# COOK ISLANDS TYPOLOGIES REPORT 2016

*Trends, Typologies and Case Studies*

Issued - October 2017

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.

# Contents

# 1. Foreword

I am very pleased to present the second annual **Typologies Report and case studies** by the Cook Islands Financial Intelligence Unit (CIFIU). 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 jurisdiction 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 through 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.

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 to ensuring our reports remain useful and relevant to our collective efforts to protect the Cook Islands against financial and other serious crimes.

**Phil Hunkin**

**Head of the Cook Islands Financial Intelligence Unit**

# 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, the financing of terrorism and the countering of proliferation.

## 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.

Reporting institutions include banks, trustee companies, money remittance and other financial service 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 analyse 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 and the Terrorism Suppression Acts;
- Currency Declaration Act 2015 / 2016;
- misconduct by any person relating to money laundering;
- fraud involving cross-border financial transactions;
- the financing of terrorism;
- the proliferation of weapons of mass destruction;
- the financing or facilitating of bribery and other corrupt practices of any sort; and
- tax evasion (whether or not relating to taxes payable in the Cook Islands).

## Working with partner agencies to combat money laundering and terrorism financing

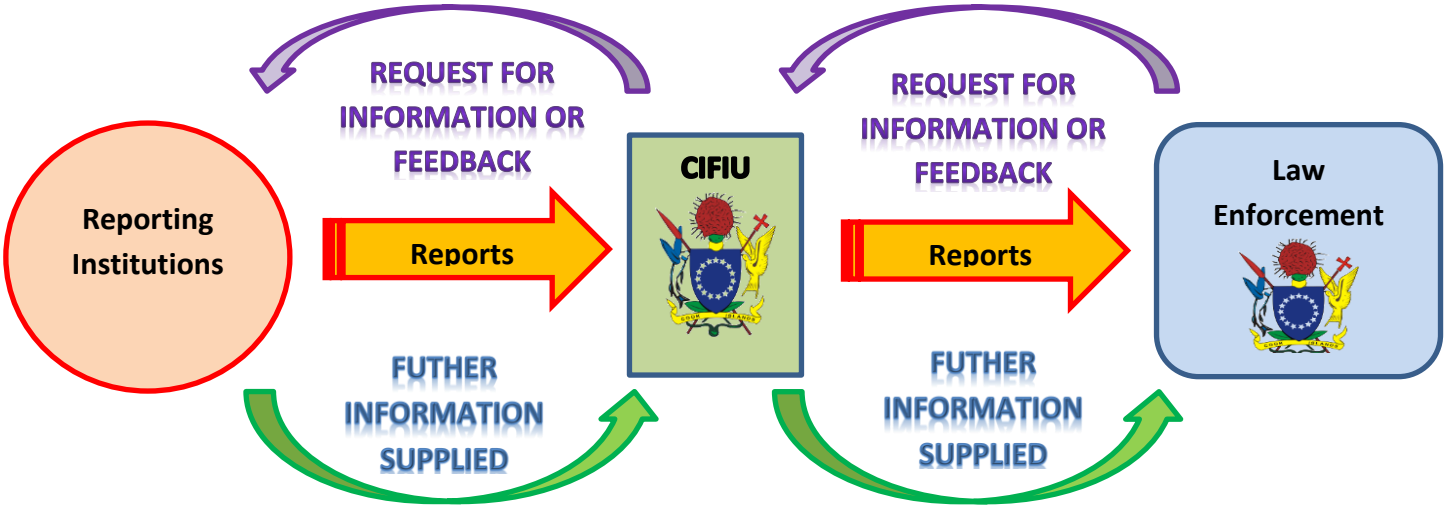
CIFIU's partner agencies include domestic law enforcement agencies and border security agencies. The CIFIU also works closely with its international counterparts to contribute to global

AML/CTF efforts. The CIFIU assisted in a number of cross-agency task force investigations in 2016 as illustrated in the case studies.

## Working with industry

In 2016 the CIFIU received thousands of financial transaction reports and reports of suspicious matters from its reporting institutions, 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 the CIFIU with its partner agencies during 2016. The case studies demonstrate the intelligence value of the transaction and suspicious reports submitted to CIFIU by reporting entities.

