COOK ISLANDS MONEY LAUNDERING AND TERRORIST FINANCING:

_____

Financial Institutions and Designated Non-Financial Businesses and Professions Sectors Review of Risk.

Phil Hunkin

October 2017

Financial Institutions and Designated Non-Financial Businesses and Professions Sector Review of Risk

Contents Page

1.0	**Foreword**	**3**
2.0	**Introduction**	**4**
3.0	**Cook Islands ML/TF Risk Assessments**	**4**
4.0	**National AML/CFT/PF Strategy for the Cook Islands**	**6**

1.0 Foreword

It is my privilege to introduce the Cook Islands Money Laundering and Terrorist Financing: Financial Institutions and Designated Non-Financial Business and Professions Sectors Review of Risk. This report has been developed to continue the very important risk assessment work that was initiated through the National Risk Assessment 2015.

The Cook Islands is committed to being a good and responsible international citizen, to do its part in fighting the laundering of proceeds from criminal activity, regardless of whether they are generated in or outside the Cook Islands, and to fight against those who wish to harm others through terrorist activities. While the Cook Islands is remote geographically, in the age of globalisation, the Cook Islands is not sheltered from serious criminal activity or terrorism or its effects.

Cook Islanders can be victims of such and they can be perpetrators. It is therefore essential that the country has a system in place to detect, disrupt and prevent money laundering, terrorist financing and proliferation financing activity in and from the Cook Islands.

Having a robust and effective AML/CFT/PF regime will ensure that the integrity and reputation of the Cook Islands financial system is upheld. A sound and well regulated financial system is a key component of meeting the Cook Islands national vision under the Te Kaveinga Nui – National Sustainable Development Plan 2016 – 2020, in particular:

- **Goal 2: Expand economic opportunities, improve economic resilience and productive employment to ensure decent work for all; and**

- **Goal 16: Promote a peaceful and just society and practice good governance with transparency and accountability.**

Not only does a strong financial system detect and disrupt proceeds from criminal and terrorist activity but it has a flow on effect of attracting more legitimate participation in it, both from within and outside the Cook Islands. This can mean more investment, job creation and economic growth for the country.

This sector review of risk leads to an important component of the evidence base for the response to money laundering, terrorist financing and proliferation financing over the coming years. The government is confident that by responding to these risks, and through continued partnership between government, law enforcement, supervisors and the private sector, we can ensure that the Cook Islands economy is a hostile environment for illicit finance and an open, attractive destination for legitimate business.

I would like to thank all the Crown agencies and reporting entities for their assistance and cooperation with the development of the sector review of risk assessments.

The recent presentations of the report's findings were very well attended and reflects the importance the Cook Islands places on identifying, understanding and where necessary taking actions to mitigate the risks identified.

I look forward to continuing to focus on ML/TF/PF risk going forward in my role as Head of FIU and as Chairman of the National AML/CFT/PF Co-Ordinating Committee.

Phil Hunkin

Head of FIU and Chairman, National AML/CFT/PF Co-Ordinating Committee

2.0 Introduction

2.1 The Cooks Islands undertook and published a National Risk Assessment in 2015. The assessment focussed on the threats, vulnerabilities and risks presented through money laundering, terrorism financing and the proliferation of weapons of mass destruction. As a consequence of the National Risk Assessment a number of measures have been deployed by the Cook Islands authorities to mitigate these risks.

2.2 To assess the benefits of these measures a **Cook Islands Money Laundering and Terrorist Financing – Primary Threats and High Risk Sectors report** was commissioned by the Financial Supervisory Commission, to undertake a risk assessment of these high risk sectors and to report the findings to the AML/CFT authorities. The report was concluded on 28th July 2017.

2.3 A further report has been commissioned through the FIU to undertake a similar assessment of sectors not incorporated as part of the Primary Threats and High Risk Sectors review. The review has been termed the **Secondary Threats and Low Risk Sectors**. The sectors that provided the focus of this review are:

- Accountants
- Lawyers
- Pearl Dealers
- Motor Vehicle Dealers
- Real Estate
- Lotto
- NPO's
- Aid development funding.

2.4 This report analyses the two reports and takes into account the substantial work undertaken by the Cook Islands since the NRA 2015 was adopted by Cabinet on 10th March 2015. The report has been titled **Financial Institutions and Designated Non-Financial Businesses and Professions Sector Review of Risk**.

3.0 Cook Islands ML/TF Risk Assessments

3.1 The Cook Islands published its National Risk Assessment on the 10th March 2015, this NRA was shared with all relevant competent authorities, self-regulatory bodies, financial institutions and DNFBP's. This outreach has enabled the Cook Islands to identify, assess and understand the risks presented through money laundering, terrorist financing and the proliferation of weapons of mass destruction. The Coordinating Committee of Agencies and Ministries (CCAM) is the government multi agency body with oversight for coordinating the activity around ML/TF risk. This body changed its name in January 2016 to the National AML/CFT Coordinating Committee (NACC). The chairman of NACC is the Head of FIU. The FIU is the leading Cook Islands competent authority with regard to ML and TF risk.

3.2 The NRA 2015 provided the framework for authorities to assess the risks and to implement measures that were commensurate to the risks identified. It also provided authorities with information that enabled them to identify areas where improvements could be made to the AML/CFT regime. The NRA 2015 assisted authorities in the prioritisation and allocation of resources. Financial Institutions and DNFBP's have used the NRA 2015 to assist in their own risk processes.

3.3 The NACC meets at regular intervals throughout the year and meetings are focussed on the outcomes of the NRA 2015, this high level Committee leads on strategy and policy to ensure that the appropriate AML/CFT regime is in place. The NACC has met on seven occasions since the beginning of

2016 and at each of the meetings the NRA 2015 and ongoing risk analysis has been undertaken. This collaboration between agencies has resulted in the Cook Islands properly identifying and understanding the money laundering and terrorist financing risks presented nationally and this domestic coordination has ensured the appropriate actions have been initiated to mitigate these risks.

3.4 The NRA 2015 made fourteen recommendations categorised under five headings; National Coordination; Transnational Risk Mitigation; National Risk Mitigation; Capacity Development and Legislative Drafting. These recommendations have been reviewed and acted upon where relevant by all the key agencies.

3.5 In development of the NRA 2017, it was determined that a targeted assessment of Cook Islands was the preferred approach. To obtain a better understanding of the nature and extent of the Cook Islands' ML/TF risk in the high risk and low risk sectors identified in the NRA 2015. NRA 2017 is a focussed Risk Assessment looking at National Risks in two specific areas; Financial Institutions and DNFBP's. Two separate reports have been commissioned. An external expert Alan Taylor was engaged by the Financial Supervisory Commission to prepare the "Cook Islands Money Laundering and Terrorist Financing – Primary Threats and High Risk Sectors" report. [1]A second report focussed on the Secondary Threats and Low Risk Sectors has been developed through the FIU Compliance Team throughout 2017. This activity is directed by the 2017 -2019 Compliance Strategic plan.

3.6 Taylor's report highlighted a number of areas where the Cook Islands could mitigate risks identified further.

- Increased STRs, data mining, FIU, Customs and Police investigations and rejections of business by service providers, may lead to a better awareness and understanding of ML/TF/FOP and more robust compliance systems to detect, deter and disrupt ML/TF/FOP activity.
- CI AML/CFT regime must be continually monitored and regularly reviewed to ensure it is adequate and appropriate for the ML threats faced by CI at any given time.
- CI may consider establishing a clear and definitive AML/CFT strategy lead by a smaller more focussed NACC;
- Training, dissemination of information and communication amongst government agencies and the private sector is essential to increase awareness and understanding of ML/TF/FOP;
- Given the enactment of FTRA 2017, FIU compliance audits can be carefully planned and structured for maximum effect;
- Section 47 FTRA 2017 should result in more STRs being filed providing a better tool and greater intelligence for FIU to assess the ML/TF/FOP threats to which CI is exposed;
- FIU should clarify with all government agencies the type of financial information it should receive for its further investigation and place a formal structure around such communication and dissemination;
- Restrictions on FIU, through lack of staff, to proactively mine financial transaction data may mean valuable information is missed. Perhaps this role could be delegated or contracted out to ensure the best possible opportunity is given to detecting ML/TF/FOP activity;
- Reporting institutions' obligation to risk assess clients and obtain CDD accordingly, needs to be closely monitored to ensure appropriate CDD is being obtained.

[1] Alan is a New Zealand qualified lawyer with 23 years' experience in the international financial services industry, 10 of those spent working in the Cook Islands. Alan has held legal, business development and senior management positions in both public and private organisations. He is currently working for the Cook Islands Financial Services Development Authority.

3.7 The FIU report Secondary Threats and Low Risk Sectors complements the Primary Threats and High Risk Sector Report. The eight sectors identified for the purpose of the FIU review have all been subject to either a desk based review or Compliance visit assessments, by the FIU. The outcomes of the risk assessment indicate an increase of risk. This is as a direct result of new legislation introduced in 2017. In particular the Financial Transactions Reporting Act, 2017 (FTRA 2017) that requires reporting institutions to manage risks including the development of risk policies. The sectors are generally required to develop their knowledge and risk based processes to more effectively mitigate the risks presented. The outcome of this risk assessment will be fed back into the work processes of the FIU Compliance Team to improve risk mitigation of the sector with the aim of lowering the overall risk.

3.8 The Cook Islands, through the FIU engaged John Chevis a UNODC consultant to review the various government agencies assessing their vulnerabilities and capacity through their effectiveness in respect of the AML/CFT regime. The UNODC were in country between the 4th April and 8th April 2016.

3.9 Peter Dench an AML/CFT Financial Sector consultant assisted in the reviewing of the work and practices undertaken by the FIU and FSC focussing on their effectiveness with respect to IO 3 and IO 5. He also looked at the extent to which technical compliance with the FATF 40 recommendations. As a part of this process Dench met with all of the banks (four), five trustee companies, three other financial institutions and one NPO. The objective of these meetings was to assist their preparation for the new FTRA legislation and the new requirements that would be placed on reporting institutions this included an analysis and explanations of the risks work that would need to be undertaken.

3.10 At the end of October 2017 senior members of the FSC, FIU and Alan Taylor presented the findings of the sector specific risk assessments to government authorities, reporting institutions, Designated Non-financial Business and Professions and NPO's. The sessions held over three days were well attended with positive contributions from the floor and interaction. In total there were fifty five different attendees.

4. National AML/CFT/PF Strategy for the Cook Islands.

4.1 The Cook Islands has developed and published an AML/CFT/PF strategy. This strategy has been directed and informed by the NRA 2015 and the significant risk based activity that has taken place in the short period of time since the NRA publication in 2015. All of the risk based activity that has occurred and outlined earlier in this report has assisted in the production of this strategy.

4.2 This strategy will be adopted by the NACC and will the AML/CFT/PF focus for the period 2017-2020. This strategy will continue to be informed from ongoing risk assessments and as such is a living document.

COOK ISLANDS MONEY LAUNDERING AND TERRORIST FINANCING:

PRIMARY THREATS AND HIGH RISK SECTORS

Alan Taylor*

28 July 2017

COOK ISLANDS MONEY LAUNDERING AND TERRORIST FINANCING: PRIMARY THREATS AND HIGH RISK SECTORS

Contents **Page**

Executive Summary 9

1. Methodology 12
2. The Cook Islands in Context 13
3. The Legal and Regulatory Framework 15
4. Predicate Offences 20
5. Primary Threats 24
6. Indicators of ML Threat 26
7. The High Risk Sectors and Other Areas for Consideration 34
8. Terrorist Financing 46
9. Effectiveness of ML/TF/FOP Measures in Place 48

Annex 1: World Bank GDP Rankings 2015 55

Annex 2: Roles of Government Agencies 56

Annex 3: High Risk Jurisdictions 58

Glossary 59

Acknowledgements 61

Executive Summary

Introduction

The Financial Action Task Force (**FATF**) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations, as adopted in 2012 *(1)* (**the Recommendations**), provide the international standards on combatting money laundering and the financing of terrorism and proliferation. The Cook Islands (**CI**) has committed to the Recommendations through its membership of the Asia/ Pacific Group on Money Laundering (**APG**), a FATF style regional body.

Recommendation 1 of the Recommendations requires each country to "identify, assess, and understand the money laundering and terrorist financing risks for the country". The interpretive notes to the Recommendations further provide that "countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on the results to all relevant competent authorities and self-regulatory bodies, financial institutions and designated non-financial bodies and professions." (**DNFBPs**) *(2)*

CI has to date sought to meet that obligation by producing the "Money Laundering Risk Analysis for the Cook Islands" in 2008 (**NRA 2008**) *(3.)*, followed by the "National Risk Assessment 2015: Money Laundering and Financing of Terrorism in the Cook Islands" (**NRA 2015**). *(4)*

The next CI national risk assessment, providing a comprehensive analyses and assessment of the money laundering/terrorist financing/financing of proliferation (**ML/TF/FOP**) risks to which the CI is potentially exposed, is scheduled to be completed by 31 October 2017 (**NRA 2017**). However, in anticipation of the APG undertaking a Mutual Evaluation of CI's anti-money laundering and countering the financing of terrorism (**AML/CFT**) (5) regime in November this year, the Cook Islands Financial Supervisory Commission (**FSC**) has requested that a targeted risk assessment be carried out focussing on the primary ML/TF/FOP threats to CI and the sectors within CI most vulnerable to those threats.

This Report seeks to provide that assessment by identifying:

- the main ML/TF/FOP threat to the CI and from where that threat originates;
- the sectors/industries/businesses within CI at most risk from that threat;
- how those sectors/industries/businesses are most vulnerable to that threat;
- the impact such threat may have on CI and its economy;
- the measures in place to counter that threat.

Following the identification process a deeper understanding of the most immediate ML/TF/FOP risks should be available to then assess the effectiveness of the measures in place to counter those risks and any further measures that CI should consider to manage and mitigate the risks identified.

This Report picks up on the conclusions of NRA 2015, in terms of high risk sectors/industries/businesses, and provides further analyses and update in the context of the current CI AML/CFT environment. It seeks to identify any additional or related ML/TF/FOP risks that may currently exist across those sectors/industries/businesses and any particular activity or operation within each which potentially exposes CI to a higher degree of risk than currently understood or anticipated.

Whilst this Report focusses on the primary ML/TF/FOP threat to CI and where CI is most vulnerable to that threat, references are also made to those sectors/industries/businesses not necessarily regarded as high risk but where some exposure to that threat exists. It is acknowledged that where a

sector/industry/business may be regarded as having low or medium ML/TF/FOP risk, that does not mean no risk, but for the purposes of this Report the risk is not regarded as sufficiently high to warrant further analyses. It is expected that those sectors and industries will be analysed in full as part of NRA 2017.

Key Findings

By most measures CI is regarded as a very small country. When defined by way of its population, domestic economy, GDP, trade levels, international fund flows, financial services industry etc. it appears fairly insignificant on a global scale and unnoticed by many. Evidence would suggest that ML/TF/FOP, and the criminality that leads to it, do not present a significant risk to CI at this time. The lack of size and complexity of CI financial sector, including trust and company service providers (**TCSPs**), may mean that it is less exposed to criminality than financial sectors in other countries.

Notwithstanding this, CI must be vigilant and proactive in the face of international criminals and terrorists who may look to exploit it due to its lack of size which may be perceived as a lack of awareness, understanding and sophistication in detecting criminal activity.

The primary ML/TF/FOP threat to CI comes from international sources. Financial crimes are not the most prevalent amongst domestic predicate offences and the proceeds of domestic crime are not significant. The sectors/industries/businesses at most risk from the primary threat are those that have exposure through international customers seeking to use CI banking system and service providers to receive, hold and transfer the proceeds of crime, or assist in the commission of a crime which may generate proceeds. In the CI context, those at most risk are financial institutions and TCSPs, given the nature of their business and lack of face to face meetings with customers. Given that up to 90% of TCSP business is from US high net worth individuals and the sole CI private bank receives and sends more funds to US than anywhere else, it is reasonable to suggest that this is the primary source of the primary threat. Other ML indicators such as suspicious transaction reports (**STRs**) and foreign requests to government agencies for information, also reflect this.

A clear and succinct national AML/CFT strategy document would be beneficial, setting out, inter alia:

- what ML/TF/FOP is and where CI is exposed;
- CI objectives regarding ML/TF/FOP;
- the CI AML/CFT regime in place, including the groups, agencies, committees etc. involved and their roles and responsibilities;
- how the regime is being/will be used to combat ML/TF/FOP;
- policies both in place and to be implemented.

A smaller more focussed National AML/CFT Co-ordinating Committee (**NACC**), being the body responsible for formulating and developing AML/CFT policies, may prove to be more effective in addressing ML/TF/FOP issues and establishing, implementing, developing and revising policy. Private sector, and in particular financial institutions and TSCPs, should be considered as members. Collaboration between government and the private sector will help achieve better understanding and acceptance of what is in CI's best interests in regards to combatting ML/TF/FOP.

Training programmes are required (and are currently being planned by FSC/FIU) for all those who have a role to play within the AML/CFT regime to improve their knowledge and understanding of ML/TF/FOP and their obligations within the regime. Those who must comply with the Financial Transactions Reporting Act 2017 (**FTRA 2017**) will require immediate assistance. In addition, members of Parliament should be included in such training programmes to assist in their understanding of the AML/CFT regime and laws they are asked to debate and pass.

The Financial Intelligence Unit (**FIU**) is responsible for receiving and analysing all financial intelligence. The analysis of such information is paramount to investigations and for detecting

ML/TF/FOP threats and methods. Due to resource constraints, it is unlikely this information and data is being thoroughly scrutinised for evidence of ML/TF/FOP activity meaning some activity may go undetected. The Police has also expressed its concern at the lack of resources to investigate ML.

CI has recently enacted FTRA 2017, and updated other ML/TF/FOP related laws, to bring CI AML/CFT regime in line with current FATF standards. FIU has the opportunity to devise a robust and well-structured audit programme to test compliance with all aspects of FTRA 2017.

TCSPs risk of being associated with ML/TF/FOP and other criminal activity is increased where TCSPs do not have control over the assets, business or other activities of entities owned by a trust to which they provide the trustee. This may be the case where the customer does not want the TCSP to be involved in the management of the entity or it may be the TSCP does not want to be exposed to potential liability arising from holding a management position. TCSPs will be at most risk where they carry out limited or no due diligence on the entity's management or its business activities and assets. Whilst CI financial system may not be at direct risk, its reputation would.

There appears to be good co-operation with foreign authorities requesting information. Also, the relationship between government agencies seems good when sharing information. However, it is not clear if all relevant information is being shared with FIU in a consistent manner. To enhance this sharing of information, the roles and responsibilities of each government agency, particularly those that receive intelligence, investigate crimes and enforce the law, could be documented putting a formal structure around the communication and dissemination of information. This could also include the recording and sharing of informal information requests from foreign authorities by government agencies to ensure they are appropriately dealt with.

The number of instances of undeclared cash being discovered at the border appears low. A contributing factor to this maybe the lack of any real means of detecting cash other than third party information. The number of STRs filed pursuant to the predecessor to FTRA 2017, being the Financial Transactions Reporting Act 2004 (**FTRA 2004**), is also relatively small. The suspicious transaction reporting requirement under FTRA 2017 may generate increased filing which in turn will provide valuable information for detecting ML methods and activity.

CI must understand where it is most at risk from ML/TF/FOP threats, where vulnerabilities exist and how they may be exploited. With understanding comes the ability to better identify those threats and vulnerabilities and act appropriately within the CI context to combat them through a concerted national effort to detect, disrupt, deter and mitigate ML/TF/FOP risks.

