermediaries are located in a jurisdiction that is implementing effectively the FATF 40 and FATF 9 Special Recommendations. In making this determination, financial institutions and cash dealers should take into account the information available on application and adequacy of implementation of the FATF 40 and FATF 9 Special Recommendations to entities in individual countries.

3F.4 In each instance of reliance on intermediaries, the financial institution and cash dealer must immediately obtain from the third party the information required in Section 3B and 3C.

While it is not necessary to obtain copies of the CDD documentation from the intermediary, financial institutions and cash dealers must take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the information obtained under Section 3F.3 will be made available without delay, if requested.

3F.5 Financial institutions and cash dealers may not rely upon intermediaries identified by the Banking Commission as non-complying with the FATF 40 and FATF 9 Special Recommendations, or intermediaries for whom the financial institution and cash dealer have independent credible reason to believe are not complying with the FATF 40 and FATF 9 Special Recommendations.

3F.6 The ultimate responsibility for implementation of the customer due diligence requirements of these Regulations remains with the financial institution and cash dealer.

3F.7 The requirements of this Section do not apply to outsourcing or agency relationships, i.e. where the agent is acting under a contractual arrangement with the financial institution or cash dealer to carry out its CDD functions.

3F.8 The requirements of this Section do not apply to business relationships, accounts, or transactions between financial institutions and cash dealers for their clients.

### Section 3G: Acceptance of New Customers

3G.1 Financial institutions and cash dealers should not accept as customers those persons whose identity and beneficial owner as required in 3B, 3C, and 3D cannot be assured or for whom sufficient information to form a customer profile cannot be gathered. In such cases, financial institutions and cash dealers should determine if they should file a suspicious activity report.

3G.2 It is important that the policy on acceptance of new customers is not so restrictive that it results in a denial of access by the general public to financial services, especially for people who are financially or socially disadvantaged.

### Section 3H: The Maintenance of Customer Information on an Ongoing Basis

3H.1 Financial institutions and cash dealers must gather and maintain customer information on an ongoing basis. Documents, data, or information collected under the CDD process should be kept up to date and relevant by taking reviews of existing records at appropriate times, particularly for higher risk categories of customers or business relationships.

### Section 3I: Ongoing Monitoring of Customer Transactions

3I.1 Financial institutions and cash dealers must monitor ongoing customer transactions. Monitoring must include the scrutiny of customer transactions to ensure that they are being conducted according to the financial institution and cash dealer's knowledge of the customer and the customer profile, and where necessary, the source of funds, and may include predetermined limits on amount of transactions and type of transactions.

3I.2 Financial institutions and cash dealers must pay special attention to all complex, unusual large transactions, or unusual pattern of transactions that have no visible economic or lawful purpose. Financial institutions and cash dealers must examine as far as possible the background and purpose of such transactions and set forth their findings in writing. Financial institutions and cash dealers must keep such findings available for examination by the Banking Commission, auditors, and any other competent authorities, for a minimum of six years. In such cases, financial institutions and cash dealers should determine if they should file a suspicious activity report.

### Section 3J: Termination of Customer Relationship

3J.1 If the financial institution and cash dealer has already commenced a business relationship and is unable to comply with the CDD required for a customer, it should terminate the customer relationship and determine if it should file a suspicious activity report.

### Section 3K: Enhanced CDD for Higher Risk Customers and Politically Exposed Persons

3K.1 Financial institutions and cash dealers must apply enhanced CDD for customers that are likely to pose a higher risk of money laundering or terrorist financing (“enhanced CDD”). Enhanced CDD should include reasonable measures to establish the source of wealth and source of funds of customers and beneficial owners identified as higher risk customers and politically exposed persons.

Enhanced CDD should be applied to customers and beneficial owners identified as higher risk customers and politically exposed persons at each stage of the CDD process.

Examples of higher risk customers and politically exposed persons can be found in Appendix 1 Part B of these Regulations. The definition of politically exposed person is in Section 9 of these Regulations.

3K.2 No customers and beneficial owners identified as higher risk customers and politically exposed persons should be accepted as a customer unless a senior member of the financial institution and cash dealer’s management has approved.

3K.3 Where a customer or beneficial owner has been accepted and the customer or beneficial owner is subsequently found to be, or subsequently becomes a higher risk customer or politically exposed person, financial institutions and cash dealers must obtain senior management approval to continue the business relationship.

3K.4 Where financial institutions and cash dealers are in a business relationship with a higher risk customer or a politically exposed person, they must conduct enhanced ongoing monitoring of that relationship.

3K.5 Financial institutions and cash dealers must put in place appropriate risk management systems to determine whether a potential customer or the beneficial owner is a high risk customer or a politically exposed person.

#### Section 3L: Simplified CDD for Lower Risk Customers.

3L.1 Financial institution and cash dealers may apply to the Banking Commission for authorization to apply reduced or simplified customer due diligence procedure. Permission will be granted by the Banking Commission only if the financial institution and cash dealer presents a procedure that complies with this Section.

3L.2 In general, customers must be subject to the full range of CDD measures as provided in this Regulation, including the requirement to identify the beneficial owner. Where the risk of money laundering and terrorist financing is lower and where information on the identity of the customer and the beneficial owner of the customer is publicly available, or where adequate checks and controls exist in national systems, in such circumstances it would be reasonable for financial institutions and cash dealers to apply simplified or reduced CDD measures when identifying and verifying the identity of the customer or beneficial owner.

3L.3 Simplified or reduced CDD measures when applied to customers that are residents in another country is limited to countries that are in compliance with and have effectively implemented the FATF 40 and FATF Special 9 Recommendations.

3L.4 Simplified or reduced CDD measures are not acceptable whenever there is a suspicion of money laundering, terrorist financing, or specific higher risk scenarios.

Examples of lower risk customers are to be found in Appendix 1 Part C of this Regulation.

#### Section 3M: Policies and Procedures on Wire Transfers

3M.1 Financial institutions and cash dealers must ensure that all persons ordering wire transfers obtain and maintain full originator information, and verify that the information is accurate and meaningful.

3M.2 Full originator information includes:

- a. the name of the originator;
- b. the originator's account number (or a unique reference number if there is no account number);
- c. the originator's address; and
- d. the originator's identification card number.

3M.3 For cross-border wire transfers (including batch transfers and transactions using a credit or debit card to effect a funds transfer), the ordering financial institution and cash dealer should be required to include full originator information in the message or payment form accompanying the wire transfer, except in the circumstances provided below for batch transfers.

3M.4 For domestic wire transfers (including transactions using a credit or debit card as a payment system to effect a money transfer), the ordering financial institution and cash dealer must include either:

- a. full originator information in the message or payment form accompanying the wire transfer, or
- b. only the originator's account number or, where no account number exists, a unique identifier, within the message or payment form.

3M.5 Section 3M.4 b may be used only if full originator information can be made available to the beneficiary financial institution and cash dealer and the Banking Commission within three working days of receiving a request.

3M.6 If a cross-border wire transfer is contained within a batch transfer and is sent by a financial institution and cash dealer, it may be treated as a domestic wire transfer provided the requirements for domestic wire transfers are met.

3M.7 The financial institution and cash dealer should ensure that non-routine transactions are not batched where this would increase the risk of money laundering or terrorist financing.

3M.8 Each intermediary in the payment chain should maintain all the required originator information with the accompanying wire transfer.

3M.9 Financial institutions and cash dealers may apply to the Banking Commission for authorization to exempt wire transfers below \$ 3,000 from the requirements of Section 3M.3 and 3M.4. Permission will be granted by the Banking Commission only if the financial institution or cash dealer presents a procedure that complies with this Section.

3M.10 Beneficiary financial institutions and cash dealers must identify and handle wire transfers that are not accompanied by complete originator information on the basis of perceived risk of money laundering and terrorist financing. Procedures to address these cases should include the financial institution and cash dealer first requesting the missing originator information from the financial institution and cash dealer that sent the wire transfer. If the missing information is not forthcoming, the financial institution and cash dealer should consider whether, in all the circumstances, the absence of complete originator information creates or contributes to suspicion about the wire transfer or a related transaction. If the wire transfer is deemed to be suspicious, then it should send a suspicious activity report to the Banking Commission. In addition, the financial institution and cash dealer may decide not to accept the wire transfer. In appropriate circumstances, beneficiary financial institutions and cash dealers should consider restricting or terminating business relationships with financial institutions and cash dealers that do not comply with this Section.

## Section 3N: Policies and Procedures on Cross Border Correspondent Banking and Similar Relationships

3N.1 Correspondent banking is defined as the provision by one bank (the correspondent) to another bank (the respondent) of credit, deposit, collection, clearing or payment services.

3N.2 Banks must develop and implement policies and procedures concerning correspondent banking. In order to provide correspondent banking services, a bank must first assess the respondent's controls against money laundering and terrorist financing and determine that they are adequate and effective. To do so, banks must gather sufficient information about respondent banks to understand their business and determine from publicly available information the reputation of the institution, quality of supervision, and whether it has been subject to a money laundering or terrorism financing investigation or regulatory action. A bank should, in general, establish or continue a correspondent relationship with a foreign bank only if it is satisfied that the bank is effectively supervised by the relevant authority. In particular, a bank should not establish or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which the bank has no presence and which is unaffiliated with a regulated financial group (i.e. a shell bank).

3N.3 The information to be collected may include, but is not limited to, details about the respondent bank's management, major business activities, where it is located, its money laundering and terrorist financing prevention efforts, the system of bank regulation and supervision in the respondent bank's country and the purpose of the account.

3N.4 A bank should pay particular attention when maintaining a correspondent banking relationship with banks incorporated in jurisdictions that do not meet international standards for the prevention of money laundering and terrorist financing. Enhanced due diligence will generally be required in such cases, including obtaining details of the beneficial ownership of such banks and more extensive information about their policies and procedures to prevent money laundering and terrorist financing.

3N.5 A bank must develop and implement policies and procedures concerning the ongoing monitoring of activities conducted through such correspondent accounts.

3N.6 Particular care should also be exercised where the bank's respondent allows direct use of the correspondent account by third parties to transact business on their own behalf (i.e. payable-through accounts). A bank must be satisfied that the respondent bank has performed the customer due diligence required in these Regulations for those customers that have direct access to the accounts of the correspondent, and that the respondent is able to provide relevant customer identification information on request of the correspondent.

## Non face-to-face transactions and new technologies

3N.7 Financial institutions and cash dealers are required to have policies in place and take such measures as are needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes.

3N.8 Financial institutions and cash dealers are required to have policies and procedures in place to address specific risks associated with non face-to face business relationships or transactions. These policies should apply when establishing customer relationships and when conducting ongoing due diligence. This should include specific and effective CDD procedures that apply to non face-to-face customers.