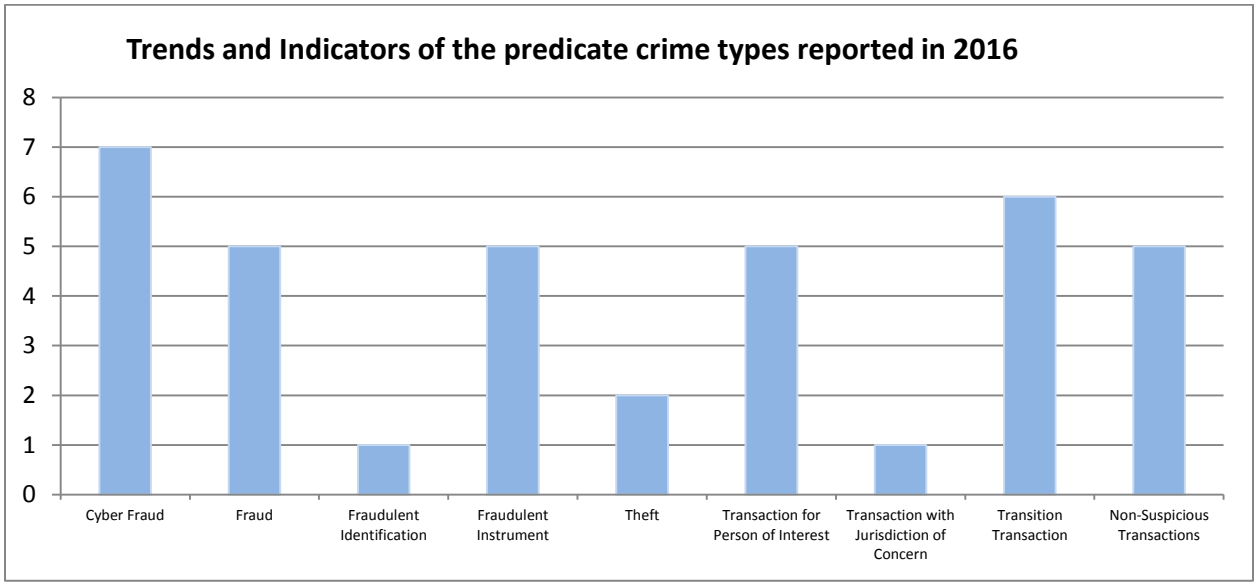
The purpose of this report is to inform the industry and the wider community about the various methods criminals use to conceal, launder or move illicit funds and to commit financial or other criminal activities. This information may assist the industry to strengthen its measures to detect money laundering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

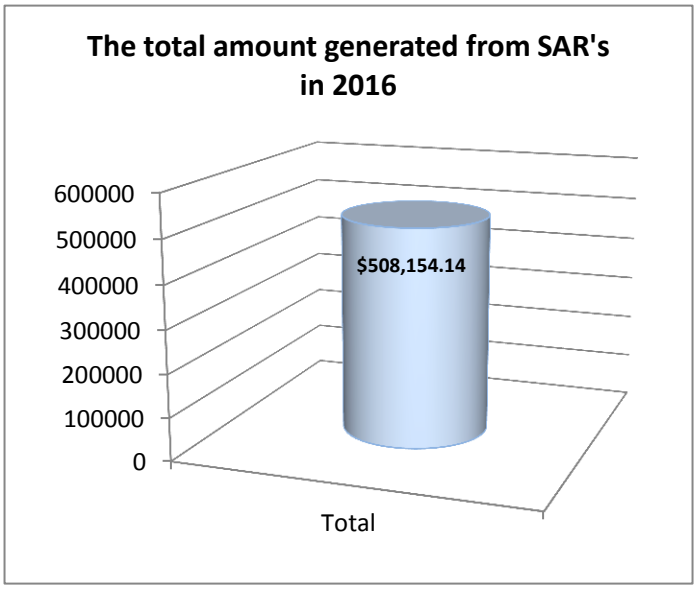
Reporting institutions should use this report to:

- determine what ML/TF vulnerabilities are most relevant to their entities;
- update their AML/CTF guidance material and training; assist with staff training programs, or raise awareness of ML/TF issues within the entity;
- assist 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 report;
- 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 to the CIFIU in 2016.