---

1. *http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)*
2. *Ibid at note A.3 page 32*
3. *Produced by Mr John Walker, Associate Professor, Wollongong University, Australia*
4. *Produced by the Cook Islands Financial Intelligence Unit together with the key Crown agencies of the Co-Ordinating Committee on Money Laundering and Terrorist Financing*
5. The use of the acronym "AML/CFT" in this Report includes the combatting of proliferation of weapons of mass destruction

1. Methodology

The methodology commonly followed when undertaking a national risk assessment is to collate and analyse relevant information from government agencies and all participants within each relevant sector of the private sector, to obtain a clear understanding of all the ML/TF/FOP risks that a country may be exposed to and where the country may be vulnerable to those risks. Upon identifying the risks, an evaluation is made of the relative exposure of a sector/industry/business activity to those risks. Various models are used in the evaluation process.

This Report is however a focussed report, focussed on the primary ML/TF/FOP threats to CI and those sectors/industries/businesses within CI that are at the most risk of being exploited by those threats.

In order to initially identify and confirm the primary ML/TF/FOP threats to CI and the sectors at most risk from those threats, the following was carried out:

- review of NRA 2008 and NRA 2015 and the evaluations and conclusions reached;
- review of the 2015 Cook Islands Typologies Report [1] (**2015 Typologies Report**);
- analyses of information and data obtained by FIU from key government agencies (available at the time of writing this Report) including information collected as part of the NRA 2017 information gathering exercise;
- analyses of information and data obtained by FIU from the private sector (available at the time of writing this Report) including information collected as part of the NRA 2017 information gathering exercise;
- discussions with key personnel in FSC and FIU;
- discussions with private sector stakeholders, in particular senior management involved in the banking and TCSP industries.

As a result, the identification of the primary threats and high risk sectors, as well as the conclusions to this Report, draws on the previous CI NRAs as well as the knowledge and experience of those within the FSC and FIU and senior management within the banking and TCSPs industries. The views of other members of the community with deep knowledge and experience of the CI, its economy, business and trade operations were also considered.

The approach taken by other countries in producing NRAs, as well as NRA models developed by the World Bank and International Monetary Fund, have been considered in the preparation of this Report. However, due to the specialised nature of this Report together with the particular circumstances and features of CI, they were used as general guidance only. Guidance was also provided by APG [2] and the United Nations Office on Drugs and Crime (**UNODC**) [3] representatives in terms of framework and approach to the preparation of this Report.

Therefore, with the assistance of the resources and expertise mentioned, the primary ML/TF/FOP threats to CI were confirmed and the business activities at most risk of being exploited were identified. Those threats and business activities will be examined later in this Report.

---

1. *Cook Islands Typologies Report 2015: Trends, Typologies and Case Studies, issued 23 June 2016*
2. *Michelle Harwood, Executive Officer, APG Secretariat*
3. *John Chevis UNODC Adviser (Anti-Money Laundering and Counter Financing of Terrorism) for the Pacific*

2. The Cook Islands in Context

CI is comprised of 15 islands situated at the heart of the South Pacific, northeast of New Zealand and south of Hawaii, covering approximately 2 million square kilometres of the Pacific Ocean. Seemingly remote, it is however very accessible by air, sea and through modern technology.

Government

CI is a self-governing nation with its own written constitution. It is a sovereign state in free association with New Zealand. It has a Westminster styled parliamentary system with democratic elections every five years. The political parties are each relatively centrist without interference from extreme political ideologies or religious beliefs or military threat. The Prime Minister is the Head of Government with the Head of State, being Her Majesty Queen Elizabeth II by her appointed representative in CI, the Queen's Representative. Legislative power is with CI Parliament (elected members of Parliament) whilst executive power is exercised by CI government (Cabinet ministers) and the Queen's Representative.

CI legal system is founded on English common law. The judiciary is independent of the executive and the legislature. It is comprised of a hierarchy of courts being a High Court and Court of Appeal with the ultimate appellate court being the Privy Council in London sitting in right of CI. CI's High Court and Court of Appeal judges are experienced New Zealand judges who provide independence. They apply CI law and have jurisdiction over all criminal and civil matters.

Domestic economy

The resident population of CI is estimated at 11,700, (1) about three-quarters of whom live on the island of Rarotonga being the main centre of trade and business activity.

Notwithstanding the economic disadvantages associated with its small size, geographical location, lack of diversity of natural resources and manufacturing capability, CI has built an economy focussed on industries such as tourism, fishing and a financial services industry with albeit a limited range of services and products.

CI is heavily reliant upon imports, in particular from New Zealand, for goods that cannot be sourced locally, including foodstuffs such as meat, fruit, vegetables, dry and canned goods, as well as clothing, household goods, building materials, machinery and vehicles for commercial and personal use. CI does not manufacture or produce any goods of sufficient quantity to have any more than a nominal impact on export markets and therefore the domestic economy. Trade deficits are supported by foreign aid, primarily from New Zealand.

CI GDP for 2015 was NZ$314 million (approx. US$209 million at current exchange rates) (2) extremely small in comparison to other countries, whether they be Pacific island neighbours, competitors for international financial services business or FATF member jurisdictions. **See Annex 1: World Bank GDP Rankings 2015**

The amount of funds coming into CI banking system from international sources is not significant in the international context or when compared to neighbouring Pacific countries and those with whom CI competes for financial services business. The net foreign assets held in the CI banking system as at 31 March 2017 was NZ$136.1 million. (3) CI is not regarded as an international or even regional finance centre.

To illustrate to what extent a developed financial service industry can be exposed to the rest of the world, and to provide a comparison (albeit an extreme one) to CI, "the UK is the world's leading exporter of financial services with a trade surplus of (US)$71 billion in 2013. The UK accounted for 41% of global foreign exchange trading in April 2013…..The UK is the single most internationally focused financial marketplace in the world." (4) It is estimated that somewhere between GBP23-57

billion is laundered within and through the United Kingdom (**UK**) each year. (5) The UK's status as one of the largest global financial centres makes it extremely vulnerable to global ML threats. Although not conclusive, or reason to be complacent, CI's status as one of the world's smallest economies and financial centres, would suggest that in comparative terms its vulnerability to global ML threats would be low.

International relations and co-operation

CI is a sovereign nation in free association with New Zealand and responsible for conducting its own foreign affairs. In 1992 the United Nations (**UN**) recognised CI's right to establish diplomatic relations with other countries. (6) Since then CI has been allowed to attend UN sponsored conferences open to "all States" as well as sign and ratify UN treaties open to "non-member states".

In the context of international financial regulation and the sharing of financial information with international authorities, CI has:

- signed and ratified the Convention on Mutual Administrative Assistance in Tax Matters, being the most powerful and comprehensive multilateral instrument available for all forms of tax cooperation including automatic exchange of information;
- signed the Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information in order to automatically exchange information pursuant to the Organisation for Economic Co-Operation and Development's (**OECD**) common reporting standard (CRS);
- entered into 33 (7) bi-lateral tax information exchange agreements (**TIEAs**) to promote international co-operation in tax matters through the exchange of information.

FSC has entered into the Multilateral Memorandum of Understanding between members of the Group of International Financial Centre Supervisors (**GIFCS**). GIFCS has 19 members from across the globe who have agreed to co-operate, consult and exchange information to assist in the carrying out of their supervisory and regulatory functions.

In addition, CI financial institutions have commenced providing financial information to the United States Internal Revenue Service (**IRS**) pursuant to the United States Foreign Account Tax Compliance Act (**FATCA**) in relation to all bank accounts held in CI by US persons.

CI is a member of OECD's Global Forum on Transparency and Exchange of Information for Tax Purposes (Global Forum). CI's phase 2 peer review (8) (published in March 2015) judged CI to be "largely compliant". Phase 2 peer reviews check that a jurisdiction is actually following the tax transparency practices set out in its legislative framework and in international agreements for exchange of information on request.

In 2009 CI underwent a mutual evaluation on AML/CFT carried out by APG to determine compliance with the FATF's Recommendations in place at that time. CI's 2nd Round report was published in July 2009 and showed CI to be in the top 20% of countries in the world for implementing international regulatory AML/CFT standards.

---

1. *The CI Statistics Office, Vital Statistics and Population Estimates September 2016* http://www.mfem.gov.ck/statistics/social-statistics/vital-stats-pop-est
2. *Information provided by Cook Islands Ministry of Finance and Economic Management, Statistics office*
3. *Cook Islands Statistics Office, Statistical Bulletin, Banking Statistics March Quarter 2017.*
4. *UK National Risk Assessment of Money Laundering and Terrorist Financing, published October 2015, at page 85, para 10.4*
5. *ibid at para 10.6*
6. *Repertory of Practice of United Nations Organs Supplement No. Volume VI Article 102*
7. *Information provided by RMD on 24.05.17*
8. http://eoi-tax.org/jurisdictions/CK#latest

3. The Legal and Regulatory Framework

The following is an outline of the legal and regulatory framework currently governing the AML/CFT regime in CI.

Strategy and Policy

NACC is responsible for formulating and developing CI AML/CFT policies as well as ensuring the institutional framework for AML/CFT covers all relevant areas of the CI economy. The Head of FIU is the Chair of NACC. NACC is made up of one member from each of the following key government agencies:

FIU; CI Police Service (**Police**); Crown Law Office (**CLO**); Revenue Management Division (**RMD**); FSC; Ministry of Foreign Affairs and Immigration (**MFAI**); Ministry of Justice (**MOJ**); Business Trade and Investment Board (**BTIB**); The Cook Islands Expenditure and Review Committee and Audit Office (**Audit**); Ministry of Marine Resources (**MMR**), CI Customs Service (**Customs**).

AML/CFT/FOP Legislation

CI has, as at 23 June 2017, updated various statutes contained in its suite of AML/CFT related legislation to bring them in to line with the Recommendations, as revised and adopted in 2012.

a. For detection, prevention and enforcement

Financial Transactions Reporting Act 2004 (FTRA 2004) was repealed and replaced by FTRA 2017 on 23 June 2017. FTRA 2004 provided that it was "an Act to facilitate the prevention, detection, investigation and prosecution of money laundering, financing of terrorism and other serious offences and the enforcement of the Proceeds of Crime Act 2003". FTRA 2004 established FIU and introduced customer due diligence, transaction monitoring and suspicious transaction reporting requirements for all "reporting institutions". "Reporting institutions" amounted to any person or entity who carried out an activity (as specified in section 2 of FTRA 2004) on behalf of a customer. Those activities endeavoured to capture the provision of any service involved in the transfer, receipt, holding, investment or management of any asset, liquid or otherwise. FTRA 2004 was administered by FIU.

Financial Transactions Reporting Act 2017 (FTRA 2017) repealed and replaced FTRA 2004 on 23 June 2017. FTRA 2017 is designed to bring CI up to the standard required by the Recommendations, as revised in 2012, in regards to the detection, prevention, investigation and prosecution of ML/TF/FOP activity. Following the enactment of FTRA 2017, CI AML/CFT regime will move to a risk based approach whereby assessments of ML/TF/FOP risk will be carried out by each "reporting institution" (1) on its business, customers and products and services, in addition to assessments already being carried out by government at a national level. Reporting institutions will be able to apply appropriate (simple, standard or enhanced) customer due diligence (**CDD**) requirements based on the perceived risk. Also the scope for filing STRs has been widened. A reporting institution will be required to report any activity that it has reasonable grounds to suspect is suspicious activity.

Financial Transactions Reporting Act 2017 Regulations (the Regulations). The Regulations were promulgated on 18 July 2017. The Regulations include:

- the types of activity, being "specified activity" as prescribed in Regulation 4, that businesses must undertake to be considered reporting institutions;
- the types of identification to be obtained for CDD purposes; and
- qualification criteria for money laundering reporting officers.

Crimes Act 1969 (CA) is the CI criminal code and contains the majority of the predicate offences to ML/TF/FOP. It was amended in 2003 by the Crimes Amendment Act 2003 to introduce the criminal offence of money laundering which was itself amended in 2004. (2) The offence of money laundering is set out in section 280A (2) CA. (3) Predicate offences to money laundering are "serious offences" (4) being any act or omission that constitutes an offence against CI law punishable by a prison term of not less than 12 months or a fine of more than NZ$5,000. Any offence against the law of another country that would constitute a "serious offence" if carried out in CI will also be a predicate offence. CA is administered by MOJ.

Countering Terrorism and the Proliferation of Weapons of Mass Destruction Act 2017 (CTPWMDA) (previously called Terrorism Suppression Act 2004 (**TSA**)). TSA was amended on 23 June 2017 by the Terrorism Suppression Amendment Act 2017 (**TSA Amendment**). The name of the statute was amended to better reflect its content following amendment. TSA was not repealed and replaced. TSA Amendment implemented laws required to meet the FATF standards on countering the financing of terrorism and unlawful proliferation. CTPWMDA provides for the suppression of terrorism by prohibiting people in CI from dealing with terrorist property or participating in terrorist activities. It establishes the regulatory framework for implementation of UN resolutions and conventions dealing with terrorism and terrorist financing. The objects of CTPWMDA have been extended by TSA Amendment to the countering of unlawful proliferation of weapons of mass destruction in addition to terrorism and terrorist financing. TSA Amendment adds further offences concerning terrorist activity and includes a number of offences concerning proliferation. CTPWMDA is administered by CLO.

Proceeds of Crime Act 2003 (PoCA) provides the legal framework for dealing with the proceeds of crime, including the seizure, restraint and forfeiture of such proceeds (domestic and foreign). It provides for investigatory orders such as search warrants and production and monitoring orders. It establishes a conviction based confiscation system**.** PoCA was amended on 23 June 2017 by the Proceeds of Crime Amendment Bill 2017 (**PoCA Amendment**). PoCA Amendment clarifies the definitions of "tainted property" and "proceeds". "Tainted property" now means the proceeds of any offence, not just the proceeds of a serious offence, as well as property used or intended to be used in or in connection with the commission of a serious offence. PoCA is administered by CLO.

Currency Declaration Act 2016 (CDA) provides for the oversight of the cross-border movement of currency and enables the seizure, detention or forfeiture of currency that is undeclared, or the proceeds of financial misconduct or unlawful activity. CDA provides Customs, FIU and Police with powers to question, search and seize in relation to cross border currency matters as well as detain such currency. CDA is administered by the FIU.

Customs Revenue and Border Protection Act 2012 (CRBPA) provides the legal framework for Customs and sets out its powers and authority. Customs is responsible for ensuring border security. It has powers to question individuals and obtain information, search for prohibited goods, investigate and prosecute (through RMD) illegal activity. Such activity primarily involves prohibited goods including drugs, firearms, cash in excess of thresholds and goods smuggled to avoid duties and levies. CRBPA is administered by RMD.

Income Tax Act 1997 (ITAXA) ITAXA provides the legal framework for charging and collecting income tax in CI and proceedings for offences against ITAXA. It sets out the powers of the Collector of Inland Revenue to obtain information for taxation purposes, both domestic and foreign. ITAXA is administered RMD.

b. Law enforcement agencies

The main CI law enforcement agencies are FIU, Police, Customs, RMD and CLO. Relevant legislation in addition to that noted in a. above includes:

Financial Intelligence Unit Act 2015 (FIUA) sets out the functions, duties and powers of FIU. FIU regulates and supervises "reporting institutions" (see definition at section 5 FTRA 2017) in respect of compliance with the oversight Acts being: FTRA 2017; POCA; Mutual Assistance in Criminal Matters Act 2003 (**MACMA**) and, since June 23 2017, CTPWMDA as amended by TSA Amendment. FIUA empowers the FIU to investigate any suspected financial misconduct that comes to its attention. "Financial misconduct" is defined in section 4 FIUA and includes ML/TF/FOP, fraud involving cross border financial transactions, financing of proliferation of weapons of mass destruction, financing or facilitating of bribery or any form of corruption, tax evasion whether or not relating to taxes payable in CI and any breach of an oversight Act. FIUA is administered by FSC.

Police Act 2102 (PA) PA provides for the governance and administration of Police including its functions, duties and powers.

c. Supervision

Financial Supervisory Commission Act 2003 (FSCA) sets out the functions, duties and powers of FSC. FSC is the prudential regulator and supervisor of licensed financial institutions and has broad powers under the FSCA to undertake on-site compliance visits and obtain information. FSC provides a supporting role to the FIU in AML/CFT supervision**.** FSCA is administered by FSC.

d. International co-operation

Mutual Assistance in Criminal Matters Act 2003 (MACMA) provides the legal framework within which CI provides or requests assistance in criminal matters to or from foreign countries. Such assistance will usually involve the provision of evidence and production, search and seizure of assets. MACMA was amended by the Mutual Assistance in Criminal Matters Amendment Act 2017 (**MACMA Amendment**) enacted on 23 June 2017. Any investigation or proceedings commenced in CI or overseas in regards to forfeiture or restraint of property, must be treated as criminal in nature where the investigation or proceedings involve tainted property. MACMA is administered by CLO.

Extradition Act 2003 (EA) sets out the framework for CI making and receiving extradition requests of and from other countries in relation to persons accused or convicted of extradition offences. EA is administered by Police.

Administration and Enforcement

The main CI law enforcement agencies are FIU, Police, Customs, RMD and CLO with Police being the lead agency for the investigation and prosecution of all criminal conduct in CI, including ML/TF/FOP and relevant predicate offences.

Each of the government agencies within NACC has a role within the CI AML/CFT regime, whether it be in the administration, supervision, communication or enforcement of AML/CFT laws, rules, regulations and policies. **See Annex 2: Roles of Government Agencies.**

In regards to the administration and enforcement of AML/CFT matters:

FIU has responsibility pursuant to FIUA to administer and enforce those statutes concerning financial misconduct. It receives, requests and analyses financial intelligence and provides the same to Police for further investigation in relation to any financial misconduct. Supervision of AML/CFT compliance by reporting institutions is a function and duty of the FIU.

Police is the lead law enforcement agency for the investigation and prosecution of all criminal conduct in CI including ML/TF/FOP offences, and relevant predicate offences. Police and FIU work together on ML/TF/FOP investigations. The Criminal Investigation Branch of the Police is the specialised group with responsibility for the investigation of all serious crimes, including drug related and financial crimes, ML/TF/FOP and proceeds of crime investigations.

CLO assists Police in the prosecution of ML/TF/FOP offences (and relevant predicate offences) and submits applications for orders under PoCA. CLO provides advice to all law enforcement agencies on prosecutions. It represents law enforcement agencies in Court and is responsible for administering mutual legal assistance requests and proceeds of crime matters. CLO is also responsible for the review and management of all legislation for Parliament and Executive Council.

RMD is a division of the Ministry of Finance and Economic Management (MFEM) and is responsible for the administration and enforcement of taxation and customs laws.

Other relevant committees within the Cl AML/CFT regime are:

Cook Islands National Intelligence Taskforce (CINIT) is an intelligence sharing body comprised of Police, FIU, Customs and Immigration (a division in MFAI). CINIT's main focus is criminal investigations but also includes investigations by other government agencies on a case by case basis;

Cook Islands Combined Law Agency Group (CLAG) is the coordinating committee for joint law enforcement operations in CI;

Cook Islands Anti-Corruption Committee (ACC) is the coordinating committee for anti-corruption strategies and policies in CI. The ACC does not have an investigative function but instead relies on its members to coordinate their efforts to address corruption cases in CI. The Head of FIU is the Chair of ACC. ACC members are FIU, Police, Audit, CLO, Office of the Ombudsman and MFEM.