## Shell Banks

3N.9 It is not permissible to establish or accept the operation of a shell bank in the Marshall Islands.

3N.10 Financial institutions and cash dealers must not enter into correspondent banking relationships with shell banks.

3N.11 Financial institutions and cash dealers must satisfy themselves that respondent financial institutions and cash dealers in a foreign country do not permit their accounts to be used by shell banks.

#### **Section 4. Transactions, Recordkeeping.**

(a) Every financial institution and cash dealer shall retain records regarding all transactions to the extent and in the manner required by this Section 4.

(b) For the purposes of this Section 4, a transaction is: a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition, of assets, and includes a deposit, credit, withdrawal, debit, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security, purchase or redemption of any traveler's check or money order, payment or order for any money remittance or transfer, or any other payment, transfer, or delivery by, through, or to a financial institution or cash dealer, by whatever means effected

(c) Recordkeeping – All financial institutions and cash dealers shall retain records necessary to reconstruct all transactions and sufficient to identify:

(1) the name, address and occupation/business or principal activity of each person conducting or involved in a transaction or on whose behalf a transaction is conducted;

(2) the identity of all financial institutions and cash dealers involved;

(3) the nature and date of the transaction, together with all advices, requests, or instructions given or received;

(4) the type and identification numbers of all accounts involved;

(5) the type and amount of currency involved, if any;

(6) if a negotiable instrument other than currency involved

(i) the name of the drawer

(ii) the name of institution on which it is drawn

(iii) the name of the payee, if any;

(iv) amount and date of the instrument

(v) the number of the instrument, if any; and

(vi) details regarding all endorsements appearing on the instrument; and

(7) name(s) of officers, employees and agent(s) and method(s) used to verify the information required by this subsection (c).

(d) Each financial institution or cash dealer shall, in addition to the records in Subsection (c), retain the following:

(1) Each check, clean draft, or money order drawn on the bank or issued and payable by it, except those drawn for \$100 or less or those drawn on accounts which can be expected to have drawn on them an average of at least 100 checks per month over the calendar year or on each occasion on which such checks are issued, and which are:

(i) dividend checks,

(ii) payroll checks,

(iii) employee benefit checks,

(iv) insurance claim checks,

(v) medical benefit checks,

(vi) checks drawn on government agency accounts,

(vii) checks drawn by brokers or dealers in securities,

(viii) checks drawn on fiduciary accounts,

- (ix) checks drawn on other financial institutions, or
- (x) pension or annuity checks.

(2) Each item in excess of \$100 (other than bank charges or periodic charges made pursuant to agreement with the customer), comprising a debit to a customer's deposit or share account, not required to be kept, and not specifically exempted, under paragraph (d)(1) of this section;

(e) Retention of records.

- (1) A financial institution or cash dealer shall maintain either the original or a microfilm, electronic or other copy or reproduction of all records, documents, advice requests and instructions regarding any transaction subject to Section 4 recordkeeping requirements for a period of six (6) years from the date of the completion of the transaction; and
- (2) all records shall be filed or stored in a readily recoverable manner as to be accessible within a reasonable time.

(f) Exemption. Nothing in this regulation shall be construed as requiring the production of any evidence of identity where there is a transaction or a series of transactions taking place in the course of a business relationship, in respect of which the applicant has already produced satisfactory evidence of identity.

## **Section 5. Reports of suspicious transactions.**

(a) General.

(1) Every financial institution and cash dealer shall file with the Banking Commissioner, to the extent and in the manner required by this Section 5, a Suspicious Activity Report (SAR) of any suspicious transaction. A financial institution or cash dealer may also file a SAR regarding any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by this section.

(A) Where a financial institution or cash dealer suspects that any transaction or any other activity could constitute or be related to terrorist financing, terrorist acts, a terrorist organization, an individual terrorist or to terrorist property the financial institution must report such suspicion to the Banking Commissioner within three working days of forming of such suspicion.

(2) For the purposes of reporting under this Section 5, a suspicious transaction is:

- (a) a transaction which includes a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition, of assets, and includes a deposit, credit, withdrawal, debit, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security, purchase or redemption of any traveler's check or money order, payment or order for any money remittance or transfer, or any other payment, transfer, or delivery by, through, or to a financial institution or cash dealer, by whatever means effected; and
- (b) which is conducted or attempted to be conducted at a financial institution or cash dealer; and
- (c) one which the financial institution or cash dealer knows, suspects or has reason to suspect that:
  - (i) involves funds or other assets derived from illegal activity; or
  - (ii) was conducted or attempted to be conducted
    - (A) in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets); or
    - (B) as part of a plan to violate or evade any Marshall Islands law or regulation or to avoid any transaction reporting requirement under Marshall Islands law or regulation; or
  - (iii) involves a transaction or transactions which:
    - (A) is/are complex or unusual; or

- (B) present an unusual pattern; or
- (C) has/have no apparent economic or lawful purpose; or
- (D) is/are not the sort of transaction in which any person or entity involved would normally be expected to engage.

(b) Filing procedures

- (1) A suspicious transaction shall be reported by completing a SAR form pursuant to the SAR's instructions, and collecting and maintaining supporting documentation as required by paragraph (c) of this Section 5.
  - (2) The SAR shall be filed with the Banking Commissioner, as indicated in the instructions to the SAR.
  - (3) The SAR shall be filed no later than three (3) working days after the date of initial detection by the financial institution or cash dealer of facts that may constitute a basis for filing a SAR. If no suspect was identified on the date of the detection of the incident requiring the filing, a financial institution or cash dealer may delay filing a SAR for an additional thirty (30) calendar days in order to identify a suspect. In no case shall reporting be delayed more than thirty three (33) calendar days after the date of initial detection of a reportable transaction. In situations involving violations that require immediate attention, such as, for example, ongoing money laundering schemes, the financial institution or cash dealer shall immediately notify the Banking Commissioner, or his designee, in addition to a later timely filing of the SAR.
- (c) Retention of records. A financial institution or cash dealer shall maintain a copy of any SAR filed and the original or business record equivalent of any supporting documentation for a period of fifteen (15) years from the date of filing the SAR. Supporting documentation shall be identified, and maintained by the financial institution or cash dealer as such, and shall be deemed to have been filed with the SAR. A financial institution or cash dealer shall make all supporting documentation available to the Banking Commission and any appropriate law enforcement agencies upon request.
- (d) Confidentiality of reports. Financial institutions and cash dealers, its employees, officers, directors, and agents shall not notify any person or entity other than those authorized by law, of the information, record or that an SAR has been prepared, or otherwise referred or furnished to the Banking Commissioner, Attorney General, court of competent jurisdiction, or other lawfully recognized person.

## **Section 6. Currency Transaction Reporting.**

- (a) Every financial institution and cash dealer shall obtain the requisite information and file with the Banking Commissioner reports of transactions in currency to the extent and in the manner herein required.
- (b) For the purposes of obtaining, information and reporting under this Section 6, a transaction in currency is:
  - (1) a deposit, withdrawal, exchange of currency, or other payment or transfer;
  - (2) involving currency of any country of a value greater than US\$10,000:
    - (i) in a single transaction; or
    - (ii) in multiple transactions taken by or on behalf of a single person within a 24 hour period when aggregated.
- (c) Prior to concluding any transaction in currency all financial institutions and cash dealers shall obtain and verify the following information:
  - (1) the name, address, citizenship/residency status, social security number or passport number and occupation/business or principal activity of each person conducting or involved in a transaction or on whose behalf a transaction is conducted;
  - (2) the nature and date of the transaction;
  - (3) the type and identification numbers of all accounts involved;

- (4) the type and amount of currency involved, and
- (5) name(s) of officers, employees and agent(s) and method(s) used to verify the information required by this subsection (c).
- (d) Verification – records to be examined. Financial institutions and cash dealers satisfy their requirement to verify information required by Section 6(c) records by obtaining from and examining:
  - (1) from individuals - original official unexpired documents bearing a photograph or reasonable alternative;
  - (2) articles of incorporation, charters, or their equivalents, or any other official documentation establishing that it has been lawfully registered and is in existence at the time of identification and which delineates the powers of their legal representatives; and
  - (3) the appropriate documentation for all persons acting, or appearing to act in a representative capacity including all the beneficiary(ies).
- (e) Reporting – transactions in currency. Filing procedures.
  - (1) Information regarding transactions in currency not otherwise exempted pursuant to subsection (g) and (h) of this Section 6 shall be reported by completing a Currency Transaction Report form (CTR) pursuant to the CTR's instructions, and collecting and maintaining supporting documentation as required by paragraph (c) of this Section 6.
  - (2) The CTR shall be filed with the Banking Commissioner, as indicated in the instructions to the CTR.
  - (3) The CTR shall be filed no later than ten (10) working days after the date of transaction in currency.
- (f) Retention of records. A financial institution or cash dealer shall maintain a copy of any CTR filed and the original or a microfilm, electronic or other copy or reproduction, or business record equivalent of any supporting documentation of a CTR for a period of six (6) years from the date of filing the CTR. Supporting documentation shall be identified, and maintained by the financial institution or cash dealer as such, and shall be deemed to have been filed with the CTR. A financial institution or cash dealer shall make all supporting documentation available to the Banking Commissioner and any appropriate law enforcement agencies upon request.
- (g) Transactions eligible for exemption from filing report.
  - (1) A transaction to which a financial institution or cash dealer is party is also eligible for exemption if:
    - (i) the other party to the transaction is a government agency of the Marshall Islands; and
    - (ii) the amount of currency involved in the transaction does not exceed an amount that is reasonably commensurate with the lawful business activities of that agency.
  - (2) A transaction is eligible for exemption if the transaction is between a financial institution and cash dealer and another financial institution and cash dealer; or
  - (3) A transaction is also eligible for exemption if:
    - (i) the transaction is between a financial institution and cash dealer and another person (in this subsection called the “customer”);
    - (ii) the customer has had, at the time when the transaction takes place, an account verified pursuant to Section 3 with the financial institution and cash dealer for one year;
    - (iii) the transaction consists of a deposit into, or a withdrawal from, an account maintained by the customer with the financial institution and cash dealer;
    - (iv) the transaction does not involve any party representing anyone in a representative capacity;
    - (v) the customer carries on a commercial enterprise (other than business that includes the selling of vehicles, vessels, aircraft, real estate brokerage, mobile home dealers, accountants, lawyers, doctors, pawnbrokers, title insurance/closing companies, trade unions, and auctioneers;
    - (vi) the account is maintained for the purposes of that business; and
    - (vii) the amount of currency involved in the transaction does not exceed an amount that is reasonably commensurate with the lawful business activities of the customer.
  - (4) A transaction is also eligible for exemption if:
    - (i) the transaction is between a financial institution and cash dealer and another person (in this subsection called the “customer”);

- (ii) the customer has had, at the time when the transaction takes place, an account verified pursuant to Section 3 with the financial institution and cash dealer for one year;
- (iii) the transaction consists of a withdrawal from an account maintained by the customer with the financial institution and cash dealer;
- (iv) the withdrawal is made for payroll purposes;
- (v) the customer regularly withdraws, from the account, currency of a value not less than \$10,000 to pay the customer's staff and employees; and
- (vi) the amount of currency involved in the transaction does not exceed an amount that is reasonably commensurate with the lawful business activities of the customer.

