

Financial Intelligence & Profiling: Case Studies

Razim Buksh
Director
Financial Intelligence Unit

FIA Seminar: 23 August 2016
Tower Level 11 – Reserve Bank of Fiji



**FIJ I N S T I T U T E O F
A C C O U N T A N T S**



FijiFIU
Fiji Financial Intelligence Unit



SYNOPSIS

The Seminar will focus on:

“FIU’s intelligence development and profiling framework based on real case studies”

- 1) Bogus phone sales
- 2) Credit card scam
- 3) ATM skimming
- 4) Trade based money laundering.
- 5) For the first time in Fiji, the seminar will highlight **Global threat of foreign terrorist fighters.**

SYNOPSIS

- ✓ Financial intelligence and profiling is a complex process of data analysis, establishing activity patterns and relationships, linking bank accounts and financial transactions to determine any illegitimate cashflow, income and assets.
- ✓ Intelligence outcomes are then linked to the laundering cycle and to the relevant predicate offence before it is disseminated to the key stakeholders.
- ✓ The 5 case studies will showcase the techniques of tactical and operational analysis.

Outline of Presentation

Section 1: The Fiji FIU & Role of the FIU;

Section 2: The Intelligence Development Process;

Section 3: Financial Data Available under FTR Act;

Section 4: Case studies.

Section 1 : Role of the FIU

- ✓ Intelligence Agency of the Government;
- ✓ Intelligence Function:
 - Receive Information;
 - Analyze Information;
 - Develop Intelligence
 - Disseminate Intelligence;
- ✓ Regulatory, Compliance & Enforcement;
- ✓ National/International Networking & Coordination;
- ✓ Assist Investigations;
- ✓ Trace Proceeds of Crime;
- ✓ Awareness & Training;