The terms of reference for NACC, CINIT, CLAG and ACC were not viewed in the preparation of this Report. It is assumed that there are distinct lines of communication between each of these groups and a common understanding of their roles and responsibilities for each to be effective.

Based on information obtained and reviewed, it would appear beneficial to all stakeholders if a clear and succinct national AML/CFT strategy document was produced setting out, inter alia:

- CI objectives regarding ML/TF and proliferation of weapons of mass destruction;
- what is ML/TF and proliferation;
- the CI AML/CFT regime in place, including the groups, agencies etc. involved and their roles and responsibilities;
- how the regime is being/will be used to combat ML/TF/FOP;
- the policies in place and how they are implemented.

It would seem appropriate that such a strategy document be issued by NACC. A smaller more focussed NACC may be more effective in addressing and targeting ML/TF/FOP issues and establishing, implementing, developing and revising policy. Contributions from the private sector and in particular the financial services industry, including TCSPs, may also be useful in gaining a better understanding of ML/TF/FOP threats and establishing relevant and meaningful policy.

Summary

A general AML/CFT framework to combat potential ML/TF/FOP risks is in place. The effectiveness of CI AML/CFT strategy, legislation, regulation, supervision, co-operation (domestically and internationally), administration and enforcement will be considered later in this Report. Recent legislative amendments are designed to strengthen the regime and bring ML/TF/FOP laws in line with the Recommendations. Those laws will need to be tested to determine effectiveness as well as suitability to deal with the ML/TF/FOP risks.

---

1. *Section 5 FTRA 2017 definition of "reporting institution"*
2. *Crimes Amendment Act 2004*
3. *Section 280 (2) "A person commits the offence of money-laundering if the person –*

(a) acquires, possesses or uses property, or engages in a transaction that involves property, knowing or having reason to believe that it is derived directly or indirectly from a serious offence;
(b) converts or transfers property with the aim of-
(i) concealing or disguising the illicit origin of that property; or
(ii) aiding any person involved in the commission of the offence, to evade the legal consequences thereof,
knowing or having reason to believe that the property is derived directly or indirectly from a serious offence;
(c) conceals or disguises the true nature, origin, location, disposition, movement or ownership of the property knowing or having reason to believe that it is derived directly or indirectly from a serious offence;
(d) renders assistance to another person for any of the above."

4. *ML definition contained in section 280A (1) CA*

4. Predicate Offences

The Crimes Amendment Act 2003 criminalised ML by the introduction of section 280A (2) CA. Section 280A was repealed and replaced by Crimes Amendment Act 2004. Under CI law a person will be guilty of a ML offence if that person knowingly deals with property derived from a "serious offence" or deals with property and is wilfully blind to the fact that it is derived from a "serious offence". (1)

A "serious offence" (i.e. a predicate offence to ML) is any act or omission that constitutes an offence against CI law punishable by a prison term of not less than 12 months or a fine of more than NZ$5,000. An offence against the law of another country that would constitute a "serious offence" if carried out in CI is also a predicate offence.

CI does not therefore have all crimes legislation for the prosecution of ML/TF/FOP, as a number of jurisdictions do, but the thresholds for "serious offences" are relatively low.

CI has a wide range of predicate offences from which a ML/TF/FOP charge can arise, a significant number of which are contained in CA, as amended. Predicate offences do, however, also exist in legislation such as:

- Transport Act 1966;
- Narcotics Act 1965;
- Income Tax Act 1997.

It is noted that any person may be convicted of the offence of ML notwithstanding the absence of a conviction in respect of a predicate offence which generated the proceeds alleged to have been laundered. (2)

Table 1. Domestic predicate offences reported to Police (3)

Predicate Offences	2014	2015	2016
Fraud	10	14	9
Theft	232	265	222
Burglary	229	161	115
Corruption/bribery	-	1	2
Drug offences	12	10	8

Note that that domestic tax evasion offences are dealt with by RMD and noted below.

Most CI domestic crime involves burglary and theft. Financial crimes do exist but the occurrences of those reported and prosecuted are relatively small as are the proceeds generated. Proceeds generated from domestic predicate crimes are considered to be for personal use or life style satisfaction. CI has a relatively large cash based economy. Many local businesses, shops and outlets operate on a cash only basis. This would indicate the possibility of co-mingling to transfer the proceeds of any domestic crime into the financial system.

To date there have been no prosecutions under or convictions of the ML offences (s280A (2), (3) CA) and only one application under PoCA to seize and confiscate the proceeds of a domestic predicate offence. This is in part due to the value of proceeds generated by domestic predicate offending being relatively low. Also, Police may consider the penalty for conviction of the predicate offence as being sufficient punishment, and to investigate further would not be an efficient use of resources. It

is noted also that reparation orders to compensate victims can be sought at sentencing for the predicate offence which may make proceedings under PoCA somewhat redundant from a local law enforcement perspective.

Notwithstanding this, in 2016 a former Member of Parliament and Minister of Marine Resources was imprisoned for 6 months after being convicted of corruption. (4) This was the first time a serving Minister of the Crown had been imprisoned for corruption. It was decided that the former Minister (who was Minister of Marine Resources at the time the crime occurred) used his position as Minister to obtain financing for a personal business venture in consideration for granting fishing licences to a Chinese company. The amount of the loan was NZ$250,000. In May this year CI Solicitor General made application to CI High Court under PoCA to seize the assets of a company owned by the former Minister or obtain a pecuniary penalty against the former Minister for the benefits he derived. This is the first time an application has been made in CI under PoCA.

Domestically the number of prosecutions and convictions of individuals who have taken part in ML of illicit proceeds from abroad is zero. There were no cases of ML reported to the Police during the period 2014 to 2016.

It is understood that none of the financial crimes committed in the period 2014 to 2016 involved a financial institution, TCSP, law firm, or any employee thereof in the course of their employment, or other CI professional advisor.

As at the end of 2016 the Police had received no foreign reports or requests in regards to organised crime or organised crime groups operating in CI. Similarly, there is no evidence of terrorist financing, terrorist acts or terrorist groups operating in CI.

There were no confirmed cases of illicit trafficking of arms, drugs or stolen goods in to or out of CI in the period 2014 to 2016.

Each of the drug offences reported within the period 2014 to 2016 was in relation to domestic cases of possession and use of marijuana and related utensils. However, the Police has noted that whilst the level and nature of drug activity and offences in CI are not high, **"**the disruption of illicit drugs trafficking is assessed as a one of the highest priority transnational crime challenges for the Pacific due to various source countries, transhipment routes, importation and production methodologies and transnational crime syndicates operating in the Pacific. The Pacific region will continue to be targeted as transhipment points for consignments of illicit drugs from South America and Asia, driven by demand within the lucrative Australian and New Zealand markets.". (5) Police and Customs therefore remain vigilant to this potential threat despite apparently not yet having been exposed to it.

Domestic Tax Evasion

Between 2014 and 2016, a total of 29 cases of tax evasion were investigated by RMD, 15 of which were prosecuted. A total of 14 enforcement actions were undertaken during the same period with 27 warning letters issued and 21 flight bans issued to prevent taxpayers absconding overseas without paying their tax. In 2014, 2015 and 2016 the total sums of $648,709.00, $811,220.00 and 770,447.36 respectively were recorded as proceeds from tax evasion. (6)

Table 2. Action taken by RMD

Revenue Management Division	2011 -2013	2014-2016
Evasion Investigation Cases Undertaken	12	29
Prosecution	3	15
Enforcements Actions	14	50
Warning Letters	131	27
Flight Bans	20	21

Table 3. Proceeds from Tax Evasion

Proceeds from Tax Evasion 2011 – 2013	$ 124,395.00	$ 741,625.00	$ 1,359,100.00
Proceeds from Tax Evasion 2014 – 2016	$ 648,709.00	$ 811,220.00	$ 770,447.36

In recent years RMD has taken a stricter approach to the filing of tax returns and payment of tax by individuals and businesses. It is that remedial work that has given rise to the relatively large amounts of unpaid tax discovered. In the past, the failure to report and pay tax has been due to CI residents not being motivated by enforcement authorities to do so, more than (with some exceptions) the intentional avoiding or evading of payment. RMD and the Courts usually take a practical position when imposing penalties and fines for non-payment of tax, seeking agreed and workable repayment plans to enable offenders to keep working in order to repay the tax debt.

Currency

Part 8 e. of this Report provides more detail of cash declarations and undeclared cash at CI borders.

It is noted that a duty free shop at the Rarotonga International Airport notified Police in October 2016 of a customer presenting a counterfeit NZ$100 note. Police identified and questioned the customer but did not lay charges. There was insufficient evidence to show that the person had any knowledge that the NZ$100 note was counterfeit.

In its response to FIU's request for NRA 2017 information, Police noted "Overall, the level of the associated money laundering threat committed domestically is generally **LOW.** However, the lack of effectively pursuing money laundering investigations by law enforcement agencies including the proceeds of crime actions relating to domestic predicate crime is of concern." (7)

International Predicate Offences

The financial flows in and out of CI are not high relative to international levels. CIs' relatively small population and domestic economy, and the fact that the funds held within the sole private bank in CI, and the assets under the administration of TCSPs, are ultimately owned by non CI residents, would indicate most predicate offences take place outside CI.

Tax evasion and fraud are the most likely international predicate offence threats to CI. The issues raised in foreign requests for information and suspicious transaction reports (STRs) reflect this as approximately 80% relate to tax and fraud matters.

CI is regarded in international circles as a "tax haven" given the existence of its offshore financial services industry and the opportunity for non CI residents to establish entities and legal arrangements under the offshore l legislation and not be charged any CI tax, duties or levies on any income, gains, property transfer etc. The prospect of non CI residents using CI financial system or its service providers to assist in evading their domestic tax regimes is therefore real. At present the statistics would indicate that the threat has not yet manifested into ML in CI.

Summary

ML is a criminal offence in CI. Predicate offences are those offences from which proceeds may be generated giving rise to ML charges. CI does not require a predicate offence to have been prosecuted with conviction before ML charges can be laid. Other points to note regarding predicate offences:

- There is a wide range of "serious offences" being predicate offences to ML;
- To date there have been no reports, investigations, prosecutions under or convictions of the ML offences;
- Domestic predicate offences tend to generate relatively small amounts of proceeds used for lifestyle purposes with ML and PoCA prosecutions not being practical;
- Domestic tax evasion is usually dealt with by RMD and the Court by way of an agreed and workable repayment plan to enable offenders to keep working in order to repay the tax debt;
- Police has indicated concern at the lack of resources to investigate ML;
- It is assumed most predicate offences, and those of real value, take place outside CI with tax evasion and fraud being the most likely.

---

1. *sections 280A (2) and (3) CA*
2. *section 280A (5) CA*
3. *information provided by Police*
4. *Police v Bishop [2016] CKHC 15; CR 594.2015, 25 August 2016*
5. *Police response to request for NRA 2017 information*
6. *RMD response to request for NRA 2017 information*
7. *Ibid note 5 above*

5. Primary Threats

In the context of AML/CFT, the FATF has through its literature defined risk to be the function of three factors; threat, vulnerability and consequences. (1)

A threat is defined as a person or group of people with the potential to cause harm. This includes criminals and terrorists, their funds and activities.

A vulnerability is seen as something that can be exploited by a threat or that may support or facilitate criminal or terrorist activities. Examples being, weaknesses in AML/CFT systems or controls that allow a particular sector, industry, service or product to be misused for ML/TF/FOP objectives.

Consequences refers to the impact or harm that ML/TF/FOP may cause and includes the effect of the underlying criminal or terrorist activity on financial systems and institutions, as well as the economy and society more generally. It is noted that some threats and vulnerabilities may have nominal effect whilst others are much more significant.

Determining the primary threats

National risk assessments typically distinguish between domestic and international ML/TF/FOP threats. In quantifying and prioritising those threats regard is given to, amongst other things, the size of a country's population, the make-up of its economy, the size of its domestic economy and the reliance placed on international sources for goods, revenues and funding.

CI's small population and GDP, relative to international levels, have previously been noted. (2) CI relies heavily on international sources for goods, revenues and funding. The main sources of government revenue are the tourism, fishing and financial services industries each of which rely heavily on non- CI residents for their business and revenue.

Fund flows into the country through the banking system are small relative to neighbouring Pacific countries and other financial service centres with whom CI competes for financial services business.

Domestically, the potential for ML exists however the volumes and values of domestic financial and asset transactions together with the number of prosecutions of domestic offences that are predicate offences to ML, indicate the domestic ML threat is not a significant or at least a primary threat. The volume of domestic crime tends towards minor theft and burglary as opposed to financial crimes, such as fraud and corruption. See Part 4 of this Report for domestic predicate offence information.

In light of factors such as: the size of the population and domestic economy; the nature of the activity within the domestic economy; the relatively low level of domestic crime and therefore predicate offences to ML/TF/FOP; the reliance of CI on international sources of business and revenue; and the amount of funds entering the CI financial system from foreign sources, the primary ML/TF/FOP threat to the CI, in general terms, is international in its origin.

The NRA 2015 noted that the threat of ML/TF/FOP to the financial institutions and TCSPs in CI was high, due to their international business and customers. It also considered that the risk presented to CI financial institutions and TCSPs from international fraud was high. However, the overall vulnerability was considered to be at a medium level given the effective oversight and supervision of those sectors by FSC and FIU.

The ML threat indicators (Part 6 of this Report) provide support for the assertion that the primary ML/TF/FOP threat to CI is international in origin. Therefore, the sectors and industries most at risk from the threat would be those with international customers. Foreign criminals may be looking to access the CI banking system to launder the proceeds of crime, or simply use CI service providers to assist in holding, hiding and moving assets that are the proceeds of crime, whether those assets are in CI or elsewhere. In addition, CI service providers may be used to assist in committing a crime that

will generate proceeds. It should be noted that CI businesses that operate internationally are also exposed to money laundering threats in the countries in which they operate.

Summary

In summary:

- The primary ML/TF/FOP threat to CI comes from international sources;
- Each CI service provider with international customers and business are exposed to some degree to this threat;
- Domestic predicate offences committed suggest ML from domestic sources is not a primary threat.

---

1. *FATF Guide National Money Laundering and Terrorism Financing Risk Assessment, February 2013*

6. Indicators of ML Threat

There are a number of indicators available to assist in assessing the ML/TF/FOP threats to which CI is exposed. They include:

a. Suspicious Transaction Reports (STRs)

Section 11 (1) FTRA 2004 provides that where a "reporting institution suspects or has reasonable grounds to suspect" that any information it has "concerning a transaction or attempted transaction may be:

- Relevant to an investigation or prosecution of a person or persons for a serious offence, a money laundering offence or a financing of terrorism offence; or
- Of assistance in the enforcement of the Proceeds of Crimes Act 2003; or
- Related to the commission of a serious offence, a money laundering offence or a financing of terrorism offence."

the reporting institution must, within 2 working days of forming that suspicion, report the transaction to the FIU.

Penalties exist for failing to report. Under FTRA 2004 an individual may be fined up to NZ$20,000 and/or imprisoned for a term of up to 2 years. A corporation may be fined up to NZ$100,000. (1) FTRA 2017 increases those penalties to a fine of up to NZ$250,000 or imprisonment for a term of up to 5 years. A corporation may be fined up to NZ$ 1 million. (2)

Auditors of reporting institutions and "supervisory bodies" (3) are also required to report any transaction or attempted transaction where they have reasonable grounds to suspect that information they have regarding such a transaction may be relevant to the investigation or prosecution of a serious offence, money laundering offence or a financing of terrorism offence. The same provision existed in FTRA 2004, but evidence suggests no such STRs have been filed.

Table 4. STRs filed with FIU pursuant to section 11(1) FTRA 2004

Sectors	2014	2015	2016	2017 to 31/3/17
Banks	26	32	24	9
TCPS	4	6	9	1
Money Remitter	-	-	3	4
Audit	1	-	-	-
DNFBP	-	1	-	1
Voluntary	-	-	3	-
Total	**31**	**39**	**39**	**15**

Table 5. STRs related to domestic and foreign activity

Activity	2014	2015	2016	2017 to 31/3/17
Domestic	17	19	19	12
Foreign	14	20	20	3
Total	**31**	**39**	**39**	**15**

- **Table 6. STRs referred to Police by FIU for investigation**

Dissemination	2014	2015	2016	2017 to 31/3/17
Police	-	3	3	-

No prosecutions have resulted from those STRs related to foreign activity investigated by Police.

Of the 39 STRs filed with FIU in 2016, 20 related to foreign activity. Of those 20, 9 suspected predicate ML offences, e.g. fraud, theft, tax crimes. FIU notified the Financial Crimes Enforcement Network (**FinCEN**), being the US equivalent of FIU, of those reports. It is understood that FinCEN would respond through the Egmont Secure Website (**ESW**) if further information is required. It is also understood that no information has been requested at this stage.

The features of the available STR information are:

- The small number of STRs filed over the period;
- Approximately 80% of STRs are filed by financial institutions (banks, money remitter);
- Fairly even split between domestic and foreign activity leading to filing;
- Low percentage of investigations and no prosecutions.
- Information sharing with FinCEN

The limitations and restrictions on STRs and filing pursuant to FTRA 2004 will be discussed in Part 9 below when considering the effectiveness of AML/CFT measures in place.

b. International Requests

CLO

Formal requests for assistance in criminal matters received by CLO pursuant to MACMA for the 7 year period 2010 to 2016 are detailed in Table 7 below. These requests were made through diplomatic channels to CI Attorney-General (**AG**) and processed by CLO. Each request from US came from the United States Department of Justice (**UNDOJ**).

Table 7. Mutual legal assistance in criminal matters requests from foreign countries 2010 to 2016

MLA Assistance Type	USA Request Includes supplementary requests	USA Orders	UK Request	Argentine Request	Australia Request	Vietnam Request	Hungary Request	Comments
Production of Property Tracking Document Orders	9	9						Includes supplementary requests, in each case property tracking documents were produced and couriered to USDOJ
Restraint of Funds	2	2 (one made ex parte)						In each case funds were restrained and repatriated by consent of the US offender
Forfeiture Orders	1	1						Funds forfeited and repatriated to USDOJ
Taking of Evidence in Cook Islands	1	1						One hearing held in Cook Islands High Court with USDOJ representatives present
Serving documents	1					1		Documents served
Miscellaneous information			1	1	1		1	Requests made but no orders pursued
	14	**13**	**1**	**1**	**1**	**1**	**1**	

No requests for legal assistance were made to the AG/CLO pursuant to MACMA in 2015 or 2016.

CLO advise that the 9 USDOJ requests relate to transfers into CI financial system via the TCSP sector.

In January 2017 a request was received from USDOJ for production of documents from the sole CI private bank. CLO obtained a production order by consent and on 17 February 2017 sent the released documents to the USDOJ.

RMD

Since 2014 RMD has received 4 requests from TIEA partners for information pursuant to TIEAs in place. Of those requests there was one each from New Zealand, Norway, Sweden and Germany. Each of the TIEA requests was TCSP related. RMD advises that it has never received any requests directly from IRS as CI does not have a TIEA with US. US requests for tax information are made directly by IRS.

FIU

FIU is a member of the Egmont Group. (4) It receives requests for information through ESW. In the period 2014 to 2016, 4 requests for information have been received through ESW, 3 of which were from FinCEN and 1 from authorities in St Kitts and Nevis. Each request related to a CI offshore entity or legal arrangement with a bank account in CI. Each request was responded to.