(h) Exemption registry. A record of each exemption granted under this section and the reason therefore must be kept by a financial institution and cash dealer in an exemption registry.

(1) For an exempted transaction between a financial institution or cash dealer and a government agency of the Marshall Islands under subsection (g)(1) and (2), the exemption registry should include the reason for the exemption and the names and addresses of the financial institution or cash dealer and/or government agencies involved in the transaction.

(2) For exempted transactions between a financial institution and cash dealer and a customer, as defined in (g) (3) and (4), the exemption registry must include the following information:

- (i) the reason for exemption;
- (ii) the customer's name, business or residential address, and his/her occupation, business or principal activity;
- (iii) a statement whether the exemption covers deposits, withdrawals or both;
- (iv) a signed statement by the customer that states the following:
  - (A) the party believes that the transaction is eligible for exemption under Section 6(g), and
  - (B) the information provided by the party to the institution in relation to the transaction is, to the best of his or knowledge and belief, true and correct;
- (v) the name and title of the person making the decision to grant the exemption; and
- (vi) any other information mandated by the Banking Commission.

(3) Class transactions. An exemption can apply to a class of transactions between a financial institution and cash dealer and eligible parties designated under Section 6(g). For class transactions, the exemption registry must also include in, addition to the requirements of Section 6(h) (1) and (2), the following:

- (i) the range of the amounts of currency involved in the class of transactions;
- (ii) the range amount of the class of transactions;
- (iii) the period during which the class of transactions is to be exempt; and
- (iv) any other information mandated by the Banking Commission.

(4) Financial institution or cash dealer must monitor the exemptions they have granted on a continual basis. A change in circumstances may warrant removal from the registry or require amending the exemption record in the registry. In addition to monitoring, each financial institution or cash dealer must commission an annual review of its exemption registry. A financial institution or cash dealer must contact each customer who has an exemption to determine whether there is a change in the customer's situation since the last date of review.

(5) The Banking Commission has the right to review the exemption registry at any time. The Bank Commission may, by appropriate order, direct the deletion of any.

## **Section 7. Assessment of Civil Money Penalties.**

(a) In addition to any criminal penalties authorized by the Banking Code, each financial institution and cash dealer, and any partner, director, officer, employee, or person participating in the conduct of the affairs of a financial institution or cash dealer who violates any provision of Part 13 of Title 17 or any of its implementing regulations shall forfeit and pay a civil money penalty to the extent and in the manner hereafter specified by this Section.

- (b) For any willful violation of any recordkeeping, reporting or verification requirement of Part 13 of Title 17 or any of its implementing regulations, the Banking Commissioner may recommend to the Office of Attorney General that it assess upon any financial institution and cash dealer, and upon any partner, director, officer, or employee thereof, or person participating in the conduct of the affairs of a financial institution or cash dealer who willfully participates in the violation, a civil money penalty not to exceed \$10,000 per violation.
- (c) For any negligent violation of any requirement of Part 13 of Title 17 or any of its implementing regulations, the Banking Commissioner may recommend to the Office of the Attorney it assess upon any financial institution and cash dealer, and upon any partner, director, officer, or employee thereof, or person participating in the conduct of the affairs of a financial institution or cash dealer who participates in the violation, a civil money penalty not to exceed \$500 per violation.
- (d) Assessment
  - (1) The Banking Commissioner shall inform the Office of the Attorney General of a violation and provide a detailed recommendation on the amount of the civil money penalty that should be sought.
  - (2) Upon receipt of the recommendation, the Office of the Attorney General must determine whether there is sufficient evidence to have the assessment enforced by the High Court.
  - (3) If the Office of Attorney General decides to enforce the assessment, written notice must be provided to the entity(ies) or person(s) from whom payment is sought. The notice must be sent out before the enforcement action is filed with the High Court.
- (e) All civil money penalties collected under this Section shall be paid over to the Treasury of the Republic of the Marshall Islands.
- (f) The resignation, termination of employment or termination of participation in the affairs of any partner, director, officer, employee, or person participating in the conduct of the affairs of a financial institution or cash dealer shall not affect the jurisdiction and authority of the Banking Commissioner to issue any Notice of assessment against such person or entity if such Notice is served within six years of their resignation, termination of employment or termination of participation in the affairs of the financial institution or cash dealer.

## **Section 8. Exceptions and exemptions.**

Subject to the provisions of the Act and these Regulations, the Banking Commissioner, in his/her sole discretion, may by written order or authorization make exceptions to or grant exemptions from the requirements of Sections 1 – 7. Such exceptions or exemptions may be conditional or unconditional, may apply to particular persons or classes of persons, and may apply to particular transactions or classes of transactions. They shall, however, be applicable only as expressly stated in the order or authorization. Any exception or exemption shall be revocable in the sole discretion of the Banking Commissioner.

## **Section 9. Application to branches and subsidiaries**

Financial institutions and cash dealers must ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with the requirements in the Marshall Islands and the FATF Recommendations.

Financial institutions and cash dealers must pay particular attention to this principle with respect to branches and subsidiaries in countries that do not or insufficiently apply the FATF Recommendations.

Where the minimum AML/CFT requirements of the Marshall Islands and the host country differ, branches and subsidiaries in host countries must apply the higher standard to the extent that the host country laws and regulations permit.

Financial institutions and cash dealers must inform the Banking Commissioner when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by host country laws, regulations or other measures.

#### Section 10 Guidelines

The Banking Commissioner may issue guidelines to assist financial institutions and cash dealers to implement and comply with their AML/CFT requirements.

### Appendix 1

#### Part A: Delayed Verification

1. Examples of situations where it may be essential not to interrupt the course of the normal conduct of business are:
  - a. non face-to-face business;
  - b. securities transactions; and
  - c. life insurance in relation to identification and verification of the beneficiary under the policy, which may take place after the business relationship with the policyholder is established, but in all such cases, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

#### Part B: Enhanced CDD for Higher Risk Customers

1. Relevant factors in determining if a customer is higher risk include if the person is:
  - a. establishing customer relations other than “face to face”;
  - k. a non-resident, or if the nationality, current residency, and previous residency of the person suggests greater risk of ML or TF;
  - l. connected with jurisdictions that lack proper standards in the prevention of ML or TF;
  - m. a politically exposed person (“PEP”) or linked to a PEP;
  - n. a high net worth individual, especially if the potential customer is a private banking customer or the source of funds is unclear;
  - o. engaged in a business that is particularly susceptible to money laundering or terrorism financing;
  - p. a legal person or arrangement that is a personal asset holding vehicle;
  - q. a legal person or arrangement whose ownership structure is complex for no good reason;
  - r. a company with nominee shareholders or shares in bearer form; and
  - s. higher risk for other reasons based on relevant information.
2. Non-face to face transactions include but are not limited to:
  - a. business relationships concluded over the Internet or by other means such as through the post;
  - b. services and transactions over the Internet including trading in securities by retail investors over the Internet or other interactive computer services;
  - c. use of ATM machines;
  - d. mobile telephone banking;
  - e. Transmission of instructions or applications via facsimile or similar means; and
  - f. making payments and receiving cash withdrawals as part of electronic point of sale transaction using prepaid or re-loadable or account-linked value cards.

3. Enhanced CDD procedures for non-face to face transactions may include:
  - a. certification of documents presented;
  - b. requisition of additional documents to complement those that are required for face to face customers;
  - c. development of independent contact with the customer.
4. Procedures for determining who is a PEP may include:
  - a. seeking relevant information from the potential customer;
  - b. referring to publicly available information; and
  - c. making access to commercial electronic databases of PEPs.
5. In applying enhanced due diligence, financial institutions and cash dealers must take care not to engage in unlawful discrimination on the basis of race, color, religion, or national origin.

Part C: Simplified CDD for Lower Risk Customers.

1. Examples of customers, transactions, or products where the risk may be lower include:
  - j. other financial institutions and cash dealers (other entities that are subject to supervision by the Banking Commission under this Regulation);
  - k. non-resident financial institutions that are subject to adequate regulation and supervision as limited by Section 3L;
  - l. public companies (or other legal persons or legal arrangements) quoted on an exchange regulated by the Banking Commission, and certain public companies quoted on a foreign exchange approved for this purpose by the Banking Commission that is subject to adequate supervision and providing the company is subject to adequate regulatory disclosure requirements, as limited by 3L;
  - m. domestic government administrations or enterprises, and certain foreign government administrations or enterprises as limited by 3L;
  - n. life insurance policies where the annual premium is no more than \$1,000.00 or a single premium of no more than \$2,500.00;
  - o. insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral;
  - p. pension, superannuation, or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;
  - q. beneficial owners of non-resident pooled accounts, provided they are subject to adequate regulation and supervision as limited by 3L;
  - r. small scale accounts and micro-credit accounts with an annual turnover of under \$200.00.
2. Non-resident and foreign entities described in b, c, d, and h may only qualify for reduced CDD if they are located in a jurisdiction that is implementing effectively the FATF 40 and FATF Special 9. In making this determination, financial institutions and cash dealers should take into account the information available on whether these countries adequately apply the FATF 40 and FATF Special 9, including by examining the approved list provided by the Banking Commission and reports, assessments, and reviews published by FATF, International Monetary Fund, and World Bank publications.
3. Simplified CDD measures are not acceptable whenever a customer has been identified by the Banking Commission as non-complying with the FATF 40 and FATF Special 9, or for which the financial institution and cash dealer have independent credible reason to believe are not complying with the FATF 40 and FATF Special 9, or for any reason that there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

## Schedule 1

### A. Procedure for verification of individuals

1. Where a financial institution and cash dealer is required to verify the identity of a person, the following information is required:

- (a) full and correct name of person and any other names previously held;
- (b) permanent address;
- (c) telephone (not including mobile phone number) and fax number (if any);
- (d) date and place of birth;
- (e) nationalities and citizenships held currently and previously by the applicant;
- (f) occupation and name of employer (if self employed, the nature of the self employment);
- (g) copy of first two pages of passport or copy of national identity card showing the following details:
  - i. number and country of issuance;
  - ii. issue and expiry date;
  - iii. signature of the person (applicable only to national identity card);
- (h) signature;
- (i) purpose of the account and the potential account activity;
- (j) written authority to obtain independent verification of any information provided;
- (k) source of income or wealth;
- (l) written confirmation that all credits to the account are and will be beneficially owned by the financial institution and cash dealer holder;
- (m) any documentary or other evidence reasonably capable of establishing the identity of that person.