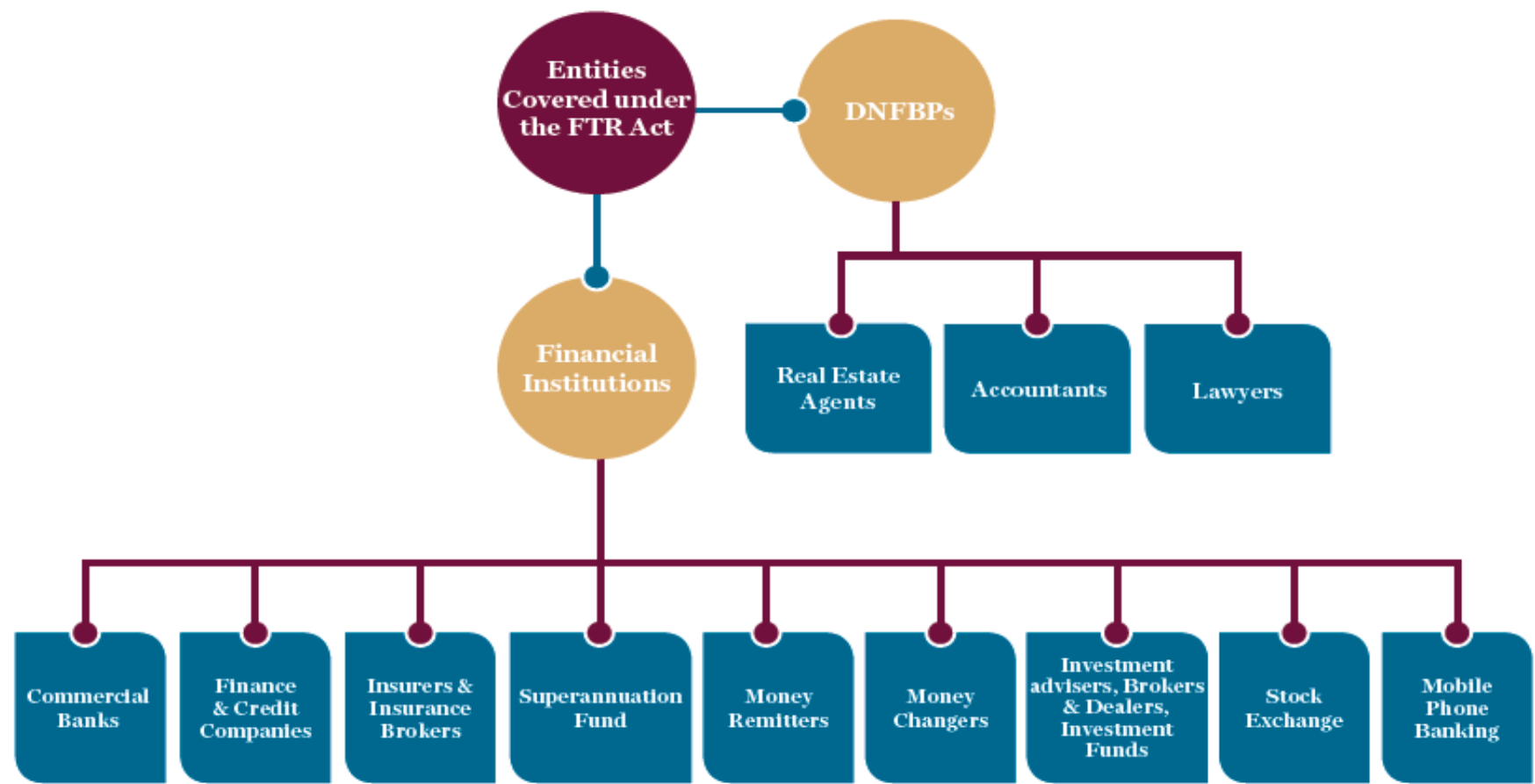
Access to Information

- FIU – FI: good working relationship;
- FIU Powers: timely access to financial records for intelligence purposes;
- FI information: FIU accessed info CANNOT be used as evidence;
- FIU Request: MUST be related to money laundering or any other serious offence;
- FI: Protected under the FTR Act;
- Two FIs recently charged under the FTR Act.



Section 2 : Definition of financial institution

Entities and Businesses Covered by the FTR Act



FIU INTELLIGENCE DEVELOPMENT FRAMEWORK



FijiFIU
Fiji Financial Intelligence Unit

FIU ANALYSIS

Operational Analysis

- ✓ uses available and obtainable information to identify specific targets, to
- ✓ follow the trail of particular activities or transactions, and
- ✓ to determine links between those targets and possible proceeds of crime, money laundering, terrorist financing and predicate offences...



FIU ANALYSIS

Strategic Analysis

- ✓ uses available and obtainable information,
- ✓ including data that may be provided by other competent authorities to identify money laundering and terrorist financing related trends and patterns, and links to
- ✓ National and industry risk assessments.



FijiFIU

Fiji Financial Intelligence Unit

FIU INTELLIGENCE DEVELOPMENT PROCESS

FIU Database

Suspicious Transaction Report



Bank Records

Deposit Slip

Cheque

Case Dissemination Report...

22 September 2010

STRICTLY CONFIDENTIAL

January 2009 to 31 August 2010. Transactions of \$1,000 and more were considered.

Year	Deposits	Withdrawals
2009	\$25,588.00	\$74,384.00
2010	\$47,528.00	\$32,348.00
TOTAL	\$73,116.00	\$106,732.00

Mr. Virendra Kumar deposited \$25,588 into the above account on 21 April 2010 reportedly stating it to be "rate of vehicles". We have established that Mr. Virendra Kumar currently has two motor vehicles (SN 435 and FY 484) and has not sold any of his vehicles since 2002.



Foreign FIUs & Law Enforcement



FIU'S INTELLIGENCE DEVELOPMENT

Mr. X



Ms. XYZ



SEARCH

Same address

Mr. X's mother in law

EFTR

SEARCH

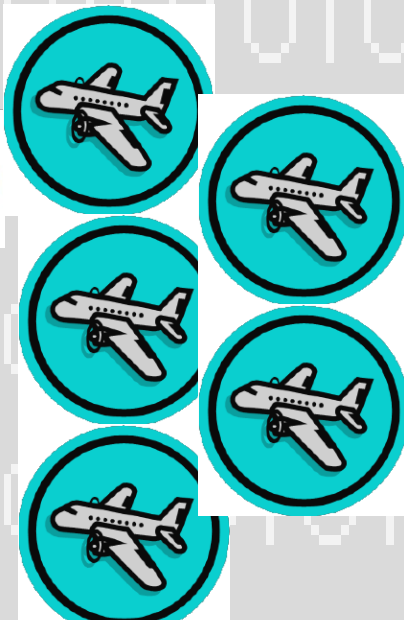
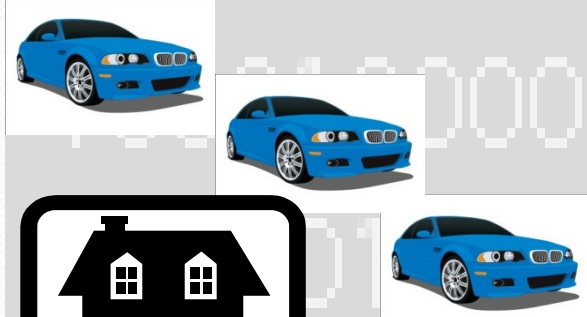
\$\$\$