Features of this formal mutual assistance information are:

- A small number of formal requests; (9 MACMA requests over 7 years, 4 TIEA requests over the last 3 years, 4 ESW requests over 3 years);
- A significant percentage of formal requests come from US;
- All 9 US requests under MACMA relate to the financial services industry and in particular the wire transfer of funds from US to CI;
- Each formal request has been responded to and dealt with;
- Only 1 MACMA request received in the last 2 and a half years. This may be explained in part by the fact that the USDOJ had a change of staff in its Washington DC office in 2014. It appears the new staff did not know who to contact in CI. CI deputy Solicitor General was asked for contact details at a meeting in Federated States of Micronesia by the US prosecutor based in the US Embassy in Philippines. The 2017 request was received shortly after.

It is understood that informal requests from foreign competent authorities are also received by law enforcement agencies in CI in relation to foreign ML offences and financial misconduct matters. The FSC has the following information available in relation to requests it has received or assisted with in the period 2014 to 2016:

FSC

- 4 March 2016 – US Securities Commission (**SEC**) requested the possible registration of a foreign restraining order. It was advised by FSC that as it was a civil forfeiture proceeding it could not be registered but assistance may be available under FIUA. There is no further information available as to whether FIU was asked to assist by FSC or whether the SEC made such a request of FIU. As a result of this request from SEC, the sole CI private bank made a policy decision to cease services to international money service businesses, including foreign exchange and trading firms, and subsequently closed 14 accounts.
- 16 August 2016 - Papua New Guinea Companies Office (**PNGCO**) requested information on the beneficial owners of an international company. PNGCO was investigating alleged fraud and illegal transactions/businesses involving farmland and cattle in PNG. FSC referred the matter to FIU for follow up. FIU provided the information requested.
- 15 December 2015 - SEC requested bank records for two bank accounts held with the CI sole private bank. SEC was investigating whether an LLC established in Nevis had violated US federal securities laws by conducting unregistered broker-dealer activity and by misappropriating investor funds. FSC referred the matter to FIU who requested information from the private bank and a response was sent to SEC on 3 February 2016. A request for further information was received from SEC on 31 January 2017 and documentation provided on 5 May 2017. No CI TCSPs were involved in this matter.

FIU

- September 2016 - A direct request was made to FIU by IRS who were investigating a US person for fraudulent activity carried out in the US. In June 2015 the US person had transferred US$2,500 to a CI solicitor as a retainer to set up a trust. The trust was never established. In May 2017 a further request for information was made regarding the transfer of US$6,000 made to a CI TCSP on 10 May 2015 by an associate of the US person under investigation. FIU is making enquiries and has co-operated with IRS at all times. The investigation is ongoing
- March 2017 – UK Metropolitan Police requested information on a former CI bank licensee as part of a UK ML investigation. The matter is still in progress with representatives of Scotland Yard due in CI on 31 August 2017 for further investigation.

There does not appear to be a register for recording such requests or a system to ensure such requests are communicated to the appropriate agency for action.

Features of this informal request information are:

- The relatively small number of requests recorded;
- Request predominantly appear to be related to CI offshore industry structures and/or bank accounts;
- Each request has been promptly dealt with;
- Not clear if informal request records are complete and appropriately documented.
- 3 of the 5 informal requests noted come from US authorities.

c. Typologies

Typologies are useful to illustrate generally the nature and extent of ML/TF/FOP threats that exist and from where they arise, as well as how criminals might specifically exploit the financial system or the services offered by a country to carry out their illegal activity. 2015 Typologies Report is the only typologies report produced by the FIU to date. A second typologies report is currently being worked on. The typologies and case studies provided in 2015 Typologies Report are taken from information reported to FIU in 2015 and provide a good illustration of how CI and its financial system may be exposed to the international threat of ML/TF/FOP.

18 of the 29 examples noted in 2015 Typologies Report involved foreign nationals seeking to transfer funds into and out of CI financial system. A significant number involved suspected fraudulent activity and illustrated the emergence of cyber fraud as a growing threat.

Structuring [5] featured 4 times, where amounts and regularity of transfers suggested customers (2 of which were foreign nationals) were seeking to avoid the legal reporting threshold of NZ$10,000. 5 examples involved foreign nationals who were found to be the subject of criminal investigations overseas.

Of the 5 Case Studies provided, only one involved the activity of a foreign national and CI offshore industry.

It is not clear from 2015 Typologies Report if each of the 29 examples provided were also the subject of STRs filed by the relevant reporting institution.

It can be assumed that none of the cases mentioned in the case studies in 2015 Typologies Report involve the prosecution of the offence of ML pursuant to s280A CA, as no such cases have been commenced in CI. 3 of the 5 cases are noted as being still under investigation.

d. Exposure to jurisdictions with high threat levels of ML/TF/FOP

Over 80% of information requests from foreign authorities, whether formal or informal, have come from US authorities. This is not surprising given the level of business activity with US persons through the banking sector and TCSPs relative to residents of other jurisdictions. As expected, given the nature of their businesses, all but a few of the STRs were filed by financial institutions (banks and money remitters) or TCSPs. Those STRs filed by TCSPs reflect the level of business activity with US persons.

International fund flow information received from the licensed banks reflects the nature of each bank's business and client base.

CI financial sector consists of 4 licensed banks and 1 licensed money change and remittance business. Of the licensed banks, 1 is government owned, 2 are regional banks with head offices outside CI and the fourth is a private bank. More information on each bank and their business is provided in Part 7 of this Report. The government owned bank is used by CI residents for domestic transactions and fund transfers to and from CI for personal and business reasons. It has indicated that the 2 jurisdictions to which most funds are transferred to and received from are New Zealand and Australia. In 2016 total funds it transferred to NZ was approximately NZ$11.3m, and received from New Zealand was approximately NZ$13.1m. Total funds received in 2016 from all jurisdictions was approximately NZ$15.6m and transferred out was approximately NZ$15m**.** It has further indicated transfer activity of less than NZ$800,000 over the three-year period 2014 to 2016 with jurisdictions regarded by the FIU as "high risk countries". **See Annex 3: High Risk Countries**. These countries are not necessarily the subject of FATF or other international body blacklists or sanctions but more generally regarded as tax havens, being countries having favourable tax regimes for non-residents. It has also indicated no activity with any UN sanctioned regime or individual or entity contained in the Consolidated UN Security Council Sanctions List (6) and only one relatively small transfer to a country regarded by FATF as having a weak AML/CFT regime, that being a transfer of NZ$23,624 to Vanuatu in 2015.

The sole private bank's client base is primarily high net worth foreign individuals with accounts in the name of CI offshore and other foreign entities/legal arrangements. It indicates that for the period 2014 to 2016 the 3 jurisdictions to which most funds were transferred were US, China and Switzerland. The 3 jurisdictions most funds were received from were US, Hong Kong and Switzerland. During the period 2014 to 2016, total funds transferred to US was approximately USD196m and received from US was approximately USD258m. Total funds received in 2016 from all jurisdictions was approximately USD216m and transferred out was approximately USD213m. The private bank is the sole domestic supplier of banking and investment services to the CI TCPS whose client base is made up of up to 90% US persons. Transfers to and from jurisdictions such as China, Hong Kong and Switzerland indicate Asian and European business but at less than 10% of the volume of the activity it has with US. The private bank has indicated reasonable levels of transfer activity with jurisdictions regarded by FIU as "high risk countries", being activity with Austria, Cayman Islands, Liechtenstein, Marshall Islands, Mauritius, Monaco, Singapore and Switzerland, where it is transferring funds to other banks or investment houses.

The private bank has also indicated no activity with any UN sanctioned regime or individual or entity contained in the Consolidated UN Security Council Sanctions List and relatively little transfer activity with countries regarded by FATF as having weak AML/CFT regimes. That activity amounted to approximately US$137,800 in total over the period 2014 to 2016, with US$120,000 of that being transferred to Laos in 2014, US$9142.36 received from Afghanistan in 2014 and US$7802.90 transferred to Bosnia-Herzegovina in 2015.

The regional bank with its head office in Australia shows New Zealand, Australia and USA as the 3 jurisdictions most funds were transferred to over the 3 year period 2014 to 2016, with most funds being received from New Zealand, Australia and Fiji. Total funds transferred to and received from New Zealand in 2016 was approximately NZ$117.1 million and NZ$30.6 million respectively. In regards to activity with New Zealand that clearly reflects where CI has most business, trade and personal ties. Total funds received from all jurisdictions in 2016 was approximately NZ$78.8 million and transferred out was approximately NZ$161.1received million. The bank has indicated relatively small transfer activity with "high risk countries" in 2016 being approximately NZ$4.65 million received (of which NZ$3.42 million came from Singapore) and approximately NZ$1.65 million

transferred out. The bank has also indicated no activity with any UN sanctioned regime or individual or entity contained in the Consolidated UN Security Council Sanctions List and relatively little transfer activity in 2016 with countries regarded by FATF as having weak AML/CFT regimes. That activity amounted to approximately NZ$531,000 transferred to and NZ$73,500 transferred from Vanuatu as well as NZ$903.93 transferred to Uganda.

The fourth licensed bank has indicated no activity in 2016 with any UN sanctioned individual or entity contained in the Consolidated UN Security Council Sanctions List. Its activity in 2016 with countries regarded by FATF as having weak AML/CFT regimes amounts to US$6,623,739 transferred to Vanuatu and US$17,244 received from Iraq, US$3,992 received from Laos, US$40,090 received from Syria and US$5,294 received from Vanuatu.

e. **Customs – Border Control and Currency Declarations**

Section 7 CDA requires each person entering or departing CI to make a "truthful currency declaration" each time they enter or leave. Offences against CDA may result in a fine of up to NZ$20,000 or imprisonment for up to 2 years. CDA repealed section 96 (1) PoCA. (7) Section 261(4) of CRBPA makes it an offence for a person to knowingly (a) make a false declaration, (b) provide a document that is not genuine or (c) provide a document that is erroneous in any material particular. The penalty for doing so is a fine of up to NZ$30,000 or imprisonment of up to 6 months (8) Therefore, by definition, these are serious offences and predicate offences to ML.

In the period 1 July 2014 to 31 December 2016 Customs received 98 border currency reports (BCRs) from individuals declaring that they held in excess of NZ$10,000 (or foreign currency equivalent) upon their arrival into or departure from CI.

Customs officers (as defined in section 4 CRBPA) have the power to question anyone crossing the CI border with currency whether or not they suspect a breach of CDA. (9) However, in order to search someone in relation to currency, the Customs officer must have reasonable grounds to suspect the person is holding undeclared currency, or currency that is the proceeds of financial misconduct or unlawful conduct. (10) Similarly, a Customs officer can question anyone entering or leaving CI in relation to whether that person "has or has had any dutiable, prohibited, undeclared or forfeited goods" (11) in his/her possession.

In the period 2014 to 2016 only 1 instance was detected of persons carrying undeclared currency (i.e. currency in excess of the minimum amount being NZ$10,000 or currency equivalent). The person in question was holding USD10,083. The detection was due to intelligence held by FIU on the person before she arrived in CI. FIU had alerted Customs and Police and she was charged under section 261(4) (c) CRBPA. The charge was eventually dismissed. Charges were not laid under PoCA as there was insufficient evidence to prove the currency in question was to be or had been used to commit a criminal offence.

It is noted that 32 of the 98 BCRs relate to individuals carrying currency on behalf of the sole money change and remittance business in CI. Each indicates that the currency is to be deposited into that company's account in New Zealand.

The method for detecting undeclared currency is reliance on BCRs and truthful declarations, and intelligence received from other sources prior to the arrival of the offender. The Rarotonga International Airport has security scanners, but they do not specifically recognise cash held within clothing, bags etc.

Summary

The ML/TF/FOP indicators do, collectively, indicate the existence of ML/TF/FOP threats to CI. The relatively small number of STRs, international requests and the volume and value of transactions

involved, should not be used as a reason to be complacent or less vigilant. The international threat appears more prevalent and significant than the domestic one. The most notable factors are:

- Most funds transferred into the CI banking system are from US and most funds transferred out go to US;
- The majority of the sole private bank's activity is conducted through CI offshore and foreign entities or legal arrangements. That includes, but is not exclusively, LLCs, international trusts and companies and foundations established, administered and operated by CI TCSPs, whose client base is up to 90% US based;
- Nearly all STRs filed are filed by banks and TCSPs.
- A significant number of foreign requests for information come from the US;
- Typologies suggest criminals are simply looking to open bank accounts in CI to hold funds and use when required. There is no indication of CI being used for more sophisticated methods to launder proceeds, e.g. trade based ML, or that these structures are part of more complex arrangements or layering or involved with terrorist or organised criminal groups;
- There is no evidence of exposure to regimes, individuals or entities on UN Security Council sanction lists and only nominal exposure to countries regarded by FATF as having strategic AML/CFT deficiencies;
- There has been only 1 recorded transfer to a jurisdiction where terrorist or organised crime groups are known to operate and reside, being a transfer to Afghanistan of USD9,142.26 in 2014.
- 2 transfers have been recorded as received from jurisdictions where terrorist groups are known to operate and reside, being US$17,244 from Iraq and US$40,090 from Syria.

The evidence available therefore suggests the primary ML threat to CI is from international sources, predominantly US. The sectors/industries/businesses at most risk are those exposed to international customers, most notably the financial institutions and TCSPs. TCSP and private bank customers are typically high net worth individuals (HNWIs), entrepreneurs and businesses with international structures and interests. The main threat would therefore appear to be those customers seeking to use CI banking and TCSP services to hold, hide and transfer assets that are either the proceeds of crime or to be used in the commission of a crime.

---

1. *section 11(2) FTRA 2004*
2. *section 63 FTRA 2017*
3. *"supervisory bodies" defined in s4 FTRA 2017 as "any institution or authority established in the Cook Islands to regulate or supervise any 1 or more reporting institution"*
4. *The Egmont Group is a global body of 154 financial intelligence units that provides a platform for the secure exchange of expertise and financial intelligence to combat ML/TF/FOP www.egmontgroup.org*
5. *"structuring" is also known as smurfing in banking industry jargon, is the practice of executing financial transactions such as making bank deposits in a specific pattern, calculated to avoid triggering financial institutions to file reports required by law,*
6. https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list
7. *section 29 CDA*
8. *section 261(5) CRBPA*
9. *section 9 CDA*
10. *section 10 CDA*
11. *section 178 CRBPA*

7. The High Risk Sectors and Other Areas for Consideration

The following will focus on those sectors/industries/businesses, both financial and non-financial, that have exposure to the ML threat posed by HNWIs, entrepreneurs and businesses with international structures and interests, some of who may be seeking to use CI financial system and service providers to hold, hide and transfer assets that are either the proceeds of crime or to be used in the commission of a crime. Exposure to such a threat may also result in CI service providers unwittingly assisting in or facilitating the commission of a crime that will generate proceeds.

Each relevant sector, industry and business has vulnerabilities which need to be recognised, understood and managed to minimise the potential consequences to CI. Compliance with the laws and regulations in place and focussed supervision are paramount in controlling and mitigating the ML threat.

This Part will focus on the primary ML threat as opposed to TF/FOP threats. Whilst TF/FOP threats are not being disregarded, and will be discussed in Part 8 of this Report, evidence suggests that TF/FOP does not provide the same degree of risk to CI at this time as ML does.

Financial Sector

Banking

CI banking industry is small in comparison to international and regional standards. It is governed by the Banking Act 2011 (**BA**) which provides for domestic and international banking business. The FSC administers the BA and can issue domestic and international banking licences.

CI banking industry consists of 4 licensed banks, 3 of which have licences to conduct international banking business. A domestic banking licence is a pre-requisite to obtaining an international banking licence. International banking business is business conducted with a person who is not a resident of CI, whereas domestic banking business is banking business that is conducted with a person who is a resident of or visiting CI, or if that person is not a resident the business is conducted in CI currency. **(1)**

FSC is host regulator to two of the banks with international banking licences. They are regional banks with their head offices outside of CI – one in Australia, the other in Papua New Guinea. They provide a full range of retail and commercial banking services to CI and non CI residents, individuals, corporates and legal arrangements but do not (by virtue of a business decision made by both) provide accounts or services to entities or legal arrangements set up by CI or foreign TCSPs. They do not therefore work within the offshore industry. They do provide online banking and debit card services to their customers, and credit cards to corporate customers.

The third bank with an international banking licence is a private bank operational only in CI. It provides private banking services (custody, asset management and investment) to HNWIs and entrepreneurs directly as well as through the services of CI and foreign TCSPs. As at 31 December 2016 the private bank had 1020 operational accounts holding approximately USD300m. 650 accounts are in the name of corporations, 231 trusts, 10 partnerships, 6 foundations and 123 individuals. 463 of those accounts were referred through CI TCSPs and 383 through non CI referrals. The remaining 174 have contacted the bank directly and been sourced without an introducer or intermediary.

The fourth bank, which is only licensed to carry on domestic banking business, is government owned and focusses on providing retail banking services to CI residents.

Each licensed bank is relatively small in terms of staff numbers and size of premises. Senior management and the compliance and operations divisions should be able to discuss matters of concern and identify and assess risk issues without delay.

The small size of the banking sector is well evidenced by the number of licensed banks and the fund flow volumes into and out of CI. The net foreign assets held in CI banking system as at 31 March 2017, through the four licensed banks, was NZ$136.1 million. (2) CI is not regarded as an international or even regional finance centre.

Threats

The main threat to the banking sector is international criminals using it to receive, hold and move funds being the proceeds of crime, or funds to be used in the commission of a crime. The nature of the activities that banks undertake mean there is a high inherent money laundering risk within the sector, however, the relatively small CI banking sector should provide advantages in monitoring and controlling this threat.

Vulnerabilities

The banking sector can be exploited where banks do not have adequate and appropriate systems, controls and procedures in place to know their clients' background, source of wealth and business activity, as well as to monitor the transactions carried out on each client's bank account. The CI private bank is most exposed to the primary ML threat due to the nature and source of its business and given that it has very little face to face contact with clients.

Consequences

Being involved, wittingly or unwittingly, in the laundering of the proceeds of crime would compromise the integrity of CIs' financial system. It would impact negatively on CI's reputation internationally as well as its international banking and trade relationships. Its ability to conduct business regionally and internationally would be at risk with the threat of financial and trade sanctions and black listings being very real. Given CI's reliance on international funding and imports, what is a small and somewhat fragile economy could suffer major harm. One bad headline could have major consequences.

Regulation

The banks are licensed and regulated pursuant to BA. BA requires FSC, as prudential supervisor, to implement internationally accepted standards for the prudential supervision of banking business and to maintain stability and confidence in CI financial system. FSC carries out annual on-site visits to review each licensed bank's compliance with its legal and regulatory obligations.

CI banks are "reporting institutions" and have therefore been subject to FTRA 2004 and now FTRA 2017 and the Regulations. The FIU is responsible for monitoring the compliance of all reporting institutions with those laws and regulations. It carries out annual on-site compliance audits of banks where it has the powers to assess each bank's level of compliance with its obligations to identify and verify its customers (section 6 FTRA 2004) and monitor transactions (section 8 FTRA 2004). It can also assess the effectiveness of their systems and processes in reporting cash transactions of more than NZ$10,000 and suspicious transactions (sections 10 and 11 FTRA 2004). Similar powers exist under FTRA 2017.