2. Paragraph 1 shall also apply to the verification of identity of the beneficial owners of all financial institutions and cash dealers.

### B. Procedures for verification of corporate entities

Where a financial institution and cash dealer is required to verify the identity of a corporate entity whether incorporated in the Marshall Islands or elsewhere, the following information is required:

- (a) certified copy of the certificate of incorporation;
- (b) certified copy of the Articles of Association of the entity;
- (c) location of the registered office or registered agent of the corporate entity;
- (d) resolution of the Board of Directors authorizing the opening of the account and conferring authority on the person who will operate the account;
- (e) confirmation that the corporate entity has not been struck off the register or is not in the process of being wound up;
- (f) names and addresses of all officers and directors of the corporate entity;
- (g) names and addresses of the beneficial owners of the corporate entity, except a publicly traded company;
- (h) description and nature of the business including:
  - i. date of commencement of business;
  - ii. products or services provided;
  - iii. location of principal business;
- (i) purpose of the account and the potential parameters of the account including:
  - i. size, in the case of investment and custody accounts;
  - ii. balance ranges, in the case of deposit accounts;
  - iii. the expected transaction volume of the account;
- (j) written authority to obtain independent verification of any information provided;
- (k) written confirmation that all credits to the account are and will be beneficially owned by the financial institution and cash dealer holder;

(l) any other official document and other information reasonably capable of establishing the structural information of the corporate entity.

#### C. Verification of identity of partnerships or unincorporated businesses

Where a financial institution and cash dealer is required to verify the identity of partnerships or other unincorporated businesses, the following information is required:

- (a) verification of all partners or beneficial owners in accordance with the procedure for the verification of individuals;
- (b) copy of partnership agreement (if any) or other agreement establishing the unincorporated business;
- (c) description and nature of the business including:
  - i. date of commencement of business;
  - ii. products or services provided;
  - iii. location of principal place of business
- (d) purpose of the account and the potential parameters of the account including:
  - i. size in the case of investment and client accounts;
  - ii. balance ranges, in the case of deposit and client accounts;
  - iii. the expected transaction volume of the account;
- (e) mandate from the partnership or beneficial owner authorizing the opening of the account and conferring authority on those who will operate the account;
- (f) written confirmation that all credits to the account are and will be beneficially owned by the financial institution and cash dealer holder;
- (g) any documentary or other evidence reasonably capable of establishing the identity of the partners or beneficial owners.

#### D. Verification of facilities established by telephone or Internet

1. Where a request is made to a financial institution and cash dealer, by telephone, Internet, or written communication for a person, corporate entity, or partnership to become a financial institution and cash dealer holder, the financial institution and cash dealer shall verify the identity of that person, corporate entity, or partnership as provided in the relevant verification procedures in items A to C as appropriate.
2. Where the financial institution and cash dealer has obtained in writing confirmation from a foreign financial institution and cash dealer located in a country determined by the Banking Commissioner as having acceptable due diligence procedures, and that the other financial institution and cash dealer has verified the identity of the person or of the corporate entity specified in paragraph 1, no further verification of identity is necessary.

**TITLE 151.  
ANTI- TERRORISM LAWS**

**CHAPTER 1.**

**COUNTER-TERRORISM**

**ARRANGEMENT OF SECTIONS**

Section

PART I- Preliminary

§101. Short Title.

§102. Commencement.

§103. Purpose.

§104. Application etc.

§105. Interpretations.

PART II – PROHIBITION, PUNISHMENT.

§106. Prohibition of Terrorist Acts.

§107. Criminal Penalties, complicity ,limitation,  
Detention.

§108. Criminal Forfeiture.

§109. Liability of Corporations etc.

§110. Civil Penalties.

§111. Private Causes of action for terrorism.

§112. Injunctions.

PART III – MEASURES TO COMBAT

TERRORISM

§113. Duty to take measures.

§114. Extradition.

§115. Mutual Legal Assistance.

§116. Intelligence sharing.

§117. No asylum.

§118. Prevention.

§119. Transfer of persons.

PART IV – OFFENSES AGAINST  
INTERNATIONAL CONVENTIONS

Division 1-Suppression of financing of terrorism

§120. Financing of terrorism prohibited.

§121. Measures to suppress terrorism.

§122. Seizure & detention of suspicious funds.

Division 2- Cross-Border Movements of  
Terrorists

§123. Terrorists inadmissible.

§124. Report of Cross-Border movement.

Section

Division 3-Weapons of Mass Destruction

§125. Weapons of Mass destruction; offenses.

Division 4-Internationally Protected Persons  
§126. Internationally protected persons offenses.

Division 5-Hostage Taking  
§127. Hostage-taking; offenses.

Division 6- Terrorist Bombing  
§128. Terrorist Bombing; offenses.

Division 7 - Plastic Explosives  
§129. Prohibition on plastic explosives; offenses.

Division 8 - Safety of Civil Aviation  
§130. Civil Aviation; offenses.  
§131. Power to take reasonable measures.  
§132. Power to disembark certain passengers.  
§133. Power to deliver alleged offenders.  
§134. No liability for action taken.

Division 9 -safety of Maritime Navigation and Fixed  
Platform  
§135. Maritime Offenses.  
§136. Nuclear Material; offenses.  
§137. Other rights obligations and responsibilities not  
affected; no liability for action taken in good faith.  
§138. Resolution of Disputes.  
§139. Implementing Regulations.

1[Title formerly reserved, now assigned this subject matter]

## **15 MIRC Ch. 1 CHAPTER 1 - COUNTER - TERRORISM**

An Act for the prevention and combating of terrorism in the Republic of the Marshall Islands, for international cooperation to combat threats to international peace and security caused by terrorist acts, and for related purposes. [This Title was previously “Reserved” in the 98 Revision , assigned here to this Act. Section numbering style modified to conform to new Code format (Rev.2003)]

Commencement: November 11, 2003  
Source: P.L. 2002-65

### **PART I - PRELIMINARY**

#### **§101. Short Title.**

This Act may be cited as the Counter-Terrorism Act, 2002. [P.L. 2002-65, §1.]

#### **§102. Commencement.**

This Act shall come into effect on the date of certification in accordance with Article IV, section 21 of the Constitution. [P.L. 2002-65, §2.]

#### **§103. Purpose.**

The purpose of this Act is to implement the United Nations Security Council Resolution 1373 and other international obligations of the Republic of the Marshall Islands for the prevention,

repression and elimination of terrorism, and for related matters. [P.L. 2002-65, §3.]

**§104. Application, jurisdiction and enforcement.**

(1) The Attorney-General shall have primary enforcement authority for this Act.

(2) This Act shall apply in respect of any crime established by this Act when the offense is committed:

- (a) in the Marshall Islands;
- (b) by a citizen of the Marshall Islands;
- (c) on board an aircraft or ship:
  - (i) registered under the laws of the Marshall Islands at the time the offense was committed;
  - (ii) operating under or flying the Marshall Islands flag;
  - (iii) which lands in the territory of the Marshall Islands with the alleged offender on board;
  - (iv) leased or chartered without a crew to a lessee who has his principal place of business in the Marshall Islands, or who is a habitual resident of the Marshall Islands;
- (d) against or on board a fixed platform while it is located on the Marshall Islands' continental shelf;
- (3) This Act shall apply in respect of any crime established by this Act when the offense:
  - (a) was directed toward or resulted in the carrying out of a crime against a citizen of the Marshall Islands, or during the commission of which a citizen of the Marshall Islands was threatened, injured or killed;
  - (b) was directed towards or resulted in the carrying out of a crime against the government of the Marshall Islands or a facility, diplomatic or consular premises of the government of the Marshall Islands abroad;
  - (c) was directed towards or resulted in a crime committed in an attempt to compel the Marshall Islands to do or abstain from doing any act;
  - (d) was committed by a stateless person who has his or her habitual residence in the Marshall Islands.
- (4) Where a person is suspected to have engaged in terrorism and the alleged offender is present in the Marshall Islands, in a case where the Marshall Islands has jurisdiction, and the alleged offender is not extradited to a foreign country that has established jurisdiction over the offense or the alleged offender, the Attorney-General shall whether or not the offense was committed in the Marshall Islands, have authority to prosecute the person in accordance with any law that is for the time being in force in the Marshall Islands.
- (5) Application of any provisions of this Act, relating to or implementing the provisions of any international terrorism convention or protocol, shall conform to and meet the requirements of the particular convention or protocol, and shall be subject to the exclusions and jurisdictional requirements contained therein. [P.L. 2002-65, §4.]

