COOK ISLANDS TYPOLOGIES REPORT 2015

Trends, Typologies and Case Studies

Issued - 23 June 2016

This Report contains useful information on the trends and typologies extracted from reports submitted and received by the Cook Islands Financial Intelligence Unit, and including case studies investigated by the FIU with its local and international partner agencies.

Table of Contents

1. Foreword

I am very pleased to present the first **Typologies Report and case studies** by the Cook Islands Financial Intelligence Unit (CIFIU) for 2015. These reports are valuable information for the key sectors here in the Cook Islands and CIFIU's partner agencies. They reveal the diversity and seriousness of the money laundering threats facing the industry and the wider community.

The reports and the case studies provided in this report present a snapshot of how criminals are seeking to misuse the Cook Island's financial system or to exploit key products and services as a vehicle to facilitate or to further disguise the nature of their criminal activity. The cases range from international individuals or possible syndicates across a number of countries who are involved in fraud schemes to generate proceeds to purchase assets to a less sophisticated domestic fraud in the Cook Islands. The case studies are consistent with the findings of the Cook Islands National Risk Assessment 2015.

This report further examines CIFIU's involvement in two multi-agency task force operations namely Operation Shadow and Operation Snap. It demonstrates how CIFIU's financial intelligence is vital to their success and details of the criminal typologies and suspicious customer behaviours that should trigger 'red flags' for Cook Islands businesses.

The CIFIU could not produce such detailed and informative resources without the valuable input of its partner agencies and the cooperation of its international counterparts.

The case studies in this report demonstrate the value of the financial intelligence generated from the transaction reports and reports of suspicious matters the FIU receives from a range of reporting institutions. I acknowledge the important role played by the industry as partners in combating serious crimes, including money laundering and countering the financing of terrorism.

I look forward to consulting with industry and partner agencies about future reports in this series. This input is crucial in ensuring our reports remain useful and relevant to our collective efforts to protect the Cook Islands against financial and other serious crimes.

Bob Williams
Head of FIU

2. Introduction

The CIFIU is the Cook Islands Anti-Money Laundering and Counter Terrorism Financing (AML/CFT) Regulator and Financial Intelligence Unit (FIU).

CIFIU's purpose is to protect the integrity of the Cook Islands financial system and contribute to the administration of justice through its expertise in countering money laundering and the financing of terrorism.

CIFIU's role

As the Cook Islands AML/CTF regulator, the CIFIU oversees the industry's compliance with the requirements of the ***Financial Transactions Reporting Act 2004*** (FTRA). Where the CIFIU detects cases of non-compliance with the FTRA, it may take appropriate enforcement action to secure compliance by the reporting institution.

A reporting institution includes banks. Trustee companies, money remittance and other financial services providers, and designated non-financial businesses and professions such as motor vehicle dealers, pearl dealers, real estate agents, lawyers, accountants and entities created under the Incorporated Societies Act 1994.

The FIU analyses the financial transaction reports submitted by reporting institutions and disseminates financial intelligence to its partner agencies to assist them in their investigations. The ***Financial Intelligence Unit Act 2015*** (FIU Act) empowers the FIU to investigate 'financial misconducts' as defined under section 4, which includes:

- a breach of any of the Oversight Acts (FTRA, Proceed of Crimes Act 2003 and the Mutual Assistance in Criminal Matters Act 2003.
- misconduct by any person relating to money laundering;
- fraud involving cross-border financial transactions;
- the financing of terrorism;
- the financing of proliferation financing of weapons of mass destruction;
- the financing or facilitating of bribery and other corrupt practices of any sort;
- tax evasion (whether or not relating to taxes payable in the Cook Islands).