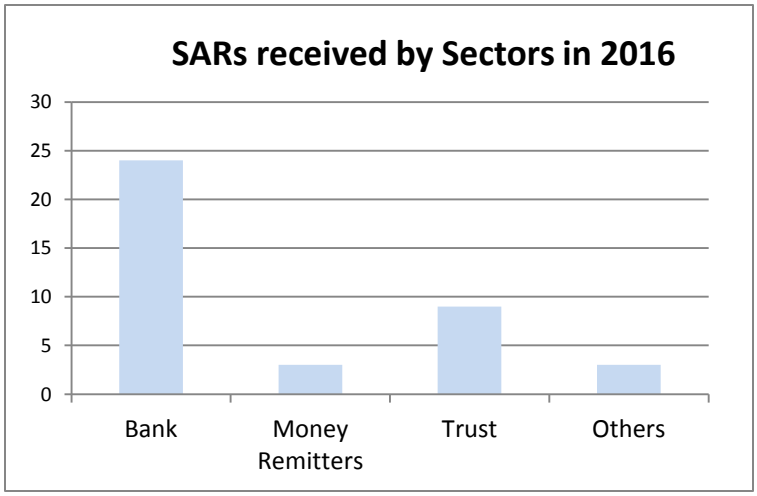




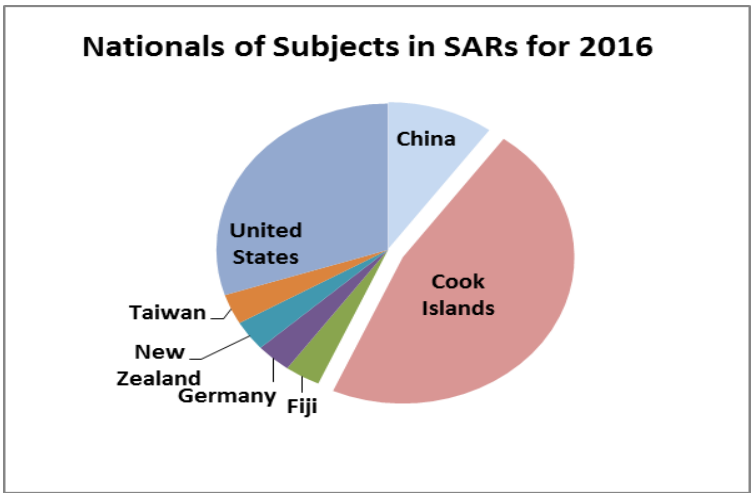

This graph provides the total value of all suspicious transactions reported to the FIU in New Zealand $.

The table below shows a fluctuating trend of SARs for the years represented from 2012 to 2016

| SARs received per annum from 2012 to 2016 | | | | | |
|---|---|---|---|---|---|
| | **2012** | **2013** | **2014** | **2015** | **2016** |
| **Suspicious Activity Reports** | 52 | 52 | 31 | 39 | 39 |

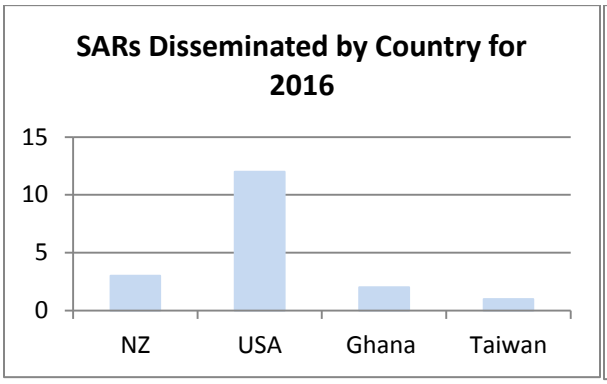


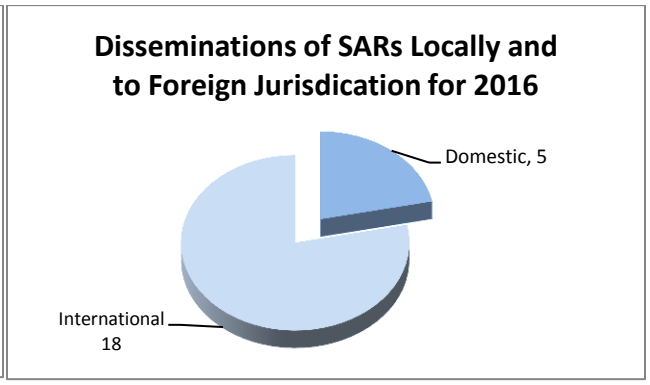

This graph represents the SARs received by major sectors submitting reports to FIU in 2016