**§105. Interpretations.**

In this Act, unless the contrary intention appears:

- (1) "alleged offender" means a person as to whom there is sufficient evidence to determine prima facie that such person has engaged in terrorism;
- (2) "Attorney-General" means the Attorney-General of the Marshall Islands, and includes the Deputy Attorney-General or any Assistant Attorney-General to whom the Attorney -General delegates authority to carry out the duties and responsibilities of the Attorney-General established under this Act;
- (3) "biological agent" means any micro-organism, virus, infectious substance, or biological product that may be engineered as a result of biotechnology, or any naturally occurring or bioengineered component of any such micro-organism, virus, infectious substance, or biological product, capable of causing:
  - (a) death, disease, or other biological malfunction in a human, an animal, a plant, or another living organism; or
  - (b) deterioration of food, water, equipment, supplies, or material of any kind; or
  - (c) deleterious alteration of the environment;
- (4) "biological weapon" means the following, together or separately, a:
  - (a) biological agent; and/or
  - (b) toxin; and/or
  - (c) delivery system;

that has been developed, produced, transferred, acquired, retained, or possessed for use as a weapon; provided, however, for purposes of this section, the term "for use as a weapon" does not include the development, production, transfer, acquisition, retention, or possession of any biological agent, toxin or delivery system for prophylactic, protective, or other peaceful purposes;

(5) "chemical weapon" means, together or separately:

(a) A toxic chemical and its precursors, except where intended for a purpose not prohibited by law as long as the type and quantity is consistent with such a purpose;

(b) A munition or device, specifically designed to cause death or other harm through toxic properties of those toxic chemicals specified in paragraph (a), which would be released as a result of the employment of such munition or device;

(c) Any equipment specifically designed for use directly in connection with the employment of munitions or devices specified in paragraph (b);

(6) "crime(s) established by this Act" means and includes:

(a) any crime punishable under Part IV of this Act; or

(b) any act or activity punishable under subsection 107 (3) of this Act;

(7) "delivery system" means, with respect to biological weapons:

(a) any apparatus, equipment, device, or means of delivery specifically designed to deliver or disseminate a biological agent, toxin, or vector; or

(b) any vector;

(8) "destructive device" means any explosive, incendiary, poison gas, or projectile-expelling weapon, capable of causing serious bodily injury or death, that has been developed, produced, transferred, acquired, retained, or possessed for use as a weapon, or any combination of parts or pieces thereof which could be used or converted for such purposes;

(9) "engage(s) in" with respect to terrorist acts, terrorism offenses and terrorism, means and includes, in an individual capacity or as a member of an organization:

(a) to perpetrate, commit or carry out, or to incite to commit or carry out; or

(b) to threaten, attempt, solicit, or conspire to carryout or commit; or

(c) to prepare or plan; or

(d) to gather information on potential targets for; or

(e) to solicit, collect or provide funds or other things of value, with the knowledge or intention that the funds or other things of value will be used:

(i) for terrorism; or

(ii) by a terrorist organization;

(f) to solicit, recruit, or train any person:

(i) to engage in terrorism;

(ii) to engage in conduct otherwise described in this section; or

(iii) for membership in a terrorist organization;

(g) to commit or carryout an act that the actor knows, or reasonably should know, affords material support, including a safe house, transportation, communications, funds, transfer of funds or other material benefit, false documentation or identification, weapons (including, without limitation, chemical, biological, or radiological weapons), explosives, or training:

(i) for terrorism; or

(ii) to any individual who the actor knows, or reasonably should know, engages in terrorism; or

(iii) for a terrorist organization.

(10) "fixed platform" means an artificial island, installation or structure permanently attached to the seabed for the purpose of exploration or exploitation of resources or for other economic purposes;

(11) "foreign country" means

(a) any country other than the Marshall Islands;

(b) every constituent part of such country, including a territory, dependency, or protectorate which administers its own laws;

(12) "foreign national" means a natural person who is a citizen of a country other than the Marshall Islands;

(13) "funds" means property and assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such property or assets, including, but not limited to, bank credits, travelers checks, bank checks, money orders, shares, securities, bonds, debt instruments, drafts, letters of credit, and currency;

(14) "in flight" means, with respect to aircraft, at any time from the moment when all the external doors are closed following embarkation until the moment when any such door is opened for disembarkation; provided, however, in the case of a forced landing, the flight shall be deemed to continue until the competent authorities take over the responsibility for the aircraft and for persons and property on board;

(15) "in service" means and includes, with respect to aircraft, from the beginning of the preflight preparation of the aircraft by ground personnel or by the crew for a specific flight until twenty-four hours after any landing; and, the period of service shall, in any event, extend for the entire period during which the aircraft is in flight;

(16) "international terrorism conventions" includes the conventions that are referred to in the Schedule to this Act, or any other convention that the Minister may, after consultation with the Minister of Foreign Affairs, by public notice in writing declare a convention for the purposes of this Act;

(17) "internationally protected person" means and includes:

(a) a Head of State, or any member of a collegial body performing the functions of a Head of State under the constitution of the State concerned, a Head of Government or a Minister of Foreign Affairs, whenever any such person is in a foreign State, as well as members of such person's family who accompany him or her;

(b) any representative or official of the Marshall Islands or of a foreign country, or any official or other agent of an international organization of an intergovernmental character who, at the time when and in the place where a crime against such person, the person's official premises, private accommodation or means of transport is committed, is entitled pursuant to international law to special protection from any attack on his or her person, freedom or dignity, as well as members of such person's family forming part of the person's household;

(18) "infrastructure facility" means any publicly or privately owned facility providing or distributing services for the benefit of the public, such as water, sewage, energy, fuel or communications;

(19) "key component of a binary or multi-component chemical system" means, with respect to precursors and chemical weapons, the precursor that plays the most important role in determining the toxic properties of the final product and reacts rapidly with other chemicals in the binary or multi-component system;

(20) "Marshall Islands" means the Republic of the Marshall Islands, and the marine areas, the air space above the territory of the Marshall Islands and includes the government of the Marshall Islands;

(21) "Minister" means the Minister of Justice of the Marshall Islands;

(22) "Nuclear material" has the same meaning as defined in the Convention on Physical Protection of Nuclear Material

(23) "person" means and includes both natural and legal persons and any foreign government or nation or any agency, instrumentality or political subdivision of any such government or nation, whether or not it is engaging in legal activities or is operating legally and in a lawful manner;

(24) "place of public use" means those parts of any building, land, street, waterway or other location that are accessible or open to members of the public, whether continuously, periodically or occasionally, and encompasses any commercial, business, cultural, historical, educational, religious, governmental, entertainment, recreational or similar place that is so accessible or open to the public;

(25) "plastic explosive" means an explosive material in flexible or elastic sheet form formulated with one or more high explosives which in their pure form has a vapor pressure less than 10<sup>-4</sup> Pa at a temperature of 25 degrees Celcius, is formulated with a binder material, and is as a mixture malleable or flexible at normal room temperature;

(26) "precursor" means, with respect to chemical weapons, any chemical reactant that takes part at any stage in the production by whatever method of a toxic chemical, and includes any key component of a binary or multi-component chemical system;

- (27) "proceeds" means any funds derived from or obtained, directly or indirectly, through or from terrorism;
- (28) "public transportation system" means all facilities, conveyances and instrumentalities, whether publicly or privately owned, that are used in or for publicly available services for the transportation of persons or cargo;
- (29) "purpose not prohibited by law" means, with respect to chemical weapons:
- (a) any peaceful purpose related to an industrial, agricultural, research, medical, or pharmaceutical activity or other activity;
  - (b) any purpose directly related to protection against toxic chemicals and to protection against chemical weapons;
  - (c) any military purpose of the Marshall Islands that is not connected with the use of a chemical weapon or that is not dependent on the use of the toxic or poisonous properties of the chemical weapon to cause death or other harm;
  - (d) any law enforcement purpose, including any domestic riot control purpose;
- (30) "ship" means a vessel of any type whatsoever not permanently attached to the sea-bed, including dynamically supported craft, submersibles, or any other floating craft;
- (31) "serious bodily injury" means physical pain, illness or any impairment of physical condition that creates a substantial risk of death or which causes serious, permanent disfigurement, or protracted loss or impairment of the function of any bodily member or organ;
- (32) "serious offense" means any offense, for which the maximum penalty is imprisonment for a period of not less than one year;
- (33) "state or government facility" means any permanent or temporary facility or conveyance that is used or occupied by representatives of a country, members of government, the legislature or the judiciary or by officials or employees of a country or any other public authority or entity or by employees or officials of an intergovernmental organization in connection with their official duties;
- (34) "substantial property damage" means damage in an amount exceeding \$10,000;
- (35) "terrorism" means and includes terrorism offenses and terrorist acts;
- (36) "terrorism offense" means:
- (a) any crime established by this Act;
  - (b) any crime established by the laws of the Marshall Islands and declared to be a terrorism offense by the Nitijela;
  - (c) any crime established by an international terrorism convention;
  - (d) any crime recognized under international humanitarian law as a terrorism offense; and (e) any crime established under the law of a foreign State, where such crime, if committed in the Marshall Islands, would constitute a terrorism offense under the laws of the Marshall Islands ;
- (37) "terrorist" means a person who engages in terrorism;
- (38) "terrorist act" means and includes any act that is intended, or by its nature or context can be reasonably regarded as intended, to intimidate the public or any portion of the public, or to compel a government or an international or regional organization to do or refrain from doing any act, and:
- (a) involves the seizing or detaining, and threatening to kill, injure, harm, or continue to detain, another person;
  - (b) endangers the life of any person;
  - (c) creates a risk to the health or the safety of the public, or to any portion of the public;
  - (d) endangers the national security or national defense of any country;
  - (e) involves substantial damage to property;
  - (f) involves the hijacking, seizure or sabotage of any conveyance (including an aircraft, vessel, ship, or vehicle), or of any fixed platform attached to the continental shelf;
  - (g) involves any act that is designed to disrupt or destroy an electronic system, including, without limitation:
    - (i) an information system;
    - (ii) a telecommunications system;
    - (iii) a financial system;
    - (iv) a system used for the delivery of essential government services;

- (v) a system used for, or by, an essential public utility;
- (vi) a system used for, or by, a transport system;
- (h) involves any act that is designed to disrupt the provision of essential emergency services such as the police, civil defense and medical services;
- (39) "terrorist organization" means a group composed of two or more persons, whether organized or not, that engages in terrorism;
- (40) "toxic chemical" means any chemical which through its chemical action on life processes can cause death, temporary incapacitation or permanent harm to humans or animals, and includes all such chemicals, regardless of their origin or of their method of production, and regardless of whether they are produced in facilities, in munitions or elsewhere;
- (41) "toxin" means the toxic material of plants, animals, microorganisms, viruses, fungi, or infectious substances, or a recombinant molecule, whatever its origin or method of production, including:
  - (a) any poisonous substance or biological product that may be engineered as a result of biotechnology produced by a living organism; or
  - (b) any poisonous isomer or biological product, homolog, or derivative of such a substance;
- (42) "vector" means, with respect to delivery systems and biological weapons, a living organism, or molecule, including a recombinant molecule, or biological product that may be engineered as a result of biotechnology, capable of carrying a biological agent or toxin to a host; (43) "weapon of mass destruction" means, any:
  - (a) destructive device;
  - (b) chemical weapon or any other weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors;
  - (c) biological weapon, or any other weapon involving a disease organism;
  - (d) nuclear material, weapon or device, and any other weapon that is designed to release radiation or radioactivity at a level dangerous to human life. [P.L. 2002-65, §5.]

## **PART II-PROHIBITION, PUNISHMENT OF TERRORIST ACTIVITIES**

### **§106. Prohibition of terrorist acts.**

Any person who knowingly, directly or indirectly, engages in terrorist act is guilty of an offence against this Act, and shall unless otherwise punishable under any other section be punishable, under section 107 of this Act. [P.L. 2002-65, §6.]