Bank account of Mrs XYZ

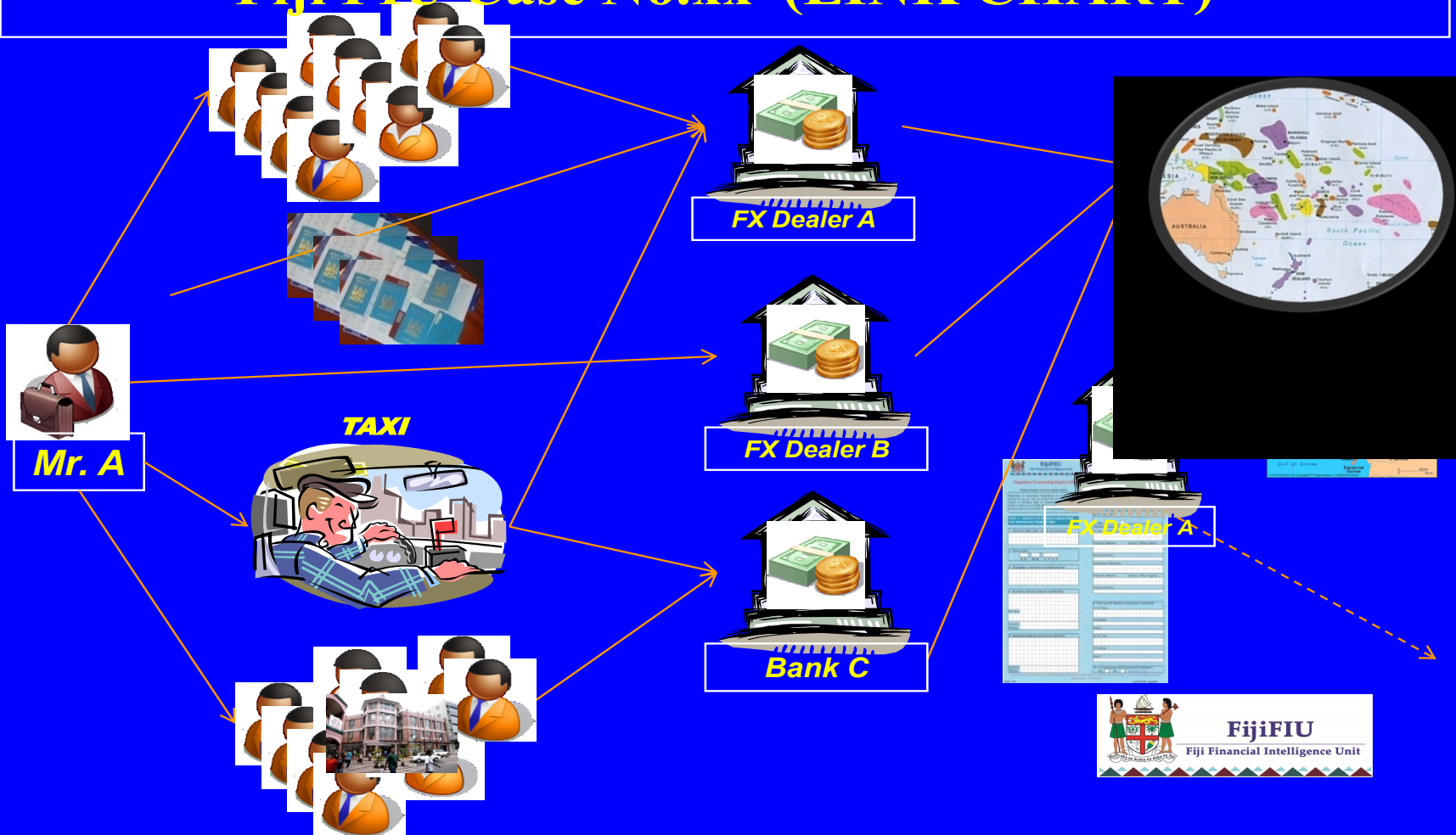
\$\$\$\$

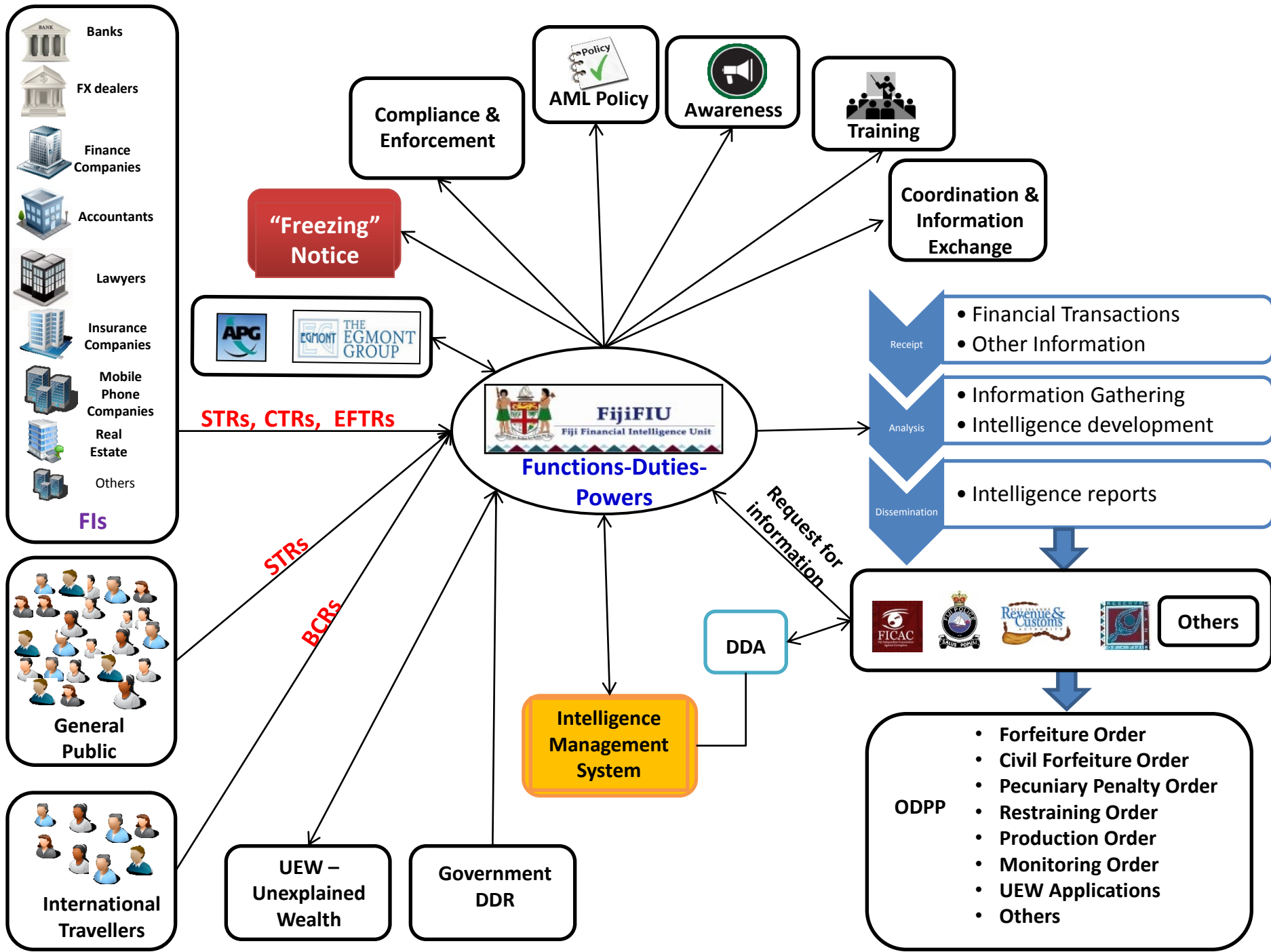
Different companies based overseas





Fiji FIU Case No.xx (LINK CHART)





“taking financial intelligence to the next level”

FIU's Alert and Monitoring System (AMS)

With AMS, the FIU can keep a track of all its reports 24/7 with the help of built-in alert rules that are specifically programmed with key suspicious indicators to detect and flag customers/clients and their suspicious financial transaction activities.

Attributes that are currently monitored by AMS includes:

- ✓ **People/entity/organization;**
- ✓ **Contact address such as residential/business/postal;**
- ✓ **Telephone and mobile number;**
- ✓ **Country;**
- ✓ **Financial transaction of certain threshold;**
- ✓ **Financial institution;**



FijiFIU

Fiji Financial Intelligence Unit



“taking financial intelligence to the next level”

FIU's Data-Mining System (DMS)

With the DMS, the FIU is able to analyze millions of financial transaction data in order to identify links, relationships and patterns of suspicious financial activities.

Patterns of suspicious financial activity identified include:

- ✓ **breakdown of financial transactions and their account holders;**
- ✓ **Money being remitted to (or received from) offshore accounts over a period of time;**