Money Changing and Remittance Businesses

There is only one licensed money changing and remittance business in CI. It provides a cash based service with transactions commonly being for less than NZ$1,000. Over the three years to 31 December 2016 it averaged approximately NZ$2.2m in receipts and NZ$1m in payments. The business' surplus cash is taken to and banked in New Zealand. Only nominal amounts are banked in CI. It would appear a significant proportion of the company's business is with CI residents who work in CI on work visas and send money to their families in their home country, and overseas families of resident Cook Islanders and tourists to CI. This is evidenced by Philippines, Fiji and Indonesia being the major recipients of funds from CI, and most payment instructions being received from Australia, New Zealand and USA.

Threats

Due to the nature of the money changing and remittance business, there is an inherent ML risk. In CI the main threat would be criminals looking to transfer cash out of CI or people unwittingly transferring funds to those who wish to use those funds in criminal or terrorist activity. The relatively small sums transacted by the money changing and remittance business would suggest it is not subject to the primary threat of HNWI individuals and entrepreneurs looking to access CI's financial system and service providers.

The licensed CI money changer and remittance business filed 3 STRs in 2016, and none in 2014 and 2015. It is noted however that during FIU's onsite audit in 2016 it discovered a cash receipt of AUD$19,950.00 that had not been reported to FIU as required under section 10 of FTRA 2004. Such offences by a body corporate are punishable by a fine of up to NZ$50,000. In this instance, a warning was given.

Vulnerabilities

The CI licensed money changing and remittance business may be vulnerable to the primary threat of ML as well as TF/FOP if it does not have adequate and appropriate systems, controls and procedures to detect those using its services are not looking to launder the proceeds of crime or fund criminal activity. The threat would appear to be low but not non-existent.

Consequences

Similar to the banking sector, any involvement in the laundering of the proceeds of crime would compromise the integrity of CIs' financial system and cause harm to its international reputation and potentially its domestic economy.

Regulation

Money changers and remitters are licensed under the Money Changing and Remittance Businesses Act 2009, which sets out the licensing and regulatory regime for money or value transfer service providers. FSC regulates and supervises money changing and remittance businesses. The sole CI licensed money changer and remittance business is part of an international organisation and subject to its AML/CFT policies and procedures. It was subject to FTRA 2004 and now FTRA 2017, and is subject to annual on-site audits by FIU.

Insurance

The domestic insurance sector in CI is small in that it serves a resident population of approximately 11,700. The vast majority of insurance business involves the insuring of residential and commercial premises and contents, and other general domestic insurance services such as accident, travel, medical, vehicle and insuring valuable assets e.g. boats, jewellery. There is some life insurance business, but generally simple term life cover and not cover requiring large single premiums such as Universal Life or Variable Universal Life or investment related insurance.

There is 1 Category A licence holder (3) authorised to carry on "insurance business" which includes "domestic insurance business" (as those terms are defined in sections 3(1) and 2(1) Insurance Act 2008 (**IA**) respectively). There is 1 Category C licence holder being authorised to carry on "international business", meaning insurance business that is not "domestic insurance business". (4) There are 4 approved external insurers, and 9 licensed insurance intermediaries being 6 agents, 1 broker, 1 manager and 1 external manager. There are 3 licensed captive insurers in CI.

The FSC licenses, regulates and supervises all insurance business in CI. IA sets out the licensing and regulatory regime for insurers and insurance intermediaries, whereas the Captive Insurance Act 2013 (**CIA**) sets out the licensing and regulatory regime for captive insurance companies.

Only insurance licence holders placing or underwriting life insurance and other investment related insurance are "reporting institutions" and therefore subject to FTRA 2004 and FTRA 2017 and oversight by FIU on AML/CFT matters.

Due to the apparent absence of any notable large single premium or investment related insurance business, the insurance sector is not for the purpose of this Report regarded as a high risk sector subject to the primary threat of ML. It will not therefore be considered in more detail. However, it is expected that NRA 2017 will look further at the insurance sector, the nature and types of insurance business being carried out and products and services being offered by each licence holder. On-site audits of resident insurance businesses and intermediaries should be considered to assess the actual value of insurance being placed and underwritten and premiums being paid. Insurance business is very technical in nature, and products and services evolve quickly.

Designated Non-Financial Businesses and Professionals

The non-financial sector is also exposed to the threat of ML/TF/FOP. In the CI context, some industries and businesses within the non-financial sector, due to the nature of their activity and customer base, may be exposed to the threat of ML/TF/FOP through international sources.

The FATF has issued guidance on DNFBPs that have similar potential to financial institutions for being used for ML/TF/FOP purposes. The FATF has proposed therefore that DNFBPs also be subject to AML/CFT regulation in order to detect, deter and prevent criminal activity.

What is classed as a DNFBP can vary depending on jurisdiction, however FATF generally regard the following businesses and professions as being included:

- Accountants
- Casinos and other gambling service providers
- TCSPs
- Dealers in precious metals and stones
- Lawyers
- Notaries and other independent legal professionals

- Real estate agents

Each of these business and professions are included in the definition of "reporting institution" in FTRA 2004 and FTRA 2017. Other businesses not included in this list may require tailored regulations to counter more specific or unique ML/TF/FOP threats they may face.

TCSPs will be the primary focus of the DNFBP assessment herein, as they are considered most at risk to the primary threat of ML/TF/FOP. Other DNFBPs will be noted but it is expected they will be assessed in more detail in NRA 2017.

TCSPs

There are currently 8 companies licensed to carry on "trustee company business" in CI, as that term is defined in section 5 Trustee Companies Act 2014 (**TCA**). Of those 8, 3 are in the initial stages of establishing their businesses, the remaining 5 are long established having been licensed in excess of 20 years. Each TCSP has very experienced senior management, in some cases having worked in the industry since the 1980s.

A company provides "trustee company business" if it registers an "offshore entity" under CI law, provides a person or service that must be provided by a licensed trustee company under CI law, or provides trust and fiduciary services. An offshore entity is defined in section 4 TCA as any entity established or registered under:

- International Companies Act 1981-82 (**ICA**);
- International Trusts Act 1984 (**ITA**);
- International Partnerships Act 1984 (**IPA**);
- Foundations Act 2012 (**FA**);
- Limited Liability Companies Act 2008 (**LLCA**);

or, the holder of an international or restricted licence under BA; the holder of a Category C licence under IA; and the holder of a captive licence under the CIA.

Any business conducted pursuant to the abovementioned legislation is generally referred to as being part of the CI offshore industry.

TCSPs are treated as financial institutions (as opposed to DNFBPs) under CI licensing laws and regulations and are therefore licensed, regulated and supervised for prudential purposes by FSC. FIU regulates and supervises TSCPS in regards to AML/CFT compliance.

CI's offshore industry was established in the 1980s initially with the passing of the ICA and the original versions of TCA, IA and BA in 1981-82. That was followed in 1984 by the ITA. It was CI Government's intention at the time to create the pre-imminent offshore centre in the South Pacific for the long term benefit of CI. The Trustee Companies Act 1981-82 (repealed by TCA) was passed to facilitate the carrying on of offshore business by providing for the establishment, licensing and regulation of trustee companies authorised to carry on the activities governed by the offshore statutes. It was not until 1989 that CI offshore industry gained some impetus with the passing of the International Trusts Amendment Act 1989. It was this amendment that introduced provisions designed to enhance the asset protection features inherent in a common law trust. These changes came about in response to demand from US attorneys seeking to strengthen the position of their US resident high net worth clients who were finding their wealth at risk due to certain socio-economic factors. US is a highly litigious society and wealthy people will get sued because they can afford to

pay. Also, as a result of that and higher jury awards, professional indemnity insurance becomes too expensive or unavailable.

As seen from the offshore legislation noted above, CI offshore industry provides a fairly standard range of structures that can be used by non CI residents for personal wealth and business planning reasons. The licensed trustee companies will also provide management, administration, fiduciary and accounting services to those entities and legal arrangements. There are no sophisticated or complex investment products offered through the CI offshore industry.

Table 8. Number of entities and trusts registered through CI offshore industry from 2014 to 2016.

TYPE OF ENTITY	*YEAR 2014 (31-Dec-14)*			*YEAR 2015 (31-Dec-15)*			*YEAR 2016 (31-Dec-16)*		
	Current	*New*	*Total*	*Current*	*New*	*Total*	*Current*	*New*	*Total*
International Company (IC)	*740*	*72*	*812*	*812*	*58*	*870*	*870*	*62*	*932*
Foreign Company (FC)	*13*	*0*	*13*	*13*	*0*	*13*	*13*	*0*	*13*
International Trust (IT)	*1666*	*191*	*1857*	*1857*	*190*	*2047*	*2047*	*207*	*2252*
International Partnership (IP)	*4*	*0*	*4*	*4*	*1*	*4*	*4*	*0*	*4*
Limited Liability Company (LLC)	*215*	*43*	*255*	*255*	*56*	*311*	*311*	*53*	*361*
Foundation (FA) not online yet	*3*	*4*	*6*	*6*	*18*	*27*	*27*	*21*	*44*
TOTAL	*2641*	*310*	*2947*	*2947*	*323*	*3272*	*3272*	*343*	***3606***

Whilst it has been in existence over 30 years, in terms of numbers CI's offshore industry is small when compared to its competitors, many of whom have not been in the offshore industry as long. CI registers the existence of offshore entities and trusts on an international register. This is not the case in many other offshore jurisdictions, especially in relation to trusts. It is not therefore possible to compare the number of trust registrations with other offshore jurisdictions. However, in regards to international companies (or equivalents), the British Virgin Islands as at 31 March 2017 had 431,776 international companies registered with 8,695 new incorporations in 1Q 2017 alone. (5) By further comparison, it is understood that Samoa has approximately 30,000 international companies currently registered. (6) As at 31 December 2016 CI had 932 international company registrations.

Approximately 90% of CI licensed trustee company clients and business revenues are derived from US through the provision of asset protection trusts, limited liability companies and related trustee, management, administration and accounting services. Most of the remainder of the offshore business is sourced from Europe and Asia.

Threats

The nature of the activities undertaken by TCSPs means there is a high inherent money laundering risk. TCSPs are generally involved in establishing and administering vehicles to hold, transfer, invest, protect and move assets. Structures can be relatively complex in their design and can distance the ultimate owner from his/her assets. This, by its very nature, is assumed to attract higher risk

customers. Given the proportionately high level of CI offshore business derived from US and that the US clients are HNWIs, it is logical to assume that is where the primary ML threat to CI originates.

The threat of CI TCSPs being used in foreign tax evasion should diminish in light of CI TCSPs' obligations to report to IRS under FATCA and CRS come 2018. In addition, trusts established for US residents are generally not tax driven, they are primarily for asset protection purposes as well as other traditional reasons for using trusts such as succession planning, avoidance of probate and pre-migration and pre-marital purposes. Trusts for US residents are structured either as domestic or foreign for US tax purposes, despite the governing law being that of CI. Those trusts structured as domestic for US tax purposes will contain appropriate wording in the trust instrument and will typically have a US resident co-trustee alongside the CI trustee. The US trustee takes care of all administrative matters including necessary trust reporting for IRS purposes. The trust is for all intents and purposes a US trust. The CI governing law and co-trustee provide protection in the event of future creditor claims against the trust settlor. It is difficult to see such a structure as posing a real ML/TF/FOP threat to CI as all administration, and in many cases assets, are held in the US where the structure would need to be compliant with US AML/CFT rules and regulations.

Vulnerabilities

Given the nature of the services provided by TCSPs there are a number of areas where criminals may look to exploit TCSPs to conceal their criminality and identity. TCSPs must therefore be vigilant in their compliance with CI AML/CFT laws and regulations.

A CI TCSP may, on behalf of customers, hold liquid assets in CI banking system through the sole CI private bank, or may hold them in foreign jurisdictions. In such circumstances, financial transactions would be taking place outside of CI and FIU would not be receiving relevant financial data. CI licensed banks are only required to report electronic transfers into and out of CI. (7) TCSPs have no obligations to report transactions they carry out in foreign jurisdictions and FIU's duty is only to ensure compliance with FTRA 2017. Although in such circumstances criminal proceeds would not be entering CI's financial system, being involved, whether knowingly or otherwise, in any financial misconduct would be damaging to CI's reputation and potentially its economic interests.

Also, it is common that CI TCSPs, as trustees of trusts, hold shares in international companies, or interests in LLCs or partnerships, whether established in CI or elsewhere, but have no control over the underlying entity or its assets. The TCSP does not necessarily provide director or management services. The risk of being involved, whether knowingly or otherwise, in criminal activity will be increased where the TCSP does not undertake due diligence on the underlying entity and its management, including obtaining regular information on the assets and business activities of the entity. The onus will be on the TCSP to understand the nature of the assets and businesses it owns to avoid being associated with assisting in criminal activity and the negative publicity and reputational damage that would ensue. It may be difficult to detect more complicated ML techniques, such as trade based ML, where the TCSP is not directly involved in the management of the entity. However, asking pertinent questions on an ongoing basis about the nature of the business, its management and activity will provide an understanding of what is and might be happening.

FTRA 2017 does not require a TCSP to obtain information on assets it holds, including assets within entities it owns as trustee of a trust. The CDD requirements of FTRA 2017 focus on the ultimate owner of the assets and not the assets themselves. It is also noted that reporting institutions are only required to obtain source of wealth information from a customer the subject of enhanced due diligence. Enhanced due diligence only needs be undertaken on politically exposed persons (**PEPs**) or

persons from jurisdictions regarded by FATF as not having adequate AML/CFT regimes or who have had sanctions imposed. Source of wealth information is not required on any other customer. Understanding how a customer has made his/her wealth would seem essential in order to properly assess the risk associated with accepting his/her assets into a trust or entity, regardless of whether the customer is considered by definition to be high risk or otherwise.

CI TCSPs are not in the business of providing bulk shell or shelf companies to corporate service providers in other jurisdictions for transfer to third parties. Some do however provide standalone international companies, LLCs or partnerships, sometimes with director and/or nominee shareholder services, but often without - generally due to potential personal liability issues. The TSCP may simply provide registered office and registration services. In such instances the TCSP will be required to carry out appropriate CDD pursuant to FTRA 2017 on its customer, but will not be required to obtain any information or due diligence on the management of the underlying entity or its assets or business activities. Again, the risk of being involved, whether knowingly or otherwise, in criminal activity is increased where the TCSP does not undertake such due diligence.

The services offered by the CI TCSPs typically, but not always, result in no face to face meetings with customers. This practice contains inherent risks of abuse by criminals therefore requiring rigorous CDD measures. However, in the context of CI TCSPs this risk would appear to be mitigated by the fact that a very significant part, if not all, of their US business is conducted through introducers, primarily US attorneys, who are licensed and regulated in the US and subject to the US AML/CFT regime, which is FATF compliant. It is generally the practice that TCSPs meet introducers either in CI or US and due diligence is obtained on them. Many of the relationships with US attorneys have been in place for several years.

Consequences

The consequences of TCSPs being involved, wittingly or unwittingly, in the laundering of the proceeds of crime are the same as for financial institutions mentioned previously. The integrity of CI's financial system would undoubtedly be compromised as would CI's international reputation, its banking and trade relationships and its ability to conduct business regionally and internationally. The possibility of financial and trade sanctions and black listings would be very real putting CI's small and somewhat fragile economy in grave danger.

Regulation

Given the risk of TCSPs being exploited by money launderers and other criminals, it is essential adequate control environments are in place to prevent the misuse of this service. TCSPs are licensed and regulated pursuant to the TCA. FSC is the prudential supervisor requiring compliance with TCA, with FIU being responsible for monitoring TCSPs' compliance with FTRA 2004, and now FTRA 2017 and the Regulations.

FTRA 2017 has been enacted to bring CI AML/CFT regime further into line with the Recommendations, as was the TCA and its accompanying regulations which were intended to provide the FSC with the powers to carry out its functions as international standards demanded. The FSC exercised those powers in 2015 when investigating a TCSP for possible breach of Trustee Companies Regulations 2014. The TCSP appealed the FSC's use of its powers to investigate the business affairs and directors of the TCSP. (8) The judge noted that FSC has wide investigative and information gathering powers (9) involving the nature, conduct or state of a licensed trustee company's business, and that those powers had not been misused in this instance.

The FIU is responsible for monitoring the compliance of all reporting institutions with AML/CFT laws and regulations. Currently FIU carries out annual on-site compliance audits of TCSPs where it has the powers to assess each TCSP's level of compliance with its obligations to identify and verify its customers (section 6 FTRA 2004) and monitor transactions (section 8 FTRA 2004). It can also assess the effectiveness of their systems and processes in reporting suspicious transactions (section 11 FTRA 2004). Similar powers exist under FTRA 2017.

FSC's supervisory team also undertakes annual onsite examinations of all TCSPs. Whilst FSC's onsite visit is more focused on prudential matters and legislative compliance, the reviews do also include a sample test of transfers paid in to, and out of, customer bank accounts. The supervision team reviews a selection of customer bank accounts maintained by each TCSP and considers the appropriateness of supporting documentation and necessary checks on funds flowing in and out of those accounts.

Lawyers

There are currently 11 law firms in CI but not all are involved in buying and selling real estate or businesses for their clients or managing their clients' money or assets or setting up and managing companies or trusts for their clients. (10) That being the case, they are not, "reporting institutions" for the purposes of FTRA 2017. Most law firms carry out domestic legal work such as family, land and criminal matters. Some work with the offshore industry providing advice to domestic and international parties on CI offshore industry law and related matters. Some, but not all have active client trust accounts. Instances have occurred where solicitors have received funds from overseas where such funds have been found to be part of suspicious activities. Although it does not appear to be common practice for law firms to use their client trust accounts to receive and hold large sums of international client monies, such instances suggest the legal profession is exposed to the primary ML/TF/FOP threat and will be further examined in NRA 2017.

High Value Dealers

People or businesses that deal or trade in high value items are subject to FTRA 2017 and the CI AML/CFT regime. The Regulations define "high value items" at section 3(1) as personal property of high worth including motor vehicles, antiques, art, pearls, precious stones and metals. The list is not exhaustive and in CI context motor vehicles and pearls would be those items most commonly traded.

There are 25 pearl dealers/businesses in CI. The CI pearl industry has reduced in size, and therefore revenue, over the past 20 years due to fewer farms cultivating pearls, increased competition and reduced demand. Pearl farmers sell pearls on a wholesale basis and in bulk to international customers and retail outlets sell to CI residents and tourists. The pearl industry's exposure to the ML threat comes through its international customer base, Japan having been a prominent wholesale market. However, information on the number and value of transactions carried out by the industry is not available to determine the actual size of the industry or the potential ML threat it might face. FIU did not receive any cash transaction reports (**CTRs**) from pearl dealers in the period 2014 to 2016. Reporting institutions must report any cash transaction greater than NZ$10,000 to FIU. There is insufficient information for this Report to consider the pearl industry a high risk sector but a closer examination should be made in NRA 2017. FIU should discuss with the pearl industry its understanding of the cash reporting requirement.

Motor vehicles are imported into CI by the 6 licensed motor vehicle dealers (**MVDs**). They are sold to CI resident customers. FIU received CTRs from 2 MVDs in the period 2014 to 2016 one of which files CTRs when the transaction value is greater than $NZ10,000, regardless of whether the payment method was cash. That MVD noted that it had 123 sales with value greater than NZ10,000 in 2016, but only 3 were paid for in cash. The remainder were paid for on hire purchase terms over a lengthy

period through electronic payments or cheque. Given the price of motor vehicles relative to CI residents' income levels, hire purchase or long term payment plans are more preferable and practical to large cash payments. Given the focus of this Report is international ML threats, MVDs dealers will not be considered further. It is suggested FIU discuss the cash reporting requirement with those MVDs not currently providing any CTRs.