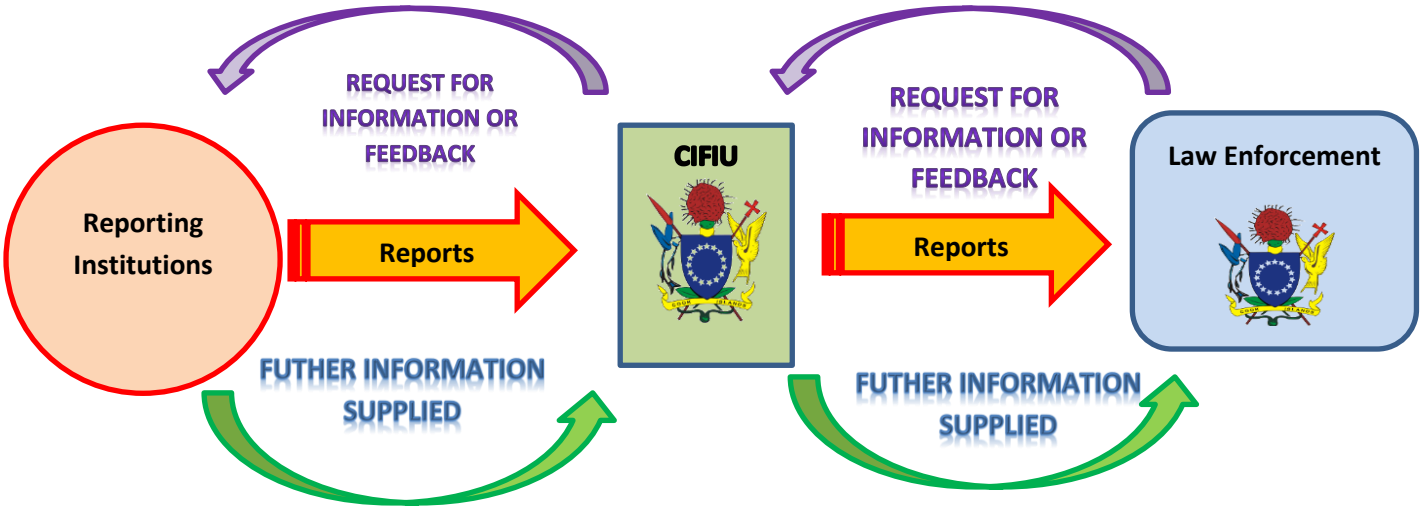
Working with partner agencies to combat money laundering and terrorism financing

CIFIU's partner agencies include domestic law enforcement agencies, border security agencies and revenue. The CIFIU also works closely with its international counterparts to contribute to global AML/CTF efforts. The CIFIU assisted in a number of cross-agency task force investigations in 2015 as provided in the case studies.

Working with industry

In 2015 the CIFIU received thousands of financial transaction reports and reports of suspicious matters from its reporting institutions, and including cross-border currency reports from its counterpart agency. The FIU analyses this transaction data to identify any potential money laundering, terrorism financing and other serious crimes. The FIU then shares that information with its domestic partner agencies and international counterparts for use in their criminal investigations and other operations. Financial transaction data assists law enforcement authorities to identify relationships between individuals and networks, the movement of funds and patterns of financial activity.

Figure1: below, illustrates how reporting by institutions provides key financial intelligence to support law enforcement investigations and how the FIU provides the information to its partner agencies on criminal trends and methods.



This report contains a range of trends and typologies extracted from the reports and case studies detailing investigations and operations undertaken by CIFIU's with its partner agencies. The case studies demonstrate the intelligence value of the transaction and suspicious reports submitted to CIFIU by reporting entities.

The purpose of this report is to inform the industry and the wider community about the various methods criminals use to conceal, launder or move illicit funds and to commit financial or other criminal activities. This information may assist the industry to strengthen its measures to detect money laundering activity and protect both businesses and customers from a criminal activity.