### **§107. Criminal penalties; criminal complicity and inchoate offenses; no time limitation on prosecution; detention of suspected terrorists.**

- (1) Unless otherwise provided, any person convicted of an offence against this Act ;
  - (a) shall, where no other punishment is prescribed in respect of that offense, be punishable by a term of not less than 30 years and not more than life imprisonment, or a fine of not more than \$100,000,000.00; or both.
  - (b) shall not be entitled to probation for an offense committed or have the term of imprisonment imposed on him run concurrently with any other term of imprisonment; and (c) shall not be entitled to bail pending his trial or his appeal against conviction for the offense.
- (2) In lieu of the amount of the fine otherwise authorized by this Act, and in addition to any term of imprisonment, a defendant who derived profits or other proceeds from a crime established by this Act may be liable to a fine of not more than twice the gross profits or other proceeds, where the profits or proceeds from the offense exceed the maximum assessable fine.
- (3) A person commits a crime, punishable under subsection (1), if that person knowingly:
  - (a) attempts, conspires, or threatens to commit;
  - (b) participates as an accomplice in;
  - (c) organizes or directs others to commit;
  - (d) contributes to the commission of;
 any crime established by this Act.
- (4) Notwithstanding any provision of any other law, statute of limitation shall not apply in respect of a crime established under this Act.

(5) Where there is reasonable ground to believe that detention of any person is necessary for the purpose of preventing such person from engaging in acts of terrorism; or to prevent any person from interfering with an investigation relating to suspected terrorism, any law enforcement officer, immigration officer, or customs official in the Marshall Islands shall have the powers to detain such person for a period of 48 hours for purposes of investigation; provided, however, such period of detention may be extended by court order for an additional 7 days, without the filing of criminal charges against such person. (6) The court, in imposing sentence on any person convicted of a terrorism offense, shall order, in addition to any other sentence imposed, that the person forfeit to the Marshall Islands all property described in section 108. [P.L. 2002-65, §7.]

#### **§108. Criminal forfeiture.**

(1) Any person convicted of a terrorism offense shall be liable to forfeit to the Marshall Islands, irrespective of any other provision of law:

(a) any property, real or personal, owned, possessed, or used by a person involved in the offense; (b) any property constituting, or derived from, and proceeds the person obtained, directly or indirectly, as the result of such offense; and (c) any of the property used in any manner or part, to commit, or to facilitate the commission of, such offense;

(2) Weapons of mass destruction, plastic explosives, and nuclear material shall be seized, confiscated and forfeited to the Marshall Islands; and the Attorney-General shall provide for their destruction or other appropriate disposition.

(3) For the purposes of forfeiture proceedings under this section, a temporary restraining order and seizure warrant may be entered upon application of the Attorney-General without notice or opportunity for a hearing when an information or complaint has not yet been filed with respect to the property, where there is probable cause to believe that the property with respect to which the order is sought would, in the event of conviction, be subject to forfeiture under this section and exigent circumstances exist that place the life or health of any person in danger.

(4) The provisions of this section shall be implemented without prejudice to the rights of third parties acting in good faith.

(5) The owner or possessor of any property seized under this section shall be liable to the Marshall Islands for any expenses incurred incident to the seizure, including any expenses relating to the handling, storage, transportation, and destruction or other disposition of the seized property.

[P.L. 2002-65, §8.]

#### **§109. Liability of corporations and other legal persons.**

(1) Legal persons, including any foreign government or nation or any agency, instrumentality or political subdivision of any such government or nation, shall be liable in the same manner and to the same extent as any natural person for any terrorism offense.

(2) The maximum assessable fine for legal persons shall be increased by ten times the amount assessable in the case of a natural person.

(3) Where in proceedings for a violation of this Act it is necessary to establish the state of mind of a corporation or other legal person, it is sufficient to show that a director, officer or agent who engaged in the conduct within the scope of his or her actual or apparent authority had that state of mind.

(4) Any conduct engaged in by:

(a) a director, officer or agent of a corporation or other legal person within the scope of his or her actual or apparent authority; or

(b) any other person at the direction or with the consent or agreement (whether express or implied) of a director, officer or agent of the corporation or legal person, where the giving of such direction, consent or agreement is within the scope of the actual or apparent authority of the director, officer or agent; shall be deemed, for the purposes of this Act, to have also been engaged in by the corporation or legal person. [P.L. 2002-65, §9.]

#### **§110. Civil penalties; reimbursement.**

- (1) The Attorney-General may bring a civil action in the Marshall Islands against any person who commits a crime established by this Act, and upon proof by a preponderance of the evidence that such person committed the offense, the person shall be subject to pay a civil penalty in an amount not exceeding \$25,000,000 for each such offense.
- (2) The imposition of a civil penalty under subsection (1) shall not preclude any other criminal or civil statutory, common law, or administrative remedy, which is available by law to the Marshall Islands or any other person.
- (3) The court shall order any person convicted of a crime established by this Act to reimburse the Marshall Islands for any expenses incurred by the Marshall Islands incident to investigation and prosecution for the offense, including, without limitation, the seizure, storage, handling, transportation, and destruction or other disposition of any property that was seized in connection with an investigation of the commission of the offense by that person.
- (4) A person ordered to reimburse the Marshall Islands pursuant to subsection (3) shall be jointly and severally liable for such expenses with each other person, if any, who is ordered under subsection (3) to reimburse the Marshall Islands for the same expenses. [P.L. 2002-65, §10.]

**§111. Private causes of action for terrorism.**

- (1) Any citizen of the Marshall Islands injured in his or her person, property, or business by reason of terrorism, or his or her estate, survivors, or heirs, may sue therefor in the High Court of the Marshall Islands and shall be entitled to recover threefold the damages he or she has sustained, and the cost of the suit, including attorney's fees.
- (2) A final judgment or decree rendered in favor of the Marshall Islands in any criminal proceeding relating to a terrorism offense shall estop the defendant from denying the essential allegations of the criminal offense in any subsequent civil proceeding under this section.
- (3) A final judgment or decree rendered in favor of any foreign country in any criminal proceeding relating to a terrorism offense shall, to the extent that such judgment or decree may be accorded full faith and credit under the law of the Marshall Islands, estop the defendant from denying the essential allegations of the criminal offense in any subsequent civil proceeding under this section.
- (4) No action shall be maintained under subsection (1) for injury or loss by reason of an act of war.
- (5) No action shall be maintained under subsection (1) against the Marshall Islands, an agency of the Marshall Islands, or an officer or employee of the Marshall Islands or any agency thereof, acting within his or her official capacity or under color of legal authority. [P.L. 2002-65, §11.]

**§112. Injunctions.**

The Marshall Islands may obtain in a civil action an injunction against:

- (1) any conduct prohibited by this Act;
- (2) the development, production, stockpiling, transferring, acquisition, retention, or possession of any:
  - (a) biological agent, toxin, or delivery system of a type or in a quantity that under the circumstances has no apparent justification for prophylactic, protective, or other peaceful purposes;
  - (b) toxic chemical, or precursor, of a type or in a quantity that under the circumstances has no apparent justification for a purpose not prohibited by law or the United Nations Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction. [P.L. 2002-65, §12.]

**PART III - MEASURES TO COMBAT TERRORISM**

**§113. Duty to take measures.**

The Attorney-General shall take appropriate measures, in accordance with the Constitution and the laws of the Marshall Islands:

- (1) as may be necessary to establish jurisdiction over and prosecute in the Marshall Islands any crime established by this Act;
- (2) to investigate terrorism, and upon receiving information that an alleged offender may be present in the Marshall Islands, take the person into custody and take other appropriate measures so as to ensure the alleged offender's presence for the purpose of prosecution;

- (3) to take into custody and extradite any alleged offender who is present in the Marshall Islands, and who is subject to arrest and detention for purposes of extradition pursuant to any law in force in the Marshall Islands;
- (4) to provide early warning and furnish any relevant information in the possession of Marshall Islands to those countries which the Attorney-General believes would have jurisdiction, where there is reason to believe that a terrorism offense has been or will be committed;
- (5) to identify, detect, freeze, seize, and obtain forfeiture of any funds used or allocated for the purpose of committing any terrorism offense as well as the proceeds derived from such offenses;
- (6) to implement, conform to, and abide by the express requirements of any international terrorism convention to which this Act relates, and to ensure that any person regarding whom the measures referred to in this section are being taken shall be afforded the protections to which such person is expressly entitled under the relevant international terrorism convention;
- (7) to prevent the cross border movement of terrorists, and to track the movement of such persons, and of persons who are members of terrorist organizations;
- (8) to prevent the admission terrorists into the Marshall Islands, except as may be necessary to secure that person's presence for the purpose of extradition or prosecution for a terrorism offense;
- (9) to prevent attacks on the person, freedom, or dignity of internationally protected persons;
- (10) to prevent the movement into or out of the territory of the Marshall Islands, of unauthorized plastic explosives (especially, unmarked plastic explosives), and to prevent their manufacture;
- (11) to provide timely notification, directly or through the depositary of the relevant international terrorism convention, when the Marshall Islands has taken a person into custody or has taken other measures with respect to any person pursuant to this section:
  - (a) to the appropriate authorities of the country of which the detained person is a citizen or national, if the person is not a citizen or national of the Marshall Islands;
  - (b) to the States Party to the relevant international terrorism convention that have established jurisdiction over the person or the offense in question in accordance with the convention, and to the depositary of the convention;
  - (c) to the country of registration of the aircraft, in cases involving aircraft;
  - (d) to the country whose flag the ship was flying, in cases involving ships;
  - (e) to any other foreign country or interested person, if the Minister considers it advisable; of the fact that such person is in custody and of the circumstances which warrant that such person is in custody and of the circumstances which warrant that person's detention. [P.L. 2002-65, §13.]

#### **§114. Extradition.**

- (1) Terrorism offenses are hereby declared to be extraditable offenses.
- (2) Extradition for terrorism offenses shall be carried out pursuant to and in accordance with any law for the time being in force in the Marshall Islands.
- (3) For the purpose of extradition, a terrorism offense shall be treated, as if it had been committed not only in the place in which it occurred but also in the territory of any country Party to an international terrorism convention that is required to establish jurisdiction over the offense in accordance with that convention. [P.L. 2002-65, §14.]

#### **§115. Mutual legal assistance.**

- (1) The Attorney-General may make a request on behalf of the Marshall Islands to the appropriate authority of a foreign country, or grant requests of a foreign country, for legal assistance in any investigation or proceeding relating to terrorism, or a terrorist organization.
- (2) Mutual legal assistance provided under this Act shall be carried-out pursuant to and in accordance with the Mutual Assistance in Criminal Matters Act, 2002. [P.L. 2002-65, §15.]