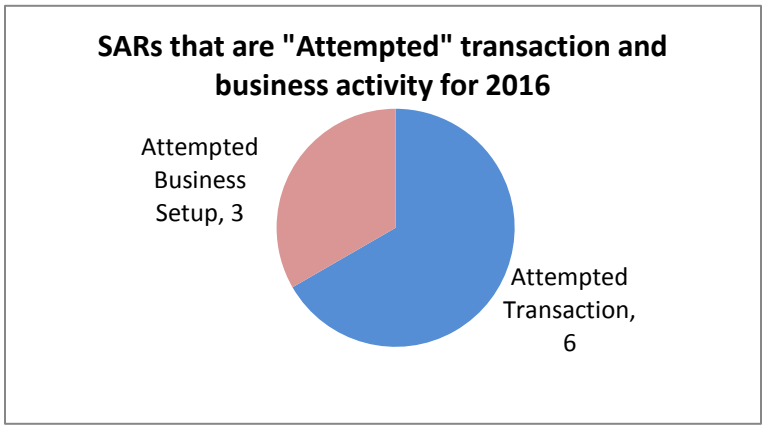



This graph represents the different portions of nationals that are a subject of a SAR for 2016

The two graphs below show the dissemination of SARs to foreign jurisdictions.




This graph show the number of "attempted" transactions and business activities of SARs for 2016

The table below shows the number of reports received by the FIU apart from SARs in the last four years:

| Other Reports received by FIU in 2013 to 2016 | | | | |
|---|---|---|---|---|
| **Reports** | **2013** | **2014** | **2015** | **2016** |
| **Border Currency Reports** | 20 | 26 | 38 | 49 |
| **Cash Transaction Reports** | 2327 | 2786 | 2692 | 3018 |
| **Electronic Funds Transfer Reports** | 6883 | 6874 | 10746 | 18789 |

## The following typologies are extracted from the reports made to the FIU in 2016:

### Transaction with Jurisdiction of Concern

September 2016, an outward transfer of an insignificant amount of money was remitted to a jurisdiction which a local individual operates a business but does not reside in that country.

### Transaction for Persons of Interest

March 2016, a request to set up an entity by a foreign individual who is on the FBI's wanted list was rejected. On two separate occasions, the same individual made contact with two other trustee companies for same purpose which were also rejected.

August 2016, a foreign individual was alerted for participating in various syndicate activities around the Pacific region.

December 2016, a foreign individual was found to be connected in a global ring of crimes in country A and country B.

### Cyber Fraud

January 2016, a fraudster impersonating a sick person was able to influence a local individual in wiring funds overseas to cover medical and life expenses. The fraudster managed to defraud the same individual again in November for the same purpose stated.

February 2016, a fraudster attempted for funds to be wire transferred but withheld beneficiary details of the transfer.

February 2016, a fraudster attempted a fraud through an email requesting immediate action for business customers to logon to their banking system to activate their online account.

May 2016, a fraudster was able to access a local bank account and transferred $3,000 dollars into another local account through the victim's online account.

November 2016, a fraudster managed to defraud a foreign individual of $30,000 for binary shares from his local trust account.

### Fraudulent Identification

March 2016, an attempted email request for the remitting of payments found the supporting identification documents to be invalid and illegitimate. The intended jurisdiction is known to facilitate different types of scam.

### Transition Transaction

February 2016, a substantial amount of seven inward transactions transferred were deposited into a local's individual account from the same ordering customer in a foreign jurisdiction.

June 2016, a local account was found to be conducting multiple transactions from ATM's in a foreign jurisdiction.

July 2016, a local individual was able to pay off loan in a short period of time.

October 2016, a bank account which has been dormant for several months suddenly received a number of deposits into the account and the withdrawal of $10,000 dollars.

October 2016, a personal bank account was used to facilitate the individual's business deposits which were then transferred to the business account in a foreign jurisdiction.