Real Estate Agents

There are 4 licensed real estate agents in CI. Land in CI is typically sold subject to a leasehold or similar interest. Freehold interests in land are not available for transfer. Foreigners are not able to acquire residential leases per se so the vast majority of transactions involving land are between locals. Foreigners can, through an application process, purchase a business in CI but such transactions are not frequent. Such a purchase may include the lease on land which can be for no more than 60 years. Real Estate Agents have not been considered a high risk to the threat of ML/TF/FOP for the purposes of this Report.

Maritime Cook Islands Limited

Maritime Cook Islands Limited (**MCI**) is a Cook Islands domestic company owned by resident Cook Islanders. It has been appointed pursuant to the Ship Registration Act 2007 (**SRA**) to administer CI Ships Registry and promote CI Ships Register in accordance with the terms of SRA. SRA is administered by Ministry of Transport (**MoT**). At present there are approximately 550 vessels registered on the Ships Register, approximately half of which are privately owned yachts. Annual fees are charged based on each vessel's tonnage and additional fees are charged for administration services provided. MCI charges and retains such fees and through a contractual arrangement pays a portion of those fees to CI Government.

The owners of vessels registered are global and generally corporations. At present the Ships Register records owners from 65 different jurisdictions. The most common jurisdictions for vessel ownership are Marshall Islands, Cook Islands, Singapore, British Virgin Islands, Russia and US. This indicates many owners will be corporations. Other jurisdictions include Panama, Liberia, China, Egypt and Kazakhstan. It was noted one recorded owner was from Iran. MCI advised it was making enquiries in regards to that matter.

Upon registration, a vessel can fly the Cook Islands flag in international waters.

Given the sometimes complex ownership structures of vessels, particularly large vessels used for transportation purposes, e.g. oil tankers, container ships etc., it may not always be straight forward to readily determine ultimate beneficial ownership and the natural person(s) being the owner(s). Ownership structures may involve a number of corporations or other entities, legal arrangements and institutional investors.

MCI's relationship with MoT is contractual. SRA does not in any way regulate the actions or behaviour of MCI in carrying out its functions under SRA. SRA does not require any specific due diligence be carried out on customers, owners of vessels or any representative thereof. Section 14 SRA provides that MCI *may* refuse registration in certain circumstances including where "the owners or any persons associated with the owners are not of good standing having been convicted of an offence elsewhere relating to the operation of *the* vessel" (emphasis added). No guidance is given as to how MCI might go about finding such information or that it must do so, and the conviction must relate to the specific vessel that the owner now seeks to register. The law is therefore very light on CDD and requiring appropriate actions to mitigate the risks of MCI's services being used by criminals, terrorists and those engaged in the proliferation of weapons.

MCI is not a reporting institution for the purposes of FTRA 2004 or FTRA 2017. It is not a business directly involved in the receipt, holding, transfer or investment of funds where such funds could be

the proceeds of crime or to be used in the commission of a crime. It does receive annual registration fees from global sources which range from NZ$2,000 TO NZ$30,000 per vessel. Whilst not involved in the financial services industry, MCI does have international customers who may seek to use its services to facilitate criminal activity. The use of vessels of all sizes to transport illegal goods, weapons etc. is common place.

MCI does have due diligence procedures in place and does keep and have access to information on the vessel's corporate owner and its representative, the vessel's manager and its crew. Crew on vessels can change frequently. Countries such as India and Philippines provide a large percentage of global crew. Members of crew are to be registered in their home jurisdiction and information on crew should be available to MCI at any given time from the International Maritime Organisation (11)

For larger vessels, when seeking registration, the "owner" will generally be a corporation representing all the owners and therefore ultimate beneficial owners. That corporation will grant a power of attorney to an individual authorising him/her to sign documentation on behalf of the corporation. MCI will generally obtain due diligence information on that person and obtain a copy of the corporation's certificate of incorporation.

Given the complexity and uniqueness of aspects of the shipping industry including vessel ownership, and given the ability of vessels to move quickly in international waters and through areas regarded as high risk for ML, terrorist and proliferation activity, it would make sense to regulate MCI's customer take on and due diligence processes, to mitigate the threat of it being used by criminals to facilitate criminal activity. One measure would be for MCI to verify that its customers are not on UN Security Council Sanction Lists. It is noted that FSC has commenced drafting regulations for MCI's business.

In the 15 years the CI Ships Register has existed 4 incidents have been recorded involving vessels flying CI's flag. One of those involved Italian authorities seeking MoT permission to board a vessel in its waters suspected of carrying drugs. Permission was granted. This information was not shared with FIU at the time but could be through appropriate regulation.

More recently MCI rejected a vessel registration application when it became apparent that the vessel was a fuel tanker intended to be taken to Syria. The registration went to another Pacific jurisdiction.

Non- Profit Organisations

As at 31 March 2017 there were 194 non-profit organisations (NPOs) registered in CI. (12) Most NPOs are small domestically run operations involving sports, religious or other community based activities. Most are domestically funded by donations and sponsorships of relatively small amounts. Given the domestic nature of CI NPOs and that evidence of fund flows and information obtained from other ML/TF/FOP indicators does not suggest they are being used or abused by terrorists, they will not be discussed in detail in this Report but will be examined further in NRA 2017.

Government Agencies

Ministry of Marine Resources

MMR is the government agency responsible for the resource management and economic development of CI marine sector. In 2016 MMR collected more than NZ$19 million in revenue,

mainly from international fishing agreements and negotiated settlements for breaches of the Marine Resources Act 2005 (**MRA**) by foreign fishing vessels. Marine resources (mainly fish) also contributed 97% of CI exports in 2016. Marine resources and fishing in particular are vital to CI economy. MMR is responsible, amongst other things, for tracking foreign vessels through CI waters. Its vessel monitoring systems are used to combat illegal, unreported, and unregulated fishing activities in CI waters. The programme includes boarding and inspection of fishing vessels at sea or at port. Surveillance operations can include aerial and sea surveillance with assistance from France, Australia, New Zealand, and US. **(14)**

A fishing vessel entering CI "fishery waters" **(15)** illegally (either unlicensed or without a purpose recognised under international law) will be liable on conviction to a fine of between NZ$100,000 to NZ$1 million. **(16)** Any person caught in possession of or buying, selling or trading fish, fish products or marine life caught in CI fishing waters in contravention of MRA shall be liable on conviction to a fine of up to NZ$500,000 and in addition an amount equivalent to the current retail value of the fish, fish product or marine resource in the market for which it is destined. **(17)**

Any act or omission in contravention of MRA may be dealt with pursuant to judicial proceedings in CI High Court. **(18)** Any proceedings commenced under MRA are however deemed to be civil proceedings. **(19)**. Offences under MRA are usually dealt with by negotiated settlement between MMR and the offending party providing an appropriate amount for the offence, including an amount to cover the market value of any marine resources illegally taken. Contravention of sections 19 and 30 of MRA can result in large fines making such breaches serious offences for ML purposes, but it appears that is not the most pragmatic or preferred method for achieving compensation.

In the years 2014, 2015 and 2016 MMR tracked 36, 36 and 44 fishing vessels respectively in CI fishery waters. The number of foreign fishing vessels caught illegally in CI fishery waters during that period were 1 in both 2014 and 2015 and 8 in 2016. 1 of the 10 illegal fishing vessels was given a warning the remainder have agreed financial settlements, which aggregate approximately NZ$3 million.

---

1. *section 4 BA*
2. *Cook Islands Statistics Office, Statistical Bulletin, Banking Statistics March Quarter 2017*
3. *section 8 Insurance Act 2008 provides categories of and restrictions on insurance licences*
4. *definition of "domestic insurance business" section 2(1) IA*
5. *British Virgin Islands Financial Services Commission 2017 Statistical Bulletin Qtr. 1*
6. *2013 Samoa International Financial Authority annual report indicates over 30,000 international company registrations. The 2013 Annual Report is the most recent published on its website is 2013*
7. *Section 46 FTRA 2017*
8. *Ora Fiduciaries Ltd v FSC 2015 CIHC, Grice J*
9. *ibid at para 112*
10. *section 4(1)(t) Regulations provides definition of lawyers as reporting institutions*
11. ***www.imo.org/en/***
12. ***information provided by MoJ***
13. ***2016 CIFA Audited Financial Statements***
14. ***www.mmr.gov.ck***
15. ***section 2 Marine Resources Act 2005, definition of "fishery waters"***
16. ***Ibid section 19***
17. ***Ibid section 30***
18. ***Ibid section 64***
19. ***Ibid section 65***

8. Terrorist Financing

Whereas ML is the use of financial systems and service providers to conceal and transfer the proceeds of crime, terrorist financing is more concerned with raising funds for criminal activities. CI links ML and TF within its AML/CFT regime and has recently legislated to include the proliferation of weapons of mass destruction into that regime.

CTPWMDA, as amended, has been enacted with the intention of meeting FATF standards on countering the financing of terrorist activities and the proliferation of weapons of mass destruction. CTPWMDA makes it a criminal offence (and a serious offence, being a predicate offence to the 280A CA money laundering offence) to deal with terrorists or terrorist property, finance terrorist acts, or participate in terrorist groups or activities. In addition, it makes it a criminal offence to transport or use a weapon of mass destruction in any way or finance such activity. Offences against CTPWMDA will result in prison terms of up to 20 years and fines up to NZ$1 million.

CTPWMDA establishes the regulatory framework for implementation of UN resolutions and conventions dealing with terrorism, proliferation and the financing of such activity. UN Security Council Sanction Lists are received by MFAI and sent to FIU for distribution to reporting institutions and government agencies. To date there has been no need for CI to implement targeted financial sanctions in accordance with UN resolutions.

CI laws and regulatory framework for countering the financing of terrorism and the proliferation of weapons of mass destruction have yet to be tested as there have been no investigations or prosecutions for terrorist financing or proliferation activities.

There is currently no evidence to suggest the existence of any terrorist groups in CI or attempting to enter CI. Also, there is no evidence of any CI individual, organisation or business knowingly assisting in the financing of terrorist activities. Similarly, there is no evidence of any foreign terrorist group or organisation seeking funding from any CI individual, organisation or business or other assistance with their terrorist activities. CI has not been mentioned in any international media as being associated with or connected to any terrorist group or activity.

No STRs received by FIU have suspected any terrorist activity. There have not been any requests received from foreign authorities for information on suspected terrorist activity. Payments out from CI banks and the money change and remittance business show only 1 payment to a jurisdiction where terrorist groups are known to be based and operate from, being a transfer to Afghanistan of USD9,142 in 2014. This payment was reported to an investigated by FIU. There have been 2 transfers in 2016 received from jurisdictions where terrorist groups are known to operate and reside, being US$17,244 from Iraq and US$40,090 from Syria.

There have been no domestic predicate offences detected that in any way relate to terrorist activity.

This lack of evidence does not mean the possibility that terrorist groups may at some time seek assistance from within CI does not exist. The law enforcement authorities and reporting institutions, particularly financial institutions and TSCPs, as well as NPOs, cannot therefore be complacent and must remain vigilant in identifying such a threat.

Terrorists are known to use low value but high volume fraud activity to fund their operations. Money change and remittance businesses, placement through cash intensive businesses, online payment systems and charities where controls are not stringent, are all methods used by terrorist groups to fund their activities. Whilst there may be no evidence of terrorist financing in CI at present, all of these methods would be available. Sectors/businesses and NPOs that could be exposed to such

threats must be aware of and alert to them and systems and controls must be in place to detect any such activity. Through its compliance audits FIU must test those systems and controls.

Training is required across government agencies, reporting institutions and NPOs on the potential threat posed by terrorist groups with typologies to evidence methods. FIU has access to all ETRs from within CI banking system and is able to proactively search that data for any transactions suspected to be linked to any criminal organisation including terrorists. The data would be a key tool in the detection of any terrorist financing activity. Terrorists operate globally. Research and investigation must not be limited to those jurisdictions on UN sanction lists or more commonly associated with terrorist activity. For example, many major terrorist groups are known to operate to some extent from within the United Kingdom, and each requires funding to some degree.

---

9. Effectiveness of the AML/CFT Measures in Place

Measuring effectiveness

There are no statistics that show annual rates of ML/TF/FOP or by what percentage ML/TF/FOP has increased/decreased from year to year globally, regionally or within individual countries. It is not possible to do so as the only figures that can be provided relate to what ML/TF/FOP activity is actually known, not what is going on undetected. So, as difficult as it is to measure rates or levels of actual ML/TF/FOP, it is also not possible to put a number on how effective laws, regulations, co-operation etc. have been in in combatting ML/TF/FOP.

What can be done is to put an AML/CFT regime in place that proactively combats ML/TF/FOP by detecting, deterring, disrupting, mitigating and ultimately preventing criminal activity and the use of the proceeds of such activity. The foundations for the regime are the legislation enacted and the understanding and implementation of the requirements of that legislation by both the public and private sectors, together with the supervision and oversight by those who ensure compliance with the laws. The effectiveness of the CI AML/CFT regime may therefore be considered in relation to certain desired outcomes, with such outcomes being assessed within the CI context. **(1)**

Understanding

It is essential that both government agencies and reporting institutions understand the potential ML/TF/FOP risks faced by CI to be able to deal with those risks appropriately.

To assist in this regard, and in addition to this Report, it is expected NRA 2017 will provide a comprehensive analysis of the risk of ML/TF/FOP activity in CI. It is also expected that a typologies report will be published in 2017 updating the one published last year. This information will be distributed to government agencies and reporting institutions to increase awareness and understanding. Effective communication being the key to understanding.

NACC is the lead group responsible for formulating and developing CI AML/CFT policies as well as ensuring the institutional framework for AML/CFT covers all relevant areas of CI economy. It is tasked with providing the strategy and direction for CI to follow. NACC is made up of a member of each of 12 government agencies, each of whose knowledge of, involvement and interest in ML/TF/FOP in the international and CI context is varied. To fulfil this role effectively, NACC's commitment to combatting and understanding of ML/TF/FOP is critical. It needs understanding before it can develop meaningful strategy and policy.

CI needs to establish a clear and coherent AML/CFT strategy. The framework needs to be communicated to all stakeholders and the public generally. The laws in place, their purpose and scope need to be clearly explained as does the role reporting institutions and the public generally play in combatting ML/TF/FOP.

FTRA 2017 requires each reporting institution to carry out an assessment of the risk of "financial misconduct" on the part of its business, customers, products, services, distribution channels and new technologies. Financial misconduct is defined in section 4 FIUA and includes ML activity, fraud, financing of terrorism and proliferation of weapons of mass destruction, acts of bribery and corruption and tax evasion. Such risk based assessments should provide a clear indication of reporting institutions' understanding of ML/TF/FOP risks as they apply to and impact their businesses and CI generally.

At present FIU carries out annual on-site audits of all financial institutions and TCSPs primarily to test compliance with CDD and in particular identification and verification. FTRA 2017 allows reporting institutions to take a risk based approach in obtaining CDD, introducing categories of CDD depending

on perceived risk, e.g. enhanced, standard, simplified. This places much greater responsibility on reporting institutions to understand, identify and assess ML/TF/FOP risks and implement appropriate controls, system and processes. The level to which this responsibility is accepted will need robust monitoring by FIU. This in turn will require a much deeper understanding by FIU of the business of each reporting institution.

In addition to the above, other measures could be considered to develop and improve understanding:

- NACC could be a smaller more focussed group, headed by FIU, with agencies who play a key role in the detection and prevention of ML/TF/FOP. Also, representatives of reporting institutions, particularly financial institutions and TCSPs (e.g. Bankers' Association, Trustee Companies Association), being the high risk sectors, should be invited to participate to provide an industry perspective. Collaboration between government agencies and the financial services industry is essential for the understanding and acceptance of CI AML/CFT regime;
- FSC/FIU are planning an AML/CFT education programme. The programme should include both government agencies and reporting institutions to ensure each is aware of and understands their obligations within the AML/CFT regime. This is essential for reporting institutions given the recent enactment of FTRA 2017.

International Co-operation

The recent amendments to MACMA were aimed at increasing the amount of information available to foreign competent authorities requesting information in relation to criminal matters. Part 6 (b) of this Report indicates CI authorities have responded in a timely and comprehensive manner when receiving formal requests from foreign authorities. It also indicates there have not been many formal requests under MACMA, TIEAs or through ESW, and that informal requests may be received by government agencies but the recording of those requests and sharing with other agencies, in particular FIU, needs structure.

Supervision

FSC is the prudential supervisor for licensed financial institutions and FIU oversees compliance with FTRA 2017, MACMA, PoCA and TSA. Both have wide powers to investigate, FSC in terms of the activity of licensed financial institutions and FIU in terms of AML/CFT compliance by reporting institutions. Both have exercised the relevant powers where necessary.

The FSC has provided information on recent instances where it has exercised its powers under section 18 FSCA to issue directives to and place conditions on the activity of licensed financial institutions. In addition, FSC appears to have a robust and rigorous vetting procedure when evaluating new licence applications and has documented evidence of potential licensees being turned away before making an application.

It has been noted (2) that FIU is only able to undertake on-site visits to confirm compliance with FTRA 2017, MACMA, PoCA and TSA (since the enactment of TSA Amendment) and not to detect ML/TF/FOP generally. Where this may be perceived as a weakness, it is also understood that authorities must be seen to be acting fairly and without bias. Such general powers may be viewed with suspicion. All on-site visits are now to be carried out "in consultation with" the reporting institution. (3) FIU also has the power to investigate any suspicion of financial misconduct. In exercising that power and carrying out on-site audits FIU has access to much information. A carefully structured audit programme will assist in detecting ML/TF/FOP trends and activity.

Given the enactment of FTRA 2017, FIU can expand the themes and focusses of its on-site audit programme for reporting institutions and particularly financial institutions and TCSPs. In addition to

testing customer identification and verification, audits can examine the monitoring of financial transactions undertaken, suspicious transaction reporting procedures and a reporting institution's business risk assessment and its understanding of and compliance with the assessment process. FIU may also look to examine structures established by TCSPs where financial assets are not held in CI but controlled by the TCSP in another jurisdiction to determine what information is held and if it forms part of the TCSPs suspicious transaction reporting procedures. Compliance by reporting institutions is essential for the AML/CFT regime to have any valuable effect. Reporting institutions must have genuine motivation to comply.

In addition, FIU could arrange a series of "mystery shopper" exercises to test customer due diligence and suspicious reporting processes**.** (4) Mystery shopper exercises are a way to identify methods and risks of ML/TF/FOP that may not be identified through other means, and to independently assess aspects of a reporting institution's AML/CFT compliance. The knowledge that mystery shopper exercises may take place may provide an incentive to reporting institutions to maintain compliance standards.

A mystery shopper exercise was recently conducted in CI among the retail banks and money change and remittance business to see how front office staff respond to unusual and suspicious behaviour. The finding was that staff questioned did not appear well trained to respond to such behaviour, which could contribute to the relatively low number of STRs filed.

Prevention

Due to the particular circumstances of a jurisdiction and the pace at which criminals adjust and adapt techniques and operations for conducting criminal activity, preventing ML/TF/FOP entirely might not be a viable goal. However, using information, mining data and implementing measures to mitigate the risks of and exposure to ML/TF/FOP methods and channels is certainly achievable.