- ✓ **Multiple transactions to a common account (or individual) by multiple individuals (or accounts);**
- ✓ **Transactions below the reporting requirement (structuring, <\$500, <\$10,000);**
- ✓ **Common denominator activity (AMS = name/address/etc)**



CASE STUDY 1: BOGUS PHONE CASES: “Buy 3 Get 1 Free”



FijiFIU
Fiji Financial Intelligence Unit



ADVERTISEMENT IN THE FIJI SUN: 27/05/2016

BUY 3 GET 1 FREE

Brand new Apple iPhone and Samsung Galaxy S7 6s 16gb/64gb/128gb

APPLE IPHONE:

Apple iPhone 6s Plus 128GB UNLOCKED \$800AUD
 Apple iPhone 6s Plus 64GB UNLOCKED \$750AUD
 Apple iPhone 6s Plus 16GB UNLOCKED \$700AUD
 Apple iPhone 6s 128GB UNLOCKED \$700AUD
 Apple iPhone 6s 64GB UNLOCKED \$650AUD
 Apple iPhone 6s 16GB UNLOCKED \$600AUD
 Apple iPhone 6 plus 128GB UNLOCKED \$650AUD
 Apple iPhone 6 Plus 64GB UNLOCKED \$600AUD
 Apple iPhone 6 Plus 16GB UNLOCKED \$550AUD
 Apple iPhone 6 128GB UNLOCKED \$600AUD
 Apple iPhone 6 64GB UNLOCKED \$550AUD
 Apple iPhone 6 16GB UNLOCKED \$500AUD
 Apple iPhone 5s 64GB UNLOCKED \$350AUD
 Apple iPhone 5s 32GB UNLOCKED \$300AUD
 Apple iPhone 5s 16GB UNLOCKED \$280AUD
 Apple iPhone 5c 32GB UNLOCKED \$300AUD
 Apple iPhone 5c 16GB UNLOCKED \$280AUD
 Apple iPhone 5 64GB UNLOCKED \$280AUD
 Apple iPhone 5 32GB UNLOCKED \$230AUD
 Apple iPhone 5 16GB UNLOCKED \$220AUD