November 2016, a fund from a donor foundation was transferred to a local individual acting for the donor to give to needy families.

### Fraudulent Instrument

June 2016, a civil proceeding was filed in a US Court against the trust and settlor for fraudulent transfer of assets as a result of the settlor defaulting on loan re payment.

June 2016, a foreign company perpetrating penny stock manipulation schemes that generated illegal gross stock sale proceeds had been charged in a US Court in March 2016.

December 2016, a local individual was appointed as an administrator to a deceased relative's estate. The account showed activities of funds going into and out of the account which became of interest to the tax department.

### Theft

February 2016, an employee's action was found to have misused staff wages and salaries inappropriately.

August 2016, an employee's action was found to have misused family member's funds inappropriately.

### Fraud

February 2016, a foreign individual is a settlor to two trust international Trusts companies who was found to deceive and defraud using false documentations.

May 2016, the Manager of a registered company who is related to the settlor of a registered trust was sued in a US Court for fraudulent dealings.

May 2016, a foreign beneficiary principal of an established foundation was detained in prison for the sale of false academic documents.

June 2016, a foreign individual was charged with allegedly taking advantage of legal status and conducting a fraudulent scheme initiating emergency enforcement proceeding by a foreign law enforcement agency.

August 2016, an instruction to wire funds to a foreign bank account under the company's name was found to be illegally providing services to investors, buyers, and sellers in securities.

### Non-Suspicious Transactions

February 2016, a local individual attempted to transfer funds into a joint account in a foreign banking facility.

June 2016, a businessman's account received a substantial amount of payments from government which were transferred into his credit card.

June 2016, a local individual sending funds to a girlfriend in a foreign jurisdiction.

July 2016, an individual remitted funds back to their own account in a foreign jurisdiction prior to departing the Cook Islands.

November 2016, a foreign individual remitting funds back to support family members in their home country.

# 4. Case Studies

## Case 1:

Client B submitted an instruction to Company A for the transfer of USD160, 858.14 to be remitted back to him in Country B. Upon receiving the instruction Bank A initiated customer due diligence as part of their standard procedures which resulted in a positive match on world check. Bank A then referred the information back to Company A for full due diligence on Client B. Bank A had hindered to proceed with the transaction until full diligence was completed. In February 2014, it was revealed criminal charges and sentencing against Client B were laid in court in Country B. The court ordered for the payment of USD15,000 fine and USD44,100 restitution penalty. The forfeiture of his assets including approximately USD1.5 million of seized funds, gold and silver coins were agreed upon. Client B also received an imprisonment term of nine years.

The FIU investigation into this matter undertook reviews of Company A and Client B followed by a formal letter issued against both parties to detain and secure the funds. International inquires involved law enforcement agencies in Country B revealed Client B as not listed in the forfeiture listing. Prior to processing of the transaction to Client B, the law enforcement agency in Country B were alerted.

## Case 2:

The FIU investigated a foreign worker Mr X, who befriended a Mr Y via Facebook. It was found that Mr Y influenced Mr X to use his local bank account as a transit account to receive and transfer funds. Mr X was promised a commission as additional payment. Mr Y accessed the two local bank accounts by breaching the bank's online account's system and transferred $3,000 into Mr X's account. Mr X withdrew funds from its account to pay off outstanding debt. Mr X intended to transfer the remaining funds through a money remitter when the transaction was interrupted. The money remitter refused to process the transaction on the grounds that the transaction was outside the subject's normal remittance behaviour. The FIU investigation resulted in the recovery of three quarter of the funds. No criminal charge was pursued.

## Case 3:

The identity of Miss A was investigated for invalid and illegitimate documentation. The initial request by Mr B instructed the payment of EURO 17,497 from Mr B's company account to Miss A's bank account in country A. The purpose of the transaction was for the release of precious metal stored in country Z. Bank A initiated customer due diligence process on Miss A. The repetitive phone calls and correspondence to Bank A by Miss A prompted a request for documentation to establish the identity of Miss A. Miss A proved to be outside Bank A's Risk Profile who therefore declined the transaction. Bank A's check and screening of the

identification documents failed to meet the bank's requirement. The copies of the identifications were alleged to be a forgery. Bank A has closed its banking relationship with Mr B.