Reporting institutions should use this report to:

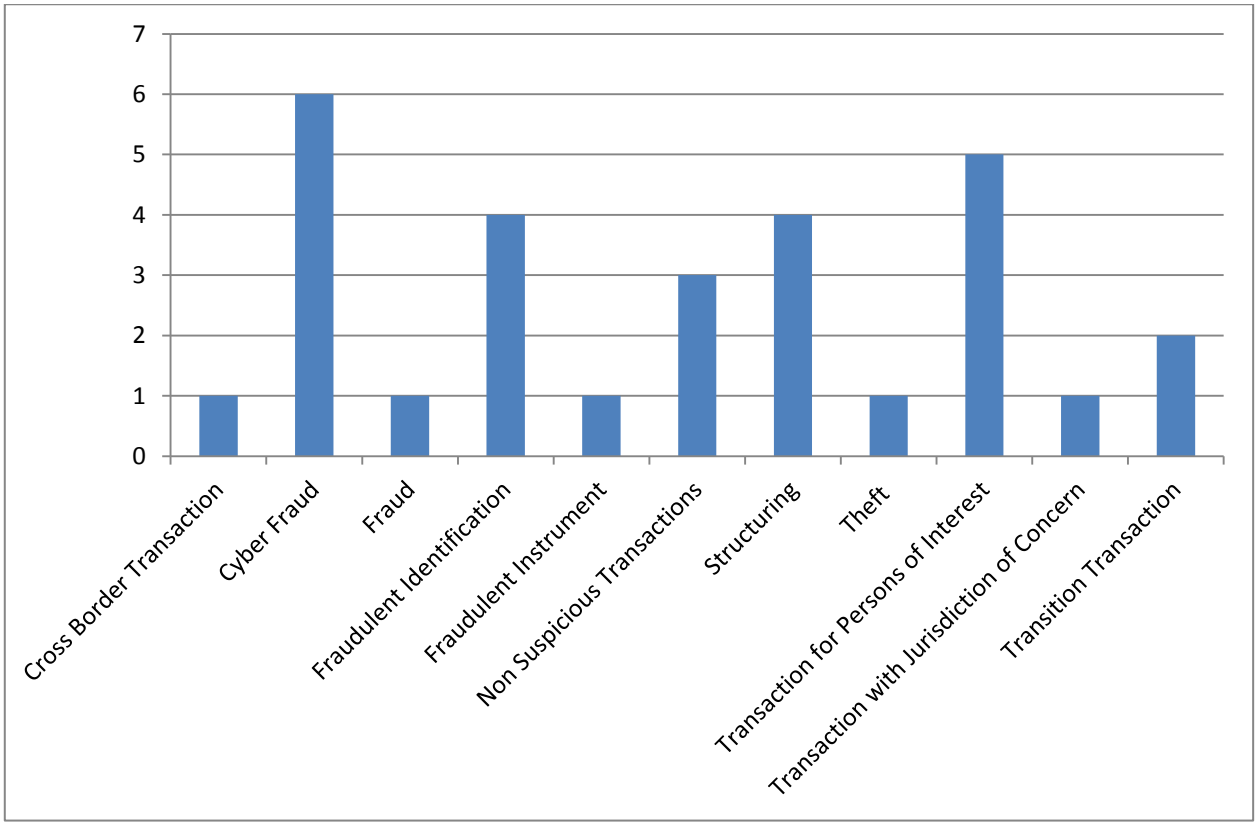
- determine what ML/TF vulnerabilities are most relevant to their entities;
- use the information to update their AML/CTF guidance material and training ; assist with staff training programs, or to raise awareness of ML/TF issues within the entity;
- use it in any ML/TF risk assessments;
- assist them in identifying and investigating unusual customer activity. Entities