Typology Reports

Typology reports can assist reporting institutions and government agencies' understanding and recognition of ML/TF/FOP methods and techniques. 2015 Typologies Report was helpful in this regard and the typologies report due out later this year will assist further. Typology reports issued by FATF/APG on an annual basis could be used as part of the training programme implemented by FIU to show the many methods and techniques used by criminals to launder the proceeds of crime and that reporting institutions may not be familiar with due to the narrow focus of their business, customer base and service offering. A reporting institution's policies, procedures, processes and controls, implemented in accordance with the requirements of applicable laws, should provide mechanisms for detection, disruption and deterrence of ML/TF/FOP amongst its own customers, business relationships and activity.

STRs

FIU's compliance audit programme can be used to determine how reporting institutions are applying measures designed to control and mitigate ML/TF/FOP risks. STRs have the potential to detect, deter and disrupt ML/TF/FOP as well as indicate reporting institutions' level of understanding and recognition. The relatively low number of STRs filed in CI may indicate an absence of ML/TF/FOP but may also indicate lack of understanding or confusion as to when to file. If reporting institutions fail to report or selectively report the value of STRs is diminished.

109 STRs were filed with FIU in the period 2014 to 2016, 104 of those were filed by financial institutions and TCSPs. STRs are a primary indicator of ML/TF/FOP activity. To be effective, reporting institutions must recognise criminal activity and the requirement to file an STR in those circumstances. Pursuant to section 11 FTRA 2004, a reporting institution was required to file an STR when it had (emphasis added):

"(1)…reasonable grounds to suspect that…. any transaction or attempted transaction may be:

(a) relevant to an *investigation or prosecution* of a person for a serious offence; or
(b) of assistance in *the enforcement* of the Proceeds of Crime Act 2003; or
(c) related to *the commission of a serious offence*…"

The filing requirements under FTRA 2017 appear far more straightforward. Section 47 FTRA 2017 provides:

"(1) a reporting institution must report to the FIU any activity it has reasonable grounds to suspect is suspicious activity".

Suspicious activity is defined at section 4 FTRA 2017 as being any transaction whether completed or intended that causes suspicion of financial misconduct or a serious offence.

The new definition moves away from the need for investigations, prosecutions or enforcement actions, to simply requiring a suspicion of financial misconduct. This should remove any confusion or misunderstanding as to whether the activity has progressed sufficiently through the criminal judicial process to warrant filing an STR.

Specific training will be required for reporting institutions on the reporting provisions in FTRA 2017, particularly as to when reporting might be expected and how those reports are used by FIU once filed. The interpretation that can be given to section 47 is that filing is not required only where an activity relates to a specific offence that can be identified as being or having been carried out, but to actions generally that appear suspicious.

Section 47 FTRA 2017 and an appropriate interpretation, should result in more STRs being filed providing a better tool and greater intelligence for FIU to assess the ML/TF/FOP risks to to which CI is exposed.

Other reporting

Other reporting designed to assist in the detection, disruption and deterrence of money laundering involves cash movements and the filing of BCRs and CTRs. Those reports however merely reflect the honesty of those required to report. Customs relies on third party intelligence to detect currency smuggling at the border. Customs officers can ask questions but only have powers to search where they have reason to believe a person is holding undeclared currency or the proceeds of financial misconduct. There appears to be little else that can be done proactively to detect undeclared currency. This may be a weakness to be exploited. Customs could consider, if it is not already doing so, advertising CI border currency requirements at each port of entry, on its website and at ports in New Zealand, Australia and US being from where the majority of visitors to CI depart.

A report on every electronic transfer (ETR) of funds within the CI banking system is filed with FIU. One of the licensed banks reported over 12,000 electronic transfers in 2016. FIU is able to search this data and has received training on data mining and how to actively search such reports. Such data and searches could prove a useful tool in detecting ML/TF/FOP however it is understood at present FIU does not have the resources available to maximise this opportunity.

Cease business

Reporting institutions are not required by law to cease a business relationship when a STR is filed and ML/TF/FOP is suspected. Such action may assist in disrupting or deterring ML/TF/FOP activity but it may not be appropriate to do so in each situation. It may be authorities require the activity be continued for investigation and prosecution purposes. Ceasing the business relationship abruptly may put the suspected party on notice allowing them to change the method of their activity. Once an STR is filed, reporting institutions are to maintain enhanced surveillance of the matter and report

subsequent activity to FIU. Communication by FIU with the reporting institution is key once the STR is filed, including guidance on how to deal with the suspected party. Pursuant to section 34 FTRA 2017, FIU has the power to direct a reporting institution how to proceed with a transaction that it has reason to suspect involves financial misconduct. It is suggested that the STR require the reporting institution to advise if it intends to continue the business relationship and if so, why, and once the STR is filed FIU discuss with that institution the appropriate way to proceed.

Rejecting business

Reporting institutions are not required by law, regulation or any guidance to keep records of rejected business. It might be that some of this business is reported by way of STR but where it is not it could be useful information in detecting ML/TF/FOP. If they are not keeping such information, reporting institutions should be encouraged to do so and could form part of the review undertaken by FIU when carrying out on-site audits.

Beneficial Ownership

FTRA 2017 requires reporting institutions obtain CDD on a risk assessed basis. Customers, or persons acting on behalf of customers, assessed as low risk who are not legal arrangements and who do not have nominee shareholders or bearer shares issued, are required to provide simplified due diligence (**SDD**). SDD requires the reporting institution to obtain customer name, address and date of birth details and a copy of a valid identification document, if a natural person, and name, country of incorporation, identification number and registered office address if a legal person. No information is required on any director, manager or ultimate beneficial owner of the legal person.

All other customers, or persons acting on behalf of customers, who are natural persons are also required to provide their nationality and relationship to the customer (if they are not the customer), whereas legal persons are also required to provide their written constitution and identification documentation on each ultimate principle, being any natural person who owns 25% or more of the shares or voting rights in the legal person or who has effective control over the management of the legal person. Similarly, for a legal arrangement, identification documentation will be required on any natural person with effective control over the legal arrangement. No definition of “effective” is provided in FTRA 2017 and there appears no requirement to have identification documentation independently certified or verified.

Where enhanced due diligence is required (i.e. on PEPs or persons from jurisdictions regarded by FATF as not having adequate AML/CFT regimes or who have had sanctions imposed) the only additional information required is in relation to the customer’s or ultimate principal’s source of wealth.

Where the customer, or person acting on behalf of a customer, is a legal arrangement, the reporting institution must obtain identification documentation on the trustee, the settlor or other person on whose instruction the legal arrangement was formed, and any known vested beneficiaries. Identification of discretionary beneficiaries is not required until distributions are made.

All beneficial ownership information is held by the reporting institution and is available to FIU upon request pursuant to section 44 FTRA 2017. If a reporting institution fails to comply with a request it will be liable to fine up to NZ$250,000 or a term of imprisonment up to 5 years if an individual, and a fine of up to NZ$1 million in any other case. Section 59 FTRA 2017 overrides the secrecy provisions or restriction on disclosure of information contained in any other law.

The provisions in FTRA 2017 on disclosure of information to FIU have yet to be tested. Beneficial ownership information has however previously been requested by foreign authorities and provided by FIU (see Part 6 b. herein). There is no evidence to suggest that reporting institutions have failed to comply with a request by FIU for beneficial ownership information.

Identification and verification of beneficial owners is an important part of the process to detect those who may be involved in criminal activity. Although FIU may be able to expand the scope of its on-site compliance audits given the enactment of FTRA 2017, confirmation that appropriate and current CDD is held is vital. In light of FTRA 2017 provisions permitting CDD on a risk assessed basis, FIU will need to ensure such provisions are being applied as intended.

Financial Intelligence

FIU is responsible for receiving and analysing all financial intelligence. It may co-ordinate with other government agencies to investigate such information. FIU receives all ETRs from the financial system, STRs and CTRs from reporting institutions and BCRs from Customs. The analysis of such information is paramount to investigations and for detecting of ML/TF/FOP threats and methods. Due to resource constraints, it is unlikely this information and data is being thoroughly scrutinised for evidence of ML/TF/FOP activity meaning some activity may go undetected.

There appears to be co-operation between government agencies when requests for assistance are made, but it is not clear if all relevant information is being shared with FIU in a consistent manner. FIU could clarify with all government agencies the type of information it should receive, when and how, and place a formal structure around such communication and dissemination.

ML Investigations and Prosecutions

There were no cases of ML/TF/FOP reported to the Police during the period 2014 to 2016. To date there have been no prosecutions under or convictions of the CI ML offence (s280A CA) and only one action commenced under PoCA to confiscate the proceeds of a predicate offence. This is in part due to the value of proceeds generated by domestic predicate offending being relatively low. Also, Police may consider the penalty for conviction of the predicate offence as being sufficient punishment, and to investigate further would not be an efficient use of resources. It is noted also that reparation orders to compensate victims can be sought at sentencing for the predicate offence which may make proceedings under PoCA somewhat redundant from a law enforcement perspective.

Until charges are laid under s280A CA and further applications made to seize assets under PoCA, it is not possible to tell the impact of those laws in deterring and disrupting ML/TF/FOP.

Summary

There is no simple or numerical measure for the effectiveness of an AML/CFT regime. Effectiveness is best measured by the cumulative effect of many measures implemented to detect, deter, disrupt ML/TF/FOP activity and reduce the channels, methods and opportunities criminals can exploit. Increased STRs, data mining, FIU, Customs and Police investigations and rejections of business by service providers, may lead to a better awareness and understanding of ML/TF/FOP and more robust compliance systems to detect, deter and disrupt ML/TF/FOP activity.

CI AML/CFT regime must be continually monitored and regularly reviewed to ensure it is adequate and appropriate for the ML threats faced by CI at any given time. In that regard it is suggested:

- CI may consider establishing a clear and definitive AML/CFT strategy lead by a smaller more focussed NACC;
- Training, dissemination of information and communication amongst government agencies and the private sector is essential to increase awareness and understanding of ML/TF/FOP;
- Given the enactment of FTRA 2017, FIU compliance audits can be carefully planned and structured for maximum effect;
- Section 47 FTRA 2017 should result in more STRs being filed providing a better tool and greater intelligence for FIU to assess the ML/TF/FOP threats to which CI is exposed;

- FIU should clarify with all government agencies the type of financial information it should receive for its further investigation and place a formal structure around such communication and dissemination;
- Restrictions on FIU, through lack of staff, to proactively mine financial transaction data may mean valuable information is missed. Perhaps this role could be delegated or contacted out to ensure the best possible opportunity is given to detecting ML/TF/FOP activity;
- Reporting institutions' obligation to risk assess clients and obtain CDD accordingly, needs to be closely monitored to ensure appropriate CDD is being obtained.

---

1. *FATF's assessment of effectiveness considers 11 Immediate Outcomes"*
2. *AML/CFT Analyses: How Does the Cook Islands AM/LCFT System Work? by John Chevis, April 2017*
3. *Section 21(1) FIUA, as amended by FIU Amendment*

ANNEX 1: World Bank GDP Rankings 2015

World Bank Ranking 2015	Country	GDP (USD millions)
1	USA	18,036,648
5	United Kingdom	2,861,091
13	Australia	1,339,141
19	Switzerland	646,002
33	Hong Kong	309,235
37	Singapore	292,739
53	New Zealand	173,754
110	Papua New Guinea	16,929
137	The Bahamas	8,854
143	Isle of Man	7,428
156	Fiji	4,426
185	St Kitts and Nevis	876
186	Samoa	761
187	Vanuatu	742
192	Tonga	435

Source: World Development Indicators Database, World Bank 28 April 2017.

http://data.worldbank.org/data-catalog/GDP-ranking-table

ANNEX 2: Roles of Government Agencies

FIU – is responsible for the administration and enforcement of AML/CFT laws. It receives, requests and analyses financial intelligence and provides the same to Police for further investigation in relation to any financial misconduct. Supervision of AML/CFT compliance by reporting institutions is a function and duty of the FIU.

Police - is the lead law enforcement agency for the investigation and prosecution of all criminal conduct in CI including ML/TF/FOP offences (and relevant predicate offences). The Criminal Investigation Branch of the Police is the specialised group with responsibility for the investigation of all serious crimes, including drug related and financial crimes, ML/TF/FOP and proceeds of crime investigations.

CLO – assists Police in the prosecution of ML/TF/FOP offences (and relevant predicate offences) and submits applications for orders under PoCA. CLO provides advice to all law enforcement agencies on prosecutions. It represents law enforcement agencies in Court and is responsible for administering mutual legal assistance requests and proceeds of crime matters. CLO is also responsible for the review and management of legislation for Parliament and Executive Council (Primary and subsidiary legislation).

RMD - is a division of the Ministry of Finance and Economic Management (MFEM) and is responsible for the administration and enforcement of taxation and customs laws.

Customs - is within in the RMD, being a division of MFEM, and was established by section 7 of CRBPA. Customs is responsible for ensuring border security. It has powers to question individuals and obtain information, search for prohibited goods, investigate and prosecute (through RMD) illegal activity, which primarily involves prohibited goods including drugs, firearms, cash in excess of thresholds and goods smuggled to avoid duties and levies.

FSC - is responsible for the prudential regulation and supervision of the financial sector (i.e. banks, insurance companies, TCSPs and money changers and remittance businesses). The FSC is also the administrator of the registry for international companies, trusts, foundations and partnerships. The FIU sits within the FSC but acts as an independent operational unit.

MFAI - is responsible for CI diplomatic relations with other States and international organisations, such as the UN. Immigration, a separate division within the MFAI, is responsible for border protection (entry and exit of persons from CI) and coordinates its efforts with Customs, FIU and Police.

MOJ - is responsible for the justice sector, including the administration of the CI Court system. In addition, MOJ is the administrator of the domestic registry of all legal entities owned and/or operated domestically including the companies and incorporated societies registers.

BTIB - is responsible for the regulation of foreign investment (and investors) into CI.

MMR - is responsible for the administration and regulation of marine resources within CI. MMR is the licensing agency for foreign fishing vessels and the law enforcement agency for illegal fishing activity. MMR co-ordinates with Police, Customs and regional counterparts in performing this function.

Audit - is responsible for the oversight of public expenditure by Crown agencies in accordance with CI government financial policies and procedures. Audit has an investigative function in relation to possible misappropriation of public resources.

ANNEX 3: High Risk Jurisdictions

Andorra
Anguilla
Antigua and Barbuda
Aruba
Austria
Bahamas
Bahrain
Belize
Bermuda
British Virgin Islands
Cayman Islands
Cyprus
Czech Republic
Delaware, USA
Dominica
Dubai
Estonia
Gibraltar
Grenada
Guernsey
Isle of Man
Jersey
Latvia
Liechtenstein
Luxembourg
Macau
Malaysia (Labuan)
Malta
Marshall Islands
Mauritius
Monaco
Netherlands Antilles
Panama
St Kitts & Nevis
St Lucia
St Vincent & the Grenadines
Seychelles
Singapore
Switzerland
Turks & Caicos Islands
United Arab Emirates
Vanuatu

GLOSSARY

Crown agencies/ministries/departments/committees

ACC- Cook Islands Anti-Corruption Committee
Audit - The Cook Islands Expenditure and Review Committee and Audit Office
BTIB – Business Trade Investment Board
CINIT - Cook Islands National Intelligence Taskforce
CLAG - Cook Islands Combined Law Agency Group
CLO – Crown Law Office
Collector - Collector of Inland Revenue, also means the Treasurer of the Revenue Management Division (RMD) of the Ministry of Finance and Economic Management
Customs – Cook Islands Customs Service
FIU – Cook Islands Financial Intelligence Unit
FSC – Cook Islands Financial Supervisory Commission
Immigration – a division within Ministry of Foreign Affairs and Immigration
MFAI – Ministry of Foreign Affairs and Immigration
MFEM – Ministry of Finance and Economic Management
MMR – Ministry of Marine Resources
MOJ – Ministry of Justice
MOT – Ministry of Transport
NACC - National AML/CFT Coordinating Committee
Police – Cook Islands Police Service
RMD – Revenue Management Division of the Ministry of Finance and Economic Management

Legislation

BA - Banking Act 2011
CA – Crimes Act 1969
CDA - Currency Declaration Act 2016
CRBPA – Customs and Revenue Border Protection Act 2012
CTPWMDA – Counter Terrorism and the Proliferation of Weapons of Mass Destruction Act 2017
EA – Extradition Act 2003
FIUA – Financial Intelligence Unit Act 2015
FIU Amendment – Financial Intelligence Unit Amendment Act 2017
FSCA – Financial Supervisory Commission Act 2003
FTRA 2004 – Financial Transactions Reporting Act 2004
FTRA 2017 – Financial Transactions Reporting Act 2017
IA – Insurance Act 2008
ICA - International Companies Act 1981-82
ITA - International Trusts Act 1984
ITAXA – Income Tax Act 1997
MACMA – Mutual Assistance in Criminal Matters Act 2003
MACMA Amendment – Mutual Assistance in Criminal Matters Amendment Act 2017
MRA – Marine Resources Act 2005
PA – Police Act 2012
PoCA – Proceeds of Crime Act 2003
PoCA Amendment – Proceeds of Crime Amendment Act 2017
SRA – Ship Registration Act 2008
TCA – Trustee Companies Act 2014
The Regulations – Financial Transactions Reporting Act 2017 Regulations
TSA – Terrorist Suppression Act 2004
TSA Amendment – Terrorism Suppression Amendment Act 2017

General

2015 Typologies Report - Cook Islands Typologies Report 2015: Trends, Typologies and Case Studies, issued 23 June 2016
APG – Asia/Pacific Group on Money Laundering
AML/CFT – Anti Money Laundering/Combatting the Financing of Terrorism
CDD – Customer Due Diligence
CI – The Cook Islands
CRS – Common Reporting Standard
DNPBs - designated non-financial bodies and professions

Egmont Group - a global body of financial intelligence units providing a platform for the secure exchange of expertise and financial intelligence to combat ML/TF/FOP www.egmontgroup.org
ESW – Egmont Secure Website
FATCA – Foreign Account Tax Compliance Act
FATF – Financial Action Task Force
FinCEN - Financial Crimes Enforcement Network
GDP – Gross Domestic Product
Global Forum - Global Forum on Transparency and Exchange of Information for Tax Purposes
HNWIs – High Net Worth Individuals
IRS – United States Inland Revenue Service
LLC – Limited Liability Company
MCI – Maritime Cook Islands Limited
ML – Money laundering
ML/TF/FOP – Money Laundering/Terrorist Financing/Financing of Proliferation
MVD - Motor Vehicle Dealer
NPO – Non-profit organisation
NRA 2008 - Money Laundering Risk Analysis for the Cook Islands published in 2008
NRA2015 - National Risk Assessment 2015: Money Laundering and Financing of Terrorism in the Cook Islands
NRA 2017 – Cook Islands National Risk Assessment scheduled for completion by 31 October 2017
NZ$ - New Zealand Dollars
OECD – Organisation for Economic and Cultural Development
PEP – Politically exposed person
SEC – United States Securities Commission
TCSP – Trust and Company Service Provider
TIEA – Tax Information Exchange Agreement
UN – United Nations
UNODC – United Nations Office on Drugs and Crime
US$ - United States Dollars

Acknowledgements:

The businesses and organisations within the Cook Islands that willingly participated in discussions and answered questionnaires on their activities and current AML/CFT compliance programmes, procedures and processes.

Key government agencies and other government departments who contributed by providing information, statistics and access to staff.

FIU for co-ordinating with other government agencies and department to collect and collate information requested for this Report.

FSC for its support in providing information and resources.

John Chevis, UNODC Adviser (Anti-Money Laundering and Counter Financing of Terrorism) for the Pacific.