SAMSUNG PHONES:

Samsung Galaxy S7 EMAIL FOR PRICE
 Samsung Galaxy S7 edge EMAIL FOR PRICE
 Samsung Galaxy S6 Edge cost \$500AUD
 Samsung Galaxy Note Edge cost \$550AUD
 Samsung Galaxy Note 4 + Gear cost \$400AUD
 Samsung Galaxy S5 + Gear \$370AUD
 Samsung Galaxy Note 3 + Gear \$330AUD
 Samsung Galaxy S4 \$2800AUD
 Samsung Galaxy SIII \$250AUD

DIGITAL / VIDEO CAMERAS:

Nikon D3S 12.1 MP Digital SLR Camera Body with Nikon EN-EL4a ...\$2000AUD
 Nikon D800 Digital SLR Camera (Body Only)..... \$1500AUD
 Nikon D3100 14.2MP DSLR Camera & 18-55 DX VR Lens + 16GB Dlx Kit...\$300AUD
 Canon EOS 1DX.....\$2000 AUD
 Canon EOS 5D Mark II 21MP DSLR Camera...\$1000 AUD
 Canon EOS 450D 12MP DSLR Camera... \$650AUD
 Canon EOS 5D Mark III



Mobile phones, iPhones and Smart phones at good prices.

For information regarding our product and purchasing process

SEND YOUR ENQUIRY TO

Skype: orderproduct

Email: orderproduct@salesperson.net

Email: orderproductbrandnew@gmail.com



FijiFIU

Fiji Financial Intelligence Unit



ADVERTISEMENT IN THE FIJI SUN: 27/05/2016

The advertisement claims to offer a “buy 3 get 1 free” deal on brand new Apple iPhones, Samsung Galaxy Series phones and digital video cameras with prices ranging from **AUD\$220** to **AUD\$2,000**. Interested customers were to contact the following emails:

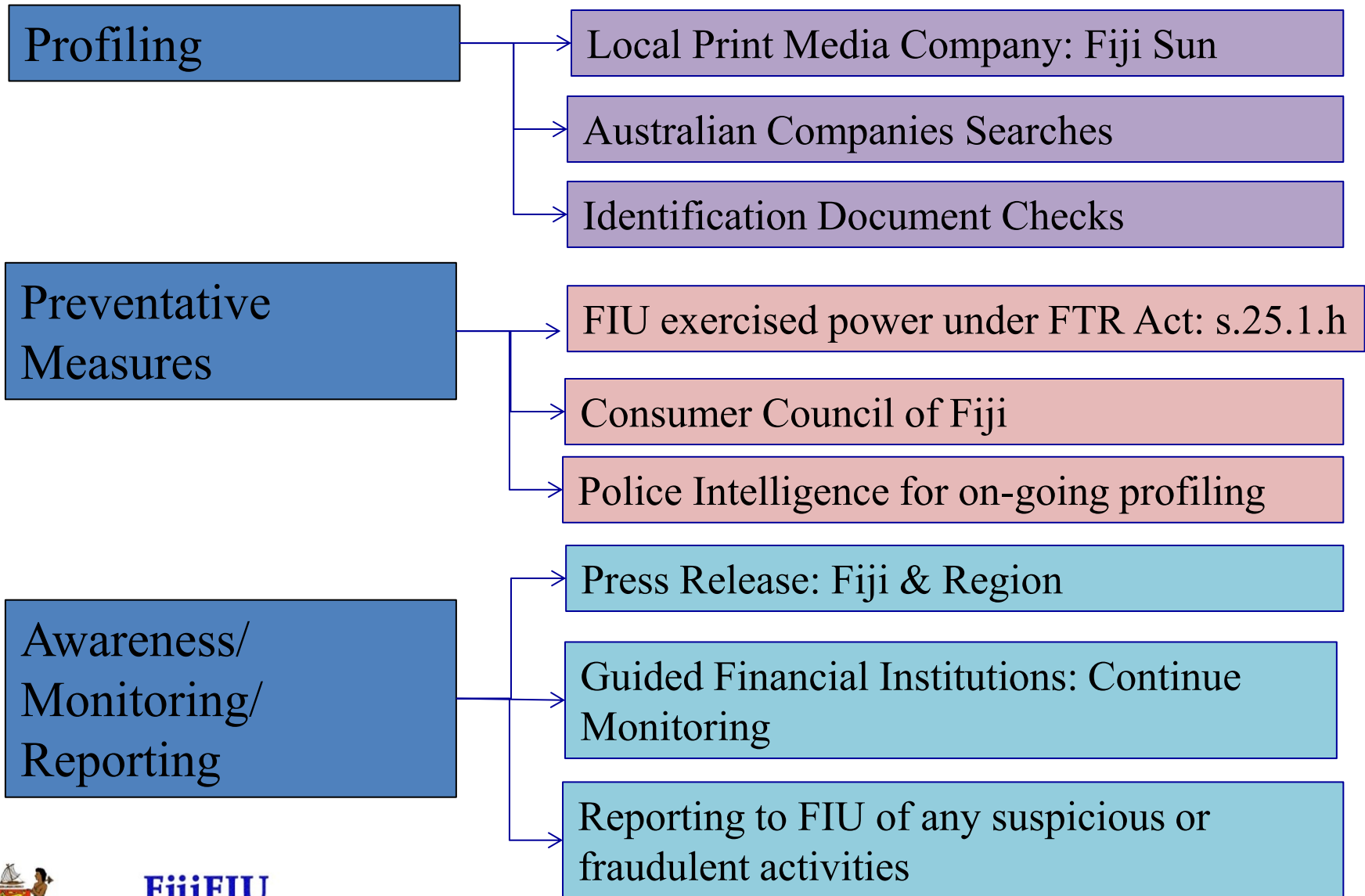
orderproduct@salesperson.net and
orderproductbrandnew@gmail.com or
Skype: orderproduct.