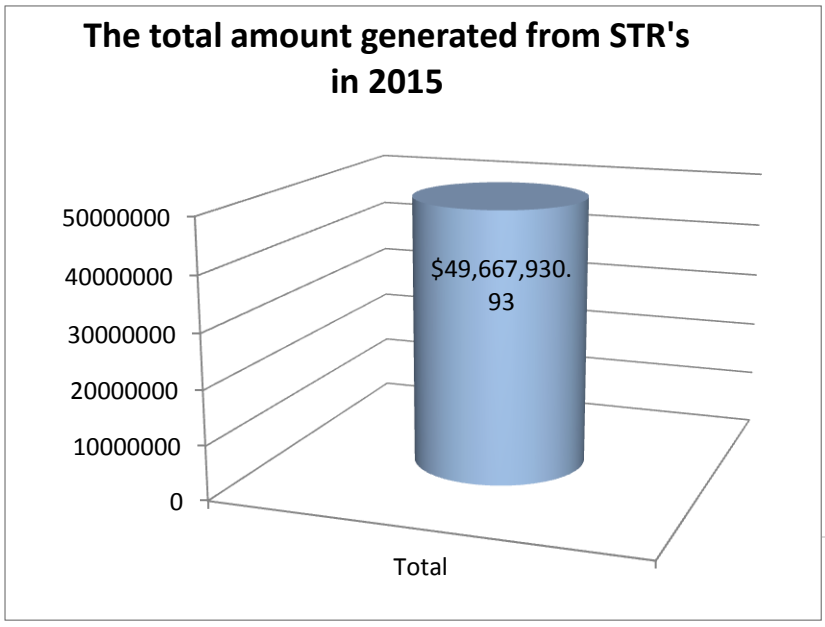
should use the risk 'indicators' in this report as a guide when describing unusual behaviour in a suspicious transaction or activity reports;

- add new and refine the existing detection scenarios and methods they use in their transaction monitoring programs;
- highlight the benefits of maintaining a robust AML/CTF regime within their institution.

3. Trends and Typologies

The following graph provides indicators or trends of the predicate crime types reported the CIFIU in 2015.





This graph provides the total value of all suspicious transactions reported to the FIU.

The following typologies are extracted from the reports made to the FIU in 2015:

Structured Transactions

On 6 January 2015, a foreign national made multiple structured outward transfers by internet banking. The individual was on contract with the government and the purpose for structuring the transfers was due to the internet banking approved maximum limit for a single transfer of $5,000.

On 15 January 2015, a foreign national who have been operating an account with a negative balance for a period of nine months received a reasonable amount of deposit which was then subsequently transferred offshore in several transactions just above the $10,000 threshold to his wife as operating expenses.

On 30 June 2015, a customer received two separate electronic funds transfers on the same day for the sum of NZ$10,000.00 each.

On 12 October 2015, a large deposit was made into a dormant account followed by three separate subsequent transfers offshore under the threshold amount of $10,000. Information obtained revealed that the funds were from the sale of a property here on Rarotonga and the couples are both foreign nationals.

Transaction with Jurisdiction of Concern

On 3 February 2015, an inward transfer of a significant amount of money was rejected from a foreign national involved in an IT software development business operating in a jurisdiction of concern.

Transaction for Persons of Interest

On 4 February 2015, a request to transfer funds to a foreign national was temporarily frozen as it related to an individual who was wanted by INTERPOL.

On 17 February 2015, a foreign national who was convicted for fraud in 2010 was found performing transactions on behalf of another individual who was a subject in an investigation by the CIFIU.

On 19 February 2015, a foreign national requested for a transfer of funds to the settlor of a trust. Information's reported in the media indicated that the individual had been implicated for the failure of a bank and involvements in money laundering, weapons and drug smuggling.

On 12 August 2015, a foreign national requested for the transfer of funds to a beneficiary who was found after being screened by the bank to have been convicted for wire fraud and false accounting.

On 25 September 2015, a foreign national requested to transfer the total balance left in the account and then to close the account was found to be under investigation for tax matters.

Cyber Fraud

On 4 February 2015, a fraudulent email request purportedly sent in the name of the email account holder requesting to transfer funds to pay for a travel and hotel expenses was rejected.

On 4 March 2015, a fraudster attempted to send an email to a local bank requesting to transfer funds to a foreign country was detected and stopped.

On 19 March 2015, a fraudster sent an email purporting of having it sent by the account holder which resulted in three transfers being made. The funds were sent to an individual in one country and the remainder to a business entity in another country.

On 24 March 2015, a fraudster attempted to send an email purporting it to have been sent by the settlor and requesting to transfer funds to a business entity in a foreign country which was detected and stopped.

On 16 June 2015, a local bank reported of a foreign company purporting to be operating in the name of the bank.

On 21 July 2015, a fraudster sent an email in an attempt to request for the transfer of funds on behalf of the account holder which was detected and stopped.