#### **§116. Intelligence sharing.**

The Attorney-General, and other law enforcement authorities and officers of the Marshall Islands designated by the Attorney General shall have the authority to share and disclose intelligence information relating to terrorism, terrorist organizations, transnational organized crime, illicit drugs,

money-laundering, illegal arms-trafficking, and illegal movement of nuclear, chemical, biological and other potentially deadly materials, and to provide early warning of such matters to the competent law enforcement authorities of:

- (1) any foreign country, that is a Party to an international terrorism convention in respect of which the Marshall Islands is also a Party;
- (2) any foreign country that is a member of the Pacific Islands Forum;
- (3) the United States, in accordance with the duties and responsibilities of the Marshall Islands under the Compact of Free Association with the United States;
- (4) any other foreign country that is a member of the United Nations. [P.L. 2002-65, §16.]

#### **§117. No asylum.**

The Republic of the Marshall Islands shall not grant refugee status or provide asylum or safe haven to any terrorist, or to any alleged offender. [P.L. 2002-65, §17.]

#### **§118. Prevention.**

(1) The Marshall Islands shall cooperate with the competent authorities of the United States and other members of the United Nations and the Pacific Islands Forum in the prevention of terrorism by taking all practicable measures to prevent and counter preparations in the Marshall Islands for the perpetration of terrorism within or outside the territory of the Marshall Islands, including measures to prohibit illegal activities of persons and organizations that knowingly encourage, instigate, organize, finance, or engage in terrorism.

(2) The Marshall Islands shall cooperate in the prevention of terrorism by exchanging information to provide early warning of possible terrorism, in particular by:

(a) establishing and maintaining channels of communication to facilitate the secure and rapid exchange of information concerning all aspects of terrorism and terrorist organizations;

(b) exchanging entry and exit data and information for ports of entry into the Marshall Islands, including airports and seaports, and coordinating administrative and other measures taken, as appropriate, to prevent the cross border movement of terrorists, and to track their movement and the movement of members of terrorist organizations; (c) conducting inquiries, with respect to terrorists and members of terrorist organizations, concerning:

(i) the identity, whereabouts and activities of persons in respect of whom reasonable suspicion exists that they engage in terrorism or are members of a terrorist organization;

(ii) the movement of funds linked to persons who engage in terrorism or are members of a terrorist organization; and

(d) participation in research and development and exchange of information regarding methods of detection of cross border movement of terrorists and members of terrorist organizations, including detection of forged or falsified travel documents, traffic in arms, explosives, illicit drugs, contraband, or sensitive materials, and cross-border movement of nuclear, chemical, biological and other potentially deadly materials, or use of communications technologies by terrorist groups. [P.L. 2002-65, §18.]

#### **§119. Transfer of persons.**

(1) Transfer of any person who is being detained or is serving a sentence in the territory of the Marshall Islands or a foreign country, whose presence is requested for purposes of identification, testimony or otherwise providing assistance in obtaining evidence for the investigation or prosecution of a terrorism offense, shall be authorized and allowed, where the person consents to the transfer, and the countries agree on the conditions.

(2) Transfer of persons referred to in subsection (1) shall be carried-out pursuant to and in accordance with requirements of any law that is for the time being in force in the Marshall Islands for convicted persons, whether or not the person to be transferred has already been convicted of an offense. [P.L. 2002-65, §19.]

### **PART IV - OFFENSES AGAINST INTERNATIONAL TERRORISM CONVENTIONS**

## **Division 1. Suppression of Financing of Terrorism**

### **§120. Financing of terrorism prohibited.**

(1) Any person who knowingly, by any means, directly or indirectly, solicits, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part:

- (a) for terrorism;
  - (b) for the benefit of persons who engage in terrorism, or for the benefit of entities owned or controlled, directly or indirectly, by persons who engage in terrorism; or
  - (c) for the benefit of persons and entities acting on behalf of or at the direction of any person referred to in subsection 1(b); commits a crime punishable by the penalties established by section 107 (1) (a) of this Act.
- (2) For an act to constitute an offense under this section it shall not be necessary that the funds were actually used to commit or carry out a terrorism offense, or terrorist act.

(3) Citizens and nationals of the Marshall Islands and any persons and entities within the Marshall Islands are prohibited from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, to any person referred to in subsection 1(b) or 1(c). [P.L. 2002-65, §20.]

### **§121. Measures to suppress financing of terrorism.**

(1) Any person, that provides a service for the transmission of money or value, including transmission through an alternative remittance system or informal money or value transfer system or network, or the agent of such person, shall be required to be licensed by the competent authorities of the Marshall Islands, and shall be subject to the disclosure requirements prescribed by the relevant authorities in relation to that type of business.

(2) All credit and financial institutions and all persons, and their agents, that provide a service for the transmission of money or value by wire transfer, shall include accurate and meaningful originator information (including name, address and account number) on funds transfers and related messages that are sent, such information to remain with the transfer or related message through the payment chain.

(3) No corporation, business, enterprise, partnership, association, or entity, shall be granted charitable or non-profit status in the Marshall Islands where there are reasonable grounds to believe that any funds solicited, collected, held, used, or owned by such corporation, business, enterprise, partnership, association, or entity, may be diverted to a terrorist or a terrorist organization. [P.L. 2002-65, §21.]

### **§122. Seizure and detention of suspicious funds.**

(1) Any law enforcement officer or customs official of the Marshall Islands may seize and, in accordance with this section detain, any funds, that the officer or official has probable cause to believe were derived from or intended for terrorism, including, without limitation, funds being imported into or exported from the Marshall Islands.

(2) Funds of, or intended for, terrorist organizations shall be frozen, seized, and in accordance with this section detained, where the organization has been designated as a terrorist organization by the United Nations Security Council, or by the Minister pursuant to regulations promulgated pursuant to this Act, or where there is probable cause to believe that the entity involved is a terrorist organization.

(3) Funds detained under subsection (1) or (2) shall not be detained for more than 48 hours after seizure, unless a judge of the High Court grants an order of continued detention for a period not exceeding 3 months from the date of seizure, upon being satisfied that:

(a) there is probable cause to believe that the funds were derived from terrorism, or are intended by any person for use in the commission of a terrorism offense or for a terrorist act; and

(b) the continued detention is justified while:

(i) its origin or derivation is further investigated; or

(ii) consideration is given to the institution in the Marshall Islands or elsewhere of criminal proceedings against any person for an offense with which the funds are connected; provided, however, upon request by the person from whom the funds were seized and detained, the court shall grant a hearing before entering an order of continued detention.

- (4) A judge of the High Court may subsequently order after hearing, with notice to all parties concerned, the continued detention of the funds if satisfied of the matters mentioned in subsection (3), but the total period of detention shall not exceed 2 years from the date of the order.
- (5) Subject to subsection (6), funds detained under this section may be released in whole or in part to the person on whose behalf the funds were imported or exported:
  - (a) by order of a judge of the High Court that continued detention is no longer justified, upon application by or on behalf of that person and after considering any views of the Attorney-General to the contrary; or
  - (b) by an authorized officer or customs official, if satisfied that their continued detention is no longer justified.
- (6) No funds detained under this section shall be released where:
  - (a) an application is made under this Act or other laws of the Marshall Islands for the purpose of:
    - (i) the confiscation and forfeiture of the whole or any part of the funds; or
    - (ii) their restraint pending determination of liability to confiscation and forfeiture; or
  - (b) proceedings are instituted in the Marshall Islands or elsewhere against any person for a terrorism offense with which the funds are connected; unless and until the proceedings relating to the relevant application or the proceedings for the offense, as the case may be, have been concluded.
- (7) Funds seized pursuant to this section shall be subject to confiscation and forfeiture pursuant to section 108 of this Act. [P.L. 2002-65, §22.]

## **Division 2. Cross-Border Movement of Terrorists**

### **§123. Terrorists inadmissible.**

- (1) The following persons shall be considered inadmissible to the Marshall Islands for purposes of immigration, or under a temporary visa of any kind, or otherwise, except for the purpose of prosecution or extradition for a terrorist offense:
  - (a) A foreign national:
    - (i) convicted of a terrorism offense; or
    - (ii) who admits to having engaged in terrorism; or
    - (iii) as to whom there is probable cause to believe such person has engaged in terrorism;
    - (iv) who the Attorney-General knows, or has reasonable ground to believe, is engaged in or is likely after entry, to engage in terrorism; or
    - (v) who has used his or her position of prominence within any country to endorse or espouse terrorism, or to persuade others to support terrorism or a terrorist organization, in a way that the Attorney-General has determined undermines the efforts of the Marshall Islands to reduce or eliminate terrorism;
    - (vi) who is a representative of a terrorist organization, specified as such in regulations promulgated by the Minister or designated as a terrorist organization by the United Nations Security Council; or
    - (vii) who is a representative of a political, social or other similar group whose public endorsement of terrorism, or terrorist organizations, the Attorney-General has determined undermines the efforts of the Marshall Islands to reduce or eliminate terrorism;
  - (b) A foreign national who the Minister, after consultation with the Attorney-General, determines has been associated with a terrorist organization or terrorism and intends while in the Marshall Islands to engage solely, principally, or incidentally in activities that could endanger the welfare, safety, or security of the Marshall Islands.
- (2) A person who is the spouse or the child of an foreign national who is inadmissible under subsection (1), shall also be inadmissible, if the activity causing the foreign national to be found inadmissible occurred within the last 5 years.
- (3) Except as otherwise provided in this section, foreign nationals who are inadmissible under this section, shall be ineligible to be admitted to the Marshall Islands for any purpose, except, when necessary for the purposes of prosecution or extradition for a terrorism offense. [P.L. 2002-65, §23.]

### **§124. Reports of cross-border movement of terrorists.**

All airlines, ships, and other entities that provide transportation, conveyance or freight services to and from the Marshall Islands shall be authorized and required to immediately report to the Attorney General

through disclosure of passenger manifests and any other available means, the intended movement of suspected terrorists into or out of the Marshall Islands, and information regarding possible forged or falsified travel documents, traffic in arms, explosives, illicit drugs, contraband, or sensitive materials, and cross-border movement of nuclear, chemical, biological and other potentially deadly materials. [P.L. 2002-65, §24.]