FijiFIU
Fiji Financial Intelligence Unit



Role of the FIU



FijiFIU

Fiji Financial Intelligence Unit

Role of the FIU

- ✓ 27/05/2016: FIU detected Bogus Advertisement in the local news dailies;
- ✓ Special 3-Member Team Formed;
- ✓ 30/05/2016: Communication with the scammers;
- ✓ 01/06/2016: Instruction Notice to Commercial Banks & Money Remittance Service Providers;
- ✓ 02/06/2016: Fiji FIU correspondence with Fiji Sun;
- ✓ 03/06/2016: Disseminated CDR to FPF;
- ✓ 03/06/2016: Fiji FIU issued a Press Release;
- ✓ 07/06/2016: Fiji FIU sent a request to UK FIU.

FIU PROFILING OPERATIONS

- ✓ Two FIU “Analysts/Agents” began to communicate with the scammers on mobile phone and emails;
- ✓ Series of emails exchanged between the scammers and Fiji FIU;
 - ❖ 2 persons identified as the scamming beneficiaries;
 - ❖ 1 beneficiary bank account and name (UK) and its details provided by the FI/general public to the FIU;



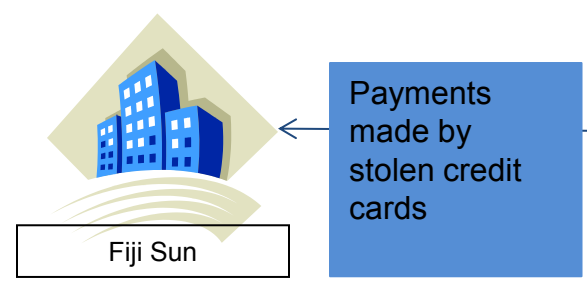
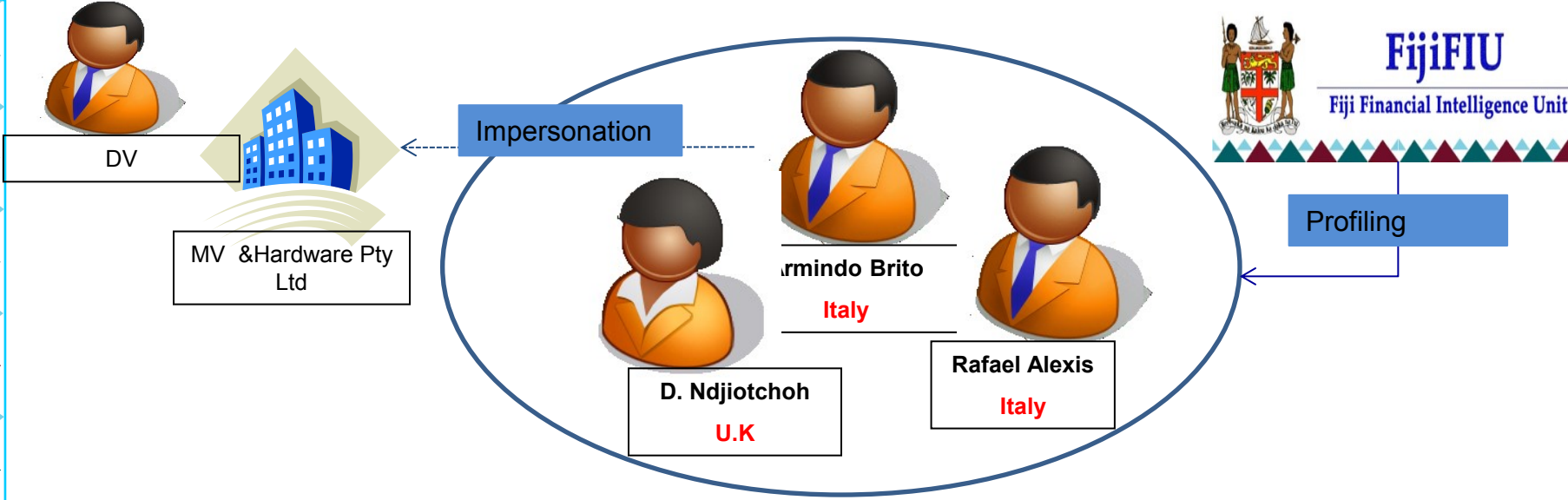
FijiFIU