Fraudulent Identification

On 17 February 2015, a foreign identification document submitted to open a bank account was found to be invalid or illegitimate. The request to open the bank account was declined.

On 24 March 2015, a foreign identification document submitted to open a bank account with a local bank was found to be fraudulent and therefore was declined.

On 30 March 2015, a foreign identification document submitted to open a bank account with a local bank was found to be fraudulent and therefore was declined.

On 12 August 2015, a foreign identification document submitted to open a bank account with a local bank was found to be fraudulent and therefore declined.

Transition Transaction

On 7 April 2015, a bank account which has been in dormant four and a half years suddenly received a large inward transfer from a Trust in country B. The individual then requested the bank to increase his internet banking limit from $1,000 to $100,000 to allow him to transfer funds into his account bank in country B.

On 7 May 2015, three large amounts of inward telegraphic transfers were received into an account for four days when it was subsequently transferred out to an import and export company in country B and to a fishing company registered in country C.

Fraudulent Instrument

On 12 May 2015, a cashier's cheque to the order of a local law firm for clean collection was found to be fraudulent after being checked and confirmed by the correspondent bank.

Theft

On 15 May 2015, a suspicion of a possible theft of client funds by the Principals of a reporting institution.

Non Suspicious Transactions

On 30 June 2015, four separate electronic funds transfer by a Theological tour group that toured Australia and New Zealand.

On 14 July 2015, a large amount of internal funds transfers between company accounts for business expenses.

On 21 August 2015, a local individual was found making a significant cash deposit of into a personal account which was being used as a trading account for a business. The same funds were later transferred to a foreign entity in country B to purchase solar panels.

Cross Border Transaction

On 15 July 2015, a foreign national made a cash deposit in a foreign currency under $10,000 but when converted into the local currency it exceeded the threshold amount of $10,000.

Fraud

On 4 November 2015, a local individual misdirected client funds for holiday forward bookings into a business account owned by him together with another individual and then subsequently transferring it into his personal account.

4. Case Studies

Case 1:

The FIU investigated the identity of Miss A, a foreign national located in country A. Miss A was listed as a director of an international company. Miss A was not identified and verified. An internet search of Miss A indicated that she was related to a Mr. B, a convicted fraudster also living in country A. The other company director Mr. C was noted to have been a long-time friend of Mr. B. Further investigation by the FIU confirmed that the company established here in the Cook Islands holds an asset and that Miss A and Mr C appeared to have been used as a front to setup the company. Mr C was also used to open a bank account at Bank A in the Cook Islands to finance the expenses of maintaining the asset which was being funded from a company established in country B. A convicted lawyer for fraud in country C was responsible for setting up of the companies and bank accounts in country B. The FIU then engaged the assistance of a law enforcement agency in country A where Mr B was suspected to have been involved in a fraudulent scheme and funds laundered to bank accounts in country C which subsequently funds the account here in the Cook Islands. The matter is still under investigation.

Case 2:

A business entity was investigated for an alleged theft of funds. The investigation uncovered that a mistake occurred when payments was made to a foreign client which was then subsequently paid back. Documents relating to the opening of a bank account in the name of a close relative of one of the director's was suspected to be a forgery which is still under investigation. However the entity has been prosecuted for other regulatory breaches.

Case 3:

A business manager misdirected funds from clients overseas for holiday accommodation forward bookings into a business account owned by him together with the accountant. The funds were directed into the business account at Bank A before it is subsequently transferred into the business manager's personal account at the same bank. The funds are then transferred to his personal account at Bank B. Part of the money was then used to purchase a vehicle. The matter is still under investigation.

Case 4:

The FIU investigated a number of prominent individuals for allegations of financial misconduct relating to public position appointment of an individual and the awarding of a

contract for projects including unauthorised advances to a private company. The matter is still under investigation.

Case 5:

An outward bound foreign national failed to declare carrying cash and negotiable bearer instruments across the border in excess of the value of NZD10,000.00. The individual was arrested and appeared before the High Court on a charge under the Customs Act where she was later discharged without conviction.