### **Division 3. Weapons of Mass Destruction**

#### **§125. Weapons of mass destruction offenses.**

(1) Except as authorized by the Cabinet, any person who;

(a) knowingly, directly or indirectly, develops, produces, ships, transports, transfers, receives, acquires, retains, possesses, imports, exports, or manufactures a weapon of mass destruction, commits a crime punishable by the penalties established by section 107(1) (a) of this Act; (b) undertakes the Act referred to in subsection (1) with the intention of engaging in terrorism or with knowledge that the weapon of mass destruction is intended to be used for terrorism, ommits an offense punishable by a term of not less than 30 years and not more than life imprisonment, or fine of not more than \$100,000,000.00; or both; (c) uses or deploys a weapon of mass destruction, commits an offense punishable by a term of not less than 30 years and not more than life imprisonment, or fine of not more than \$100,000,000.00; or both. [P.L. 2002-65, §25.]

### **Division 4. Internationally Protected Persons**

#### **§126. Internationally protected persons offenses.**

(1) Any person who knowingly, by any means, directly or indirectly, perpetrates: (a) a murder, kidnaping or other attack upon the person or liberty of an internationally protected person; (b) a violent attack upon the official premises, the private accommodation or the means of transport of an internationally protected person, likely to endanger the person or his or her liberty; commits a crime punishable by the penalties established by section 107 of this Act. [P.L. 2002-65, §26.]

### **Division 5. Hostage-Taking**

#### **§127. Hostage-taking offenses.**

Any person who knowingly, directly or indirectly, seizes or detains or threatens to kill, or injure another person (the "hostage") in order to compel a third party, namely, the Marshall Islands, a foreign country, an international intergovernmental organization, a natural or legal person, or a group of persons, to do or abstain from doing any act as an explicit or implicit condition for the release of the hostage, commits a crime punishable under section 107 of this Act. [P.L. 2002-65, §27.]

### **Division 6. Terrorist Bombing**

#### **§128. Terrorist bombing offenses.**

Any person who knowingly, directly or indirectly, delivers, places, discharges, deploys, or detonates any explosive or incendiary weapon or lethal device that is designed, or has the capability, to cause death, serious bodily injury, or substantial property damage in, into or against a place of public use, a State or government facility, a public transportation system or an infrastructure facility:

(1) with the intent to cause death or serious bodily injury; or

(2) with the intent to cause extensive destruction of such a place, facility or system, where such destruction results in or is likely to result in major economic loss; commits a crime punishable by a term of a term of not less than 30 years and not more than life imprisonment, or fine of not more than \$1,000,000,000.00; or both. [P.L. 2002-65, §28.]

### **Division 7. Plastic Explosives**

#### **§129. Prohibition on plastic explosives; offenses.**

(1) Unless expressly authorized by the Cabinet, plastic explosives shall be prohibited in the Marshall Islands; provided, however, where authorized by the Cabinet for legitimate needs, plastic explosives must contain a detection agent, as defined by the Convention on the Marking of Plastic Explosives for the Purpose of Detection, and as described in the "Technical Annex" to that convention.

(2) Any person who knowingly, by any means, directly or indirectly, develops, produces, ships, transports, transfers, receives, acquires, retains, possesses, manufactures, imports, or exports an unauthorized plastic explosive commits a crime punishable by a minimum of 10 years imprisonment and a maximum fine of US \$50,000,000.00.

(3) Where a person engages in the act referred to in subsection (2) with the intent to engage in terrorism, the person commits an offense and shall upon conviction be punishable under section 107 (1) (a).

(4) Where a person referred to in subsection (2) uses or deploys the plastic explosives, the person shall be guilty of an offense and shall upon conviction be punishable by a term of not less than 30 years and not more than life imprisonment, or a fine of not more than \$1,000,000,000.00 or both. [P.L. 2002-65, §29.]

## **Division 8. Safety of Civil Aviation**

### **§130. Civil aviation offenses.**

In any airspace or territory where any international civil aviation convention or protocol referred to in paragraphs 1, 2, 3, and 7 of the Schedule would apply, any person who knowingly, directly or indirectly:

(1) performs an act of violence against a person on board an aircraft in flight if that act is likely to endanger the safety of that aircraft; or

(2) by force or threat thereof, or by any other form of intimidation, seizes or exercises control of an aircraft in flight;

(3) destroys an aircraft in service or causes damage to such an aircraft which renders it incapable of flight or which is likely to endanger its safety in flight; or

(4) places or causes to be placed on an aircraft in service, by any means whatsoever, a device or substance which is likely to destroy that aircraft, or to cause damage to it which renders it incapable of flight, or to cause damage to it which is likely to endanger its safety in flight; or

(5) destroys or damages air navigation facilities used in international air navigation, or interferes with their operation, if any such act is likely to endanger the safety of aircraft in flight; or

(6) communicates information which the person knows to be false, thereby endangering the safety of an aircraft in flight;

(7) using any device, substance or weapon:

(a) performs an act of violence against a person at an airport serving international civil aviation, which causes or is likely to cause serious injury or death; or

(b) destroys or seriously damages the facilities of an airport serving international civil aviation or aircraft not in service located thereon or disrupts the services of the airport; commits an offense punishable under section 107 (1) (a) ; provide however that where in committing the offense, the person uses or deploys a weapon of mass destruction, the person shall be liable to a fine of up to \$1,000,000,000.00. [P.L. 2002-65, §30.]

### **§131. Power to take reasonable measures.**

(1) The aircraft commander may, when he or she has reasonable grounds to believe that a person has committed, or is about to commit, on board the aircraft:

(a) a criminal offense; or

(b) an act which, whether or not it is a criminal offense, may or does jeopardize the safety of an aircraft or of persons or property therein, or which jeopardizes good order and discipline on board an aircraft; impose upon such person reasonable measures, including restraint, which are necessary:

(c) to protect the safety of the aircraft, or of persons or property therein; or

(d) to maintain good order and discipline on board; or

(e) to enable the aircraft commander to deliver such person to competent authorities or to disembark the person in accordance with the provisions of this chapter.

(2) The aircraft commander may require or authorize the assistance of other crew members and may request or authorize, but not require, the assistance of passengers to restrain any person whom the aircraft commander is entitled to restrain.

(3) Any crew member or passenger may also take reasonable preventive measures without such authorization when the crew member or passenger has reasonable grounds to believe that such action is immediately necessary to protect the safety of the aircraft, or of persons or property therein.

(4) Measures of restraint imposed upon a person in accordance with this section shall be imposed in accordance with and conform to the requirements of the Convention on Offenses and Certain Other Acts Committed on Board Aircraft. [P.L. 2002-65, §31.]

**§132. Power to disembark certain passengers.**

The aircraft commander may, in so far as it is necessary to protect the safety of the aircraft, or of persons or property therein or to maintain good order and discipline on board, disembark, in accordance with the Convention on Offenses and Certain Other Acts Committed on Board Aircraft, any person who the aircraft commander has reasonable grounds to believe has committed, or is about to commit, on board the aircraft an act contemplated by section 131(1)(b). [P.L. 2002-65, §32.]

**§133. Power to deliver alleged offenders to competent authorities.**

The aircraft commander may deliver to competent law enforcement authorities, in accordance with the Convention on Offenses and Certain Other Acts Committed on Board Aircraft, any person who the aircraft commander has reasonable grounds to believe has committed on board the aircraft an act which, in the commander's opinion, is a serious offense according to the criminal laws of the country of registration of the aircraft. [P.L. 2002-65, §33.]

**§134. No liability for actions taken.**

For actions taken in accordance with section 131, 132 or 133, neither the aircraft commander, any other member of the crew, any passenger, the owner or operator of the aircraft, nor the person on whose behalf the flight was performed shall be held responsible in any proceeding on account of the treatment undergone by the person in respect of whom the actions were taken. [P.L. 2002-65, §34.]

**Division 9. Safety of Maritime Navigation and Fixed Platforms**

**§135. Maritime offenses.**

In any waters where the convention and protocol referenced in paragraphs 8 and 9 of the Schedule to this Act would apply, any person who knowingly, directly or indirectly:

(1) seizes or exercises unauthorized control over a ship or fixed platform by force or threat thereof or by any other form of intimidation; or,

(2) injures or kills any person, or endangers the safe navigation of a ship or the safety of a fixed platform, by:

(a) committing an act of violence against a person on board the ship or fixed platform; or

(b) destroying or damaging the ship, its cargo, or the fixed platform; or

(c) placing or causing to be placed any device or substance on the ship or fixed platform; or

(d) destroying or damaging maritime navigational facilities or interfering with their operation; or

(e) communicating information which the person knows to be false; commits a crime punishable under section 107(1) (a) of this Act; provided, however, where, in committing such crime, the person uses or deploys a weapon of mass destruction the person shall be liable to fine of up to \$1,000,000,000.00. [P.L. 2002-65, §35.]

**Division 10. Nuclear Material:**

**§136. Nuclear material offenses.**

(1) Any person who intentionally, by any means, directly or indirectly:

- (a) without lawful authority, receives, possesses, uses, transfers, alters, disposes of, or disperses nuclear material, under circumstances which cause or are likely to cause death or serious bodily injury to any person or substantial damage to property;
- (b) commits a theft or robbery of nuclear material;
- (c) embezzles or fraudulently obtains nuclear material;
- (d) makes a demand for nuclear material by threat or use of force or by any other form of intimidation;
- (e) threatens:
  - (i) to use nuclear material to cause death or serious bodily injury to any person or substantial property damage; or
  - (ii) to commit a theft or robbery of nuclear material in order to compel a natural or legal person, or an international organization, or country to do or to refrain from doing any act; commits a crime punishable by a term of not less than 30 years and not more than life imprisonment, or a fine of not more than \$1,000,000,000.00; or both. [P.L. 2002-65, §36.]

**§137. Other rights, obligations and responsibilities not affected; no liability for actions taken in good faith.**

- (1) Nothing in this Act shall affect other rights, obligations and responsibilities of the Marshall Islands and individuals under international law, in particular the purposes of the Charter of the United Nations, the Compact of Free Association with the United States, international humanitarian law and other relevant conventions.
- (2) Nothing in this Act entitles the Marshall Islands or any other country to undertake in the territory of the other the exercise of jurisdiction or performance of functions that are exclusively reserved for the authorities of that country by its domestic law.
- (3) Persons shall be immune from suit and civil liability for actions taken in good faith pursuant to and in accordance with this Act. [P.L. 2002-65, §37.]

**§138. Resolution of disputes.**

Any dispute between the Marshall Islands and any other Party to an international terrorism convention concerning the interpretation or application of this Act relating to application of the convention shall be resolved in accordance with the provisions of the relevant international terrorism convention. [P.L. 2002-65, §38.]

**§139. Implementing regulations.**

The Minister may prescribe such rules and regulations, as the Minister deems reasonably necessary to implement the provisions of this Act. [P.L. 2002-65, §39.]

2011

© Asia/Pacific Group on Money  
Laundering