Fiji Financial Intelligence Unit



Role of the FIJI FIU ANALYSTS

- ✓ FIU Analyst X emailed to the scammers by a dedicated gmail account enquiring about the phone deals. The email communication was sent via a protected IP address. No communication was sent via the RBF network.
- ✓ FIU Analyst Y engaged in telephone conversation with the alleged scammers to ascertain further details.
- ✓ FIU Analysts X & Y engaged in financial profiling

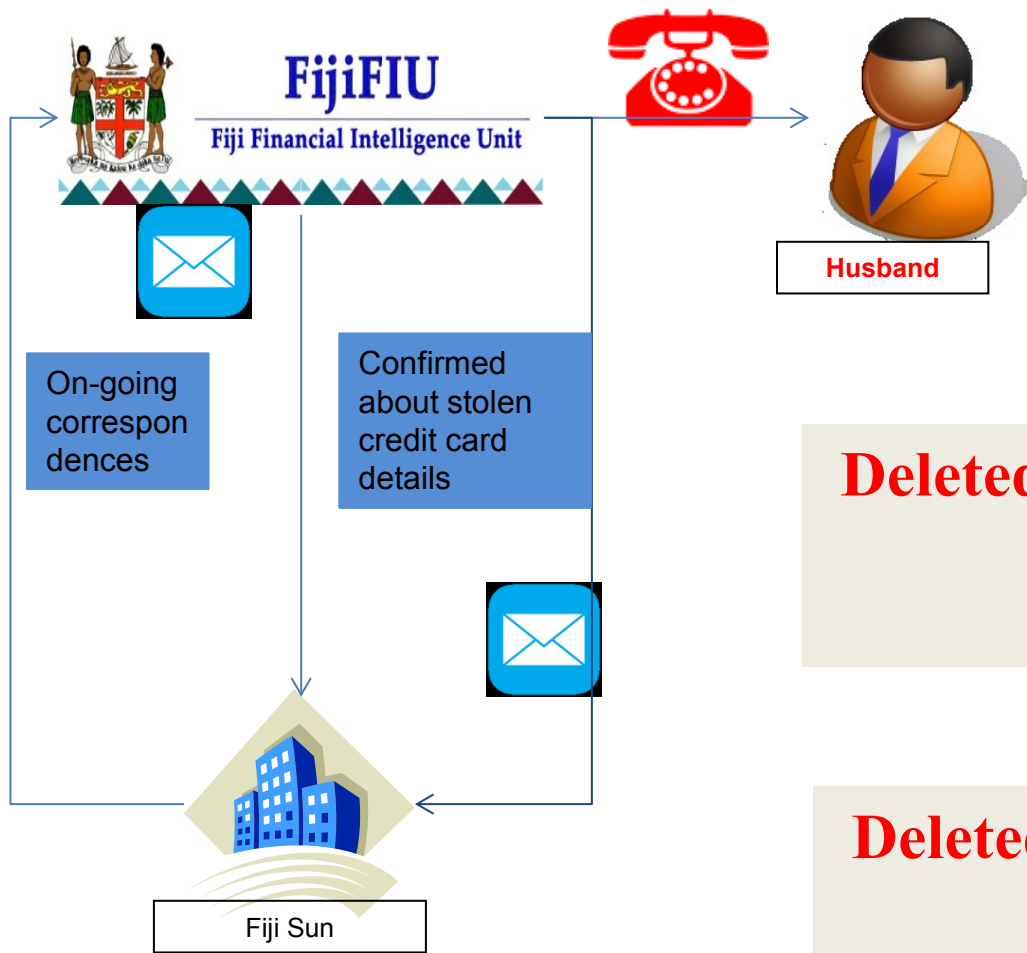


Credit Card 1: - MASTERCARD
 Payment on CARD
 NO:54Deletednumbers7 EXP:10/20
 CVV:132 NAMES ON CARD:
Mr. RP

Credit Card 2: - VISACARD
 VISA CARD NO: 41Deleted numbersCVV:100
 (New card details after first card rejected)

Credit Card 3: - VISACARD
 VISA CARD NO:4120397130187211
 Exp:05/18 Cvv:938





Deleted content

Deleted content

Deleted content

Deleted content

CONTACT WITH SCAMMERS

On Mon, May 30, 2016 at 5:24 PM, Sale department

<orderproductbrandnew@gmail.com> wrote:

Thank you for the mail and interest in our products and services. All Our product is brand new and comes with 1 year international warranty and 6 Months return policy. Kindly get back to us with brand and model of product you want to buy from us, With quantity needed, Also your direct phone number.

SALE REP.

CODE 35636

PHONE CONSULTANTS LIMITED

Registered No: 04693120

Address:83 NOTTINGHAM ROAD,

ITALY BRANCH

CODE 6778



FijiFIU

Fiji Financial Intelligence Unit





Fiona Usa <ladyfiousa@gmail.com>

ORDER PAYMENT TODAY.....