Michelle Harwood, Executive Officer, APG.

**Alan Taylor was engaged by the Financial Supervisory Commission to prepare the "Cook Islands Money Laundering and Terrorist Financing – Primary Threats and High Risk Sectors" report. Alan is a New Zealand qualified lawyer with 23 years' experience in the international financial services industry, 10 of those spent working in the Cook Islands. Alan has held legal, business development and senior management positions in both public and private organisations. He is currently working for the Cook Islands Financial Services Development Authority.*

COOK ISLANDS MONEY LAUNDERING AND TERRORIST FINANCING:

Secondary Threats and Low Risk Sectors

Phil Hunkin

October 2017

COOK ISLANDS MONEY LAUNDERING AND TERRORIST FINANCING: Secondary Threats and Low Risk Sectors

Contents Page

1.0 Executive Summary	64
2.0 Introduction	64
2.1 Secondary Threats and low risk sectors	64
2.2 AML/CFT Strategic plan	65
3.0 Risk Assessments sector by sector	66
3.1 Overview	66
3.2 Accountants	66
3.3 Lawyers	66
3.4 Pearl Dealers	67
3.5 Motor Vehicle Dealers	67
3.6 Real Estate	67
3.7 Lotto	68
3.8 Non Profit Organisations	68
3.9 Aid development funding	68
3.10 Graphical findings of Risk assessment	69
3.11 Analysis of Reports received by the FIU	69
4.0 Conclusions	70
5.0 Recommendations	71

1.0 Executive Summary

1.1 All Cooks Islands authorities contributed to and developed a National Risk Assessment around Money Laundering and Terrorism Financing over a period from 2014 to 2015. The National Risk Assessment was published in 2015 (NRA 2015).

1.2 The NRA 2015 has been utilised by Government agencies to enhance the AML / CFT regime within the Cook Islands. This regime incorporates Laws, Regulations, Enforcement and other measures mitigate the ML/TF risks identified. The NRA has allowed Government to determine prioritisation and an efficient allocation of resources.

1.3 The NRA has also enabled financial institutions and Designated Non-Financial Businesses and Professions (DNFPB's) to support the conduct of their own risk assessments. This is assisting the development of a holistic risk based approach to AML/CFT in the Cook Islands.

1.4 In 2017 the Cook Islands authorities led by the Financial Supervisory Commission (FSC) and the Financial Intelligence Unit (FIU) undertook a sectors based risk assessment exercise. This activity was designed to build upon the NRA 2015 and to have a focussed assessment of the risk presented. This report is focussed on the Secondary Threats and Low Risk Sectors and complements the Primary Threats and High Risk Sector Report.

1.5 The eight sectors identified for the purpose of the review have all be subject to either a desk based review or have been subject to Compliance assessments by the FIU. The activity supports the AML/CFT Compliance Strategic Plan 2017 – 2019 that was published in December 2016 and was developed and informed by NRA 2015. The outcomes of the risk assessment indicate an increase of risk. This is as a direct result of new legislation introduced in 2017. In particular the Financial Transactions Report Act, 2017 (FTRA 2017) that requires reporting institutions to manage risks including the development of risk policies.

1.6 The sectors are generally required to develop their knowledge and risk based processes to better mitigate the risks presented. This outcome of this risk assessment will be fed back into the work processes of the Compliance Team FIU to improve risk mitigation of the sector with the aim of lowering the overall risk.

2.0 Introduction

2.1 Secondary threats and low risk sectors

The Cooks Islands undertook and published a National Risk Assessment in 2015. The assessment focussed around the threats, vulnerabilities and risks presented through money laundering, Terrorism financing. As a consequence of the National Risk Assessment a number of measures have been deployed by the Cook Islands authorities to mitigate these risks.

To assess the benefits of these measures a Primary Threats and High Risk Sectors report was commissioned by the Financial Supervisory Commission to undertake a risk assessment of these high risk sectors and to report the findings to the AML/CFT authorities. The report was concluded in July 2017.

A further report has been commissioned through the FIU to undertake a similar assessment of sectors not incorporated as part of Primary Threats and High Risk Sectors review. The review has been termed the **Secondary Threats and Low Risk sectors**. The sectors that will provide the focus of this review are:

- Accountants
- Lawyers
- Pearl Dealers
- Motor Vehicle Dealers
- Real Estate
- Lotto
- NPO's
- Aid development funding.

2.2 AML/CFT Compliance Strategic Plan 2017 - 2019

The development of domestic legislation has seen the Financial Transactions Reporting Act 2004 being replaced by the Financial Transactions Reporting Act 2017. The impact and transition between statutes has been carefully planned and implemented by the CIFIU and other authorities. The new legislation provides a much higher focus to a risk based approach. This new approach identified a further requirement to conduct a risk assessment of the low risk sectors.

In November 2016 the Head of CIFIU published an AML/CFT Compliance Strategic Plan 2017 - 2019 for the Cook Islands. The CIFIU is the primary AML/CFT Supervisor in collaboration with the Financial Supervisory Commission (FSC) on a delegated AML/CFT Supervisory role, and the country's Prudential Regulator. The plan was adopted by the FSC Board to continue the improvements to the AML/CFT regime that the Cook Islands have introduced over recent years and also to continue to mitigate the outcomes of the 2015 NRA.

The plan seeks to "To contribute to the national, regional and global fight against money laundering, the financing of terrorism and proliferation financing, and other serious crimes through a robust and effective AML/CFT Compliance Regime".

The following mission statement underpins the plan. *Endeavour to protect the Cook Islands from any risks of money laundering, terrorist financing, proliferation financing or other serious crime activities, and thus contribute to a safe and a stable financial sector for the people of the Cook Islands and foreign investors.*

The mission is embraced by undertaking a robust offsite and onsite compliance examinations, information collection, analysis, monitoring and where necessary the dissemination of information on suspected money laundering, the financing of terrorism or proliferation financing activities and other serious crimes to the relevant domestic, and international law enforcement authorities.

The plan is predicated against seven strategic goals:

- Goal 1 – To promote full compliance with the requirements of the FTRA 2017.
- Goal 2 – To review and enhance THE AML/CFT Compliance framework of a new

and existing reporting institution to comply with the FTRA 2017.

- Goal 3 – Implement an effective and robust AML/CFT Compliance framework.
- Goal 4 – Undertake an effective risk-based AML/CFT compliance examination.
- Goal 5 – Monitor the implementation of the AML/CFT Compliance framework.
- Goal 6 – Promote effective relationships with reporting institutions.
- Goal 7 – Promote capacity and professional development for AML/CFT Supervisors.

3.0 Risk assessments sector by sector

3.1 The sectors below have been subject to on-going assessment by the Compliance Team of the Financial Intelligence Unit over a period of years. These on-going assessments and other activity has provided the information required to analyse the risk presented by each sector. The outcomes of this analysis is outlined below and the assessed risk rating. The risk rating was achieved through the assessment of two elements of risk the vulnerability and the threat/Likelihood of ML and TF. The highest level is rated as one and the lowest level rated as a five. These two figures are added together to provide a level of overall risk. The outcomes of this exercise are articulated in the table at 3.10 below.

3.2 Accountants

In NRA 2015 it was identified that the majority of Accountants within the Cook Islands fell outside of the FTRA. There is one exception KPMG. The NRA 2015 considered the risk presented by the Accountancy sector as low.

Accountancy business has been subject to onsite reviews in 2013 and 14. Additionally five accountancy businesses were subject to a desk based review by the Compliance team of the FIU in March and April 2017. Analysis of this review identified that there was an absence of risk based policies and a low level of understanding of their obligations under the FTRA. This presents a vulnerability of ML and TF. The threat or likelihood was considered to be low due to the nature of the business undertaken by the sector. This sector do not provide or operate Trustee services. The accountancy sector had submitted one SAR in the period 2015 to date. The risk presented by the Accountancy sector is **LOW / MEDIUM**.

3.3 Lawyers

The Cook Islands has eight legal firms and they are relatively small organisations the largest has three lawyers and some are sole practices. In NRA 2015 the risk presented by Lawyers was presented as low. However most Law firms did not meet the definition of Reporting Institutions for the purposes of the FTRA 2004. The introduction of the new FTRA 2017 legislation has now established the sector as reporting entities. In the period February – May 2017 the FIU surveyed five lawyer firms and were subject to both an onsite and a desk based review. The Legal sector had submitted two SAR's in the period 2015 to date. On the basis of their responses, together with other information available both closed and open source. The absence of risk identification and risk management documented processes, together with business in other high risk areas and concerns from other authorities led to the conclusion that the risk presented by the Lawyers sector is **MEDIUM / HIGH**.

3.4 Pearl Dealers

The Cook Islands Pearl Authority [CIPA] was established in 1994 and provides direction and regulation of the pearl industry in the Cook Islands. CIPA supports the industry by marketing Cook Islands Pearls to the rest of the world and by providing a Pearl Exchange through which the trade can buy and sell the highest quality of authentic Cook Islands Pearls.

There are 25 Pearl dealers identified within the Cook Islands. In March and April 2017 a desk based review was conducted by the FIU. Pearl dealers are regulated by the FTRA 2017. In the NRA 2015 the findings of the assessment were that Pearl Dealers presented a low risk in relation to money laundering and terrorist financing.

The findings of the desk based review identified that Pearl Dealers generally did not have risk policies that enabled to fully identify risks presented. This creates a vulnerability that is some way mitigated by the relatively low transaction values across the industry. The threat and likelihood of the sector engaging with money launderers or terrorist financing was considered as medium / low. Pearls were added to the definition of cash by virtue of the Currency Declaration Act 2015/16 (CDA). This has meant that Pearls on import or export from the Cook Islands are subject for the first time to the declaration requirements of the CDA. This new requirement further mitigates the threat level. The Pearl sector have not submitted any SAR's. The risk presented by the Pearl Dealers is **LOW / MEDIUM**.

3.5 Motor vehicle dealers

The FIU has identified six motor vehicle dealers that are Reporting Institutions for the purpose of the FTRA 2017. In the NRA 2015 the findings of the assessment were that Motor Vehicle Dealers (MVDs) presented a low risk in relation to money laundering and terrorist financing.

Motor vehicles are imported into CI by the 6 licensed MVDs. They are sold to CI resident customers. FIU received CTRs from 2 MVDs in the period 2014 to 2016. The MVD noted that it had 123 sales with value greater than NZ$10,000 in 2016, but only 3 were paid for in cash. The remainder were paid for on hire purchase terms over a lengthy period through electronic payments or cheque.

Onsite reviews of Motor Vehicle Dealers have been undertaken in 2013, 2014 and 2017. In March / April 2017 a further desk based review of four motor vehicle dealers was undertaken by the FIU. The analysis of the desk based review identified that motor vehicle dealers had a low level of recognition of risk presented through ML and TF, an absence of written risk based policies and procedures identified a medium vulnerability risk. The threat and likelihood of ML or TF was assessed as medium / low this was mitigated through the positive response of the sector to the desk based review and subsequent activity in response to the threat identified. The risk presented by the motor vehicle dealers is **LOW / MEDIUM**

3.6 Real estate

In the NRA 2015 the findings of the assessment were that Real Estate Dealers presented a low risk in relation to money laundering and terrorist financing. There are still four Real Estate dealers in the Cook Islands. Onsite reviews of the sector were undertaken in 2011 and 2013. Two of these businesses were subject to a desk based review in March and May this year, the conclusions identified that there

was a low level of vulnerability and the threat and likelihood was considered a medium risk. There was an absence of risk awareness and no policies to manage risk were in place. There were no SAR's submitted by the Real Estate sector in the period 2015 to date. The risk presented by the Real Estate Agents is **LOW / MEDIUM**

3.7 Lotto

Cook Islands Tattslotto is the only lottery agency based in the Cook Islands. The games played are the Ozlotto, Powerball and Tattslotto of Australia. Part of the money from tickets sold goes towards sport in the Cook Islands. The Lotto is a reporting institution for the purposes of the FTRA 2017. A desk based review of the Lotto identified a low level of risk. There were no SAR's submitted by the Lotto in the period 2015 to date. The risk presented by the Lotto is **LOW.**

3.8 Non Profit Organisation's

Non-profit organisations (NPO'S) in the Cook Islands are required to register with the Ministry of Justice as at March this year there were 194 NPO's registered. A desk based risk review was conducted of the NPO sector in September 2017. Through a selection process based on monetary size of each organisation twenty – five NPO's were required to complete a comprehensive questionnaire. The analysis of the 17 responses identified that generally the sector have a low knowledge of their obligations with respect to AML/CFT. None of the respondents had risk policies in place. This is balanced by the fact that they are mainly small organisations and run mainly for domestic causes.

There are four NPO's that have been identified that have been in receipt of foreign aid these have been identified as Cook Islands Football Association, Red Cross, Cook Islands Women's Association and Te Ipukanea Society. The international element of these charities increase their vulnerability to ML and TF and as such we have treated these differently and they have been subject to onsite visits. (To incorporate outcome when completed.)

NRA 2015 identified that awareness training had been delivered to the NPO sector in 2012 in respect of the FTRA 2004 and Currency declaration obligations. The findings of NRA 2015 was that the level of threat and vulnerability was considered to be low. The risk presented by the NPO sector is **MEDIUM.**

3.9 Aid development funding.

Cook Islands Development Coordination Division (Division) of the Ministry of Finance and Economic Management.

The Division is directed by the Cook Islands Development Partner Policy and reports to the National Sustainable Development Commission (NSDC).

The policy states that the achievement of the Cook Islands development outcomes will be supported by the effective and efficient use of Official Development Assistance, aligned to the National Sustainable Development Plan (NSDP).

The Division fosters relationships with a broad range of development partners to broker coordinated arrangements. These activities are increasingly delivered through diverse partnerships at a variety of levels including local government, civil society, private sector and national government agencies.

The Division seeks to provide high quality development advice to partners including Ministers, government agencies, committees, community groups, private interest groups and donors.

The Division hosts the country liaison office of the Asian Development Bank and contributes to the development of concessional loans and blended financing arrangements with other partners like European Investment Bank and Development Partners like the People's Republic of China.

Estimated Official Development Assistance over the coming three years along with past spends are reported in the national budget document annually. The Division produces annual financial statements which aim to produce a complete picture of Official Development Assistance provided to the Cook Islands and its allocation by sector and activity.

The Division met with officials of the FIU and provided the FIU with information on how they managed the ML and CFT risks. All of the business that they conduct is done at a Government to Government level. They will always know which country and where any aid is coming from. They consider the risk to be negligible.

The Division were asked how they deal with any political interference. This is managed effectively through the financial guidelines for all ministries. The document is titled Financial Policies and Procedures Cook Islands Government. Each project is subject to a project plan and these will be followed precisely. Scrutiny is provided at a high senior level and is subject to a four eyes approach. They do not have a specific compliance programme.

This area is not subject to the FTRA 2017 and no SAR's have been received from this sector. The risk presented through the aid sector is considered to be **LOW**.

3.10 Graphical findings of the Risk assessments undertaken by the FSC / FIU.

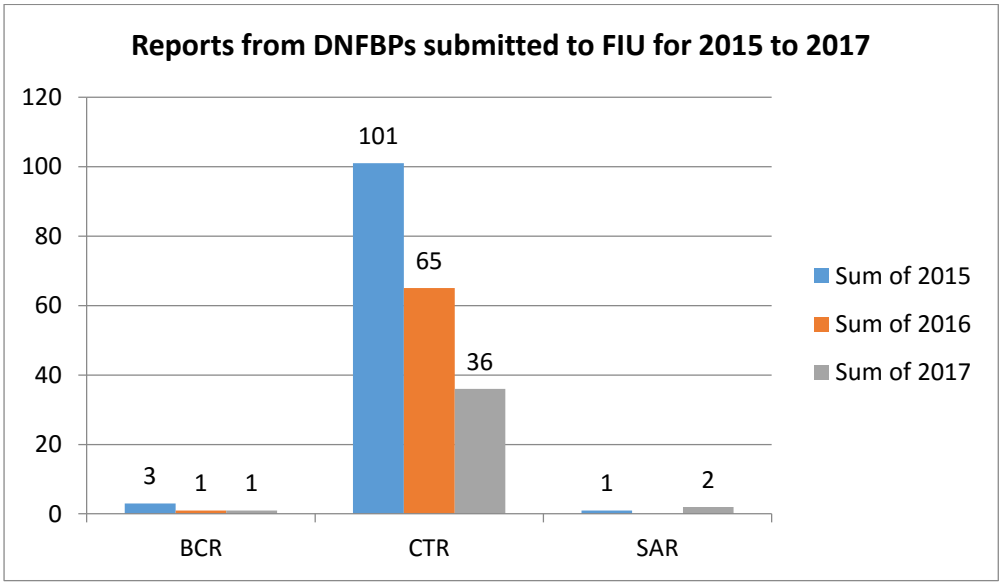
FTRA 2017 Entities	No. Surveyed	Sector	Vulnerability	Threat / Likelihood	Score/ average	Risk
1	5	**Accountants**	4	4	8 / 4	Low /Medium
5	5	**Lawyers**	2	2	4 / 2	Med/High
4	2	**Real Estate**	4	3	7 / 3.5	Low /Medium
6	4	**Motor Vehicle Dealers**	3	4	7 / 3.5	Low /Medium
25	16	**Pearl Dealers**	4	4	8 / 4	Low /Medium
131	17	**NPOs**	3	3	6 / 3	Medium
X	1	**Aid / Development**	5	5	10/5	Low
4	0	**High NPOs**				See NPO's
1	1	**Lotto**	4	5	9 / 4	Low

3.11 Analysis of Reports received by the FIU

Table showing Reports from DNFBPs submitted to FIU for 2015 to 2017

Reports	2015	2016	2017
Suspicious Activity Reports (SAR)	1		2
Cash Transaction Reports (CTR)	101	65	36
Border Currency Reports (BCR)	3	1	1

Graph showing trends of reports from DNFBPs submitted to FIU for 2015 to 2017



The suspicious activities of 3 reports were from a law firm and an accounting firm of subjects committing an offence of a crime.

The cash transaction reports were from motor vehicle dealers who have purchased high value products with cash.

The border currency reports which are reported by Customs were from pearl dealers who were bringing in or taking out business funds for business purposes.

4.0 Conclusions

4.1 The risk assessment has resulted in a positive benefit for the Cook Islands DNFPB's previously categorised as low risk. The benefits include increased knowledge and awareness of the AML/CFT regime, an awareness of their legal obligations under the new FTRA legislation and a better understanding of the risks presented of ML and TF. They are also aware of the requirements to have risk mitigating procedures in place through written policy. It has also enabled FSC and FIU to better

understand the vulnerabilities and threats for this sector. The FSC / FIU have been able to gain knowledge from their activities and as a consequence will be able to better inform a risk based approach in relation to planning in the future.

4.2 All sectors engaged for this risk assessment were cooperative and where there were gaps identified in their knowledge and understanding of AML / CFT, the FIU were provided with confidence that these sectors take their obligations seriously and that remedial steps would be undertaken to ensure that they improved around any shortcomings identified. The FIU were grateful for the cooperation and commitment demonstrated.

4.3 The Lawyers and NPO sector were identified as medium / high and medium respectively and as such they will be required to introduce good practices to reduce the risk presented.

4.4 All other sectors were already working to reduce their risk to Low.

5.0 Recommendations

5.1 That the Lawyers and NPO's remain in focus as part of the Compliance Strategic plan 2017 -2019. With a focus on reducing the risk presented in respect of Ml and CFT.