1 message

Sale department <orderproduct@salesperson.net>

Tue, May 31, 2016 at 4:45 PM

To: [redacted]sa@gmail.com>

Hello Fiona,
3 X Apple iPhone 5 16GB UNLOCKED \$1010FJD
Plus 1 free Samsung Galaxy S4
Free Shipping
Total Cost:- \$1010 FJD

So in order to proceed with shipment , Below is the Company Financial Accountant details (Name and Address) you need to transfer the payment through western union transfer online www.westernunion.com or go to any western union money transfer shop nearer your location for the transfer.

FULL NAME : Armindo brito
Address: Via Cristoforo Colombo,70,
City:Campania
Napoli, Italy
Post code:80133

As soon as you make the payment , get back to us with the Money Transfer details as below :

MTCN NUMBER : ???????.....10 DIGIT NUMBER
SENDERS NAME : ??????
SENDERS ADDRESS : ??????
AMOUNT TRANSFERRED : ???????

so that we can confirm your payment and proceed immediately with shipment.Once we confirm your payment we will ship your order immediately and then send you details ..

- 1.Tracking codes # Fedex
- 2.Air way Bill
- 3.Commercial Reception
- 4.Commercial Invoice to review order.

Awaiting payment details to proceed.

Thanks !

SALE REP.
CODE 35636

Sent: Tuesday, May 31, 2016 at 8:34 AM
From: [redacted]sa@gmail.com>
To: orderproduct@salesperson.net
Subject: IPHONE 5

hi salesdepartment,

i want to buy 3 phones so i can get 1 free. i want to buy 3 apple iphone5 16 gb and the free one i will like to get a samsung phone.

**CONTACT WITH
SCAMMERS**



FijiFIU
Fiji Financial Intelligence Unit



CORRESPONDENCE WITH WESTERN UNION GLOBAL

- ✓ Additional financial profiling and networking



INSERT AUDIO RECORDING

- ✓ Communication with the scammers:
FIU Special Undercover Agent



Deleted content

**FIU exercised
power under
FTR Act:
s.25.1.h:
FIU
Instruction
Notice**



FijiFIU
Fiji Financial Intelligence Unit



Deleted content

REQUEST BY FIJI FIU TO FIJI SUN: DISCONTINUE ADVERTISING



FijiFIU
Fiji Financial Intelligence Unit



PRESS RELEASE BY FIJI FIU



PRESS RELEASE

Press Release No.	: 15/2016	Telephone	: (679) 331 3611 / 322 3333
Date	: 3 June 2016	Facsimile	: (679) 330 2094 / 331 6454
		Email	: info@rbf.gov.fj or info@fijifiu.gov.fj

BOGUS PHONE SALES – “BUY 3 GET 1 FREE”

The Fiji Financial Intelligence Unit (FIU) would like to warn and advise members of the public to exercise extreme caution when responding to advertisements through the print media, unsolicited emails and communication through social media on cheap mobile phone deals that make promises such as “buy 3 get 1 free”.

The Director of FIU, Mr Razim Buksh said that the FIU has established that the “buy 3 get 1 free” advertisement in the local print media on 27 May 2016 and 1 June 2016 is bogus and a scam.

The advertisement claims to offer a “buy 3 get 1 free” deal on brand new Apple iPhones, Samsung Galaxy Series phones and digital video cameras with prices ranging from AUD\$220 to AUD\$2,000. Interested customers were to contact the following emails: orderproduct@salesperson.net and orderproductbrandnew@gmail.com or Skype: [orderproduct](https://www.skype.com/en/contacts/voice/orderproduct).

Mr Buksh said that this was a well-planned scam by international criminal gangs that used a fake email address purporting to be from two legitimate businesses in Australia and three sets of stolen personal credit card details to pay for the advertisement. The FIU was able to verify with the owners of the Australian businesses that they had nothing to do with the bogus phone sales scam. The criminals had also used stolen ID cards and were purporting to be “sales staff” of a legitimate telecommunications related company based in the United Kingdom. The beneficiaries were located in Italy and the United Kingdom there could be other criminal syndicates located elsewhere.



FijiFIU
Fiji Financial Intelligence Unit



Role of the FIU

- ✓ It was established by Fiji FIU that the payments made for the adverts were done using stolen credit cards;
- ✓ Western Union was alerted and the beneficiary details provided to them for monitoring and reporting;
- ✓ Fijians cautioned of the bogus advertisement;
- ✓ Engagement with the Consumer Council of Fiji and the Fiji Police Force; and
- ✓ UK FIU was alerted to the possible use of a UK based bank account by the scammers.



FijiFIU

Fiji Financial Intelligence Unit



CASE STUDY 2: CREDIT CARD SCAM



CASE STUDY 2: CREDIT CARD SCAM

The Fiji FIU received three STRs on the bank accounts of Company X and Company Y for conducting several fraudulent transactions from newly installed EFTPOS terminals.

The owners of the companies opened business accounts and rented EFTPOS terminals using fake foreign passports.

Companies X and Y received deposits totalling \$0.7 million from merchant sales over a period of two weeks. Fiji FIU analysis of the company records revealed that the Companies X and Y were shell companies.

Further analysis of the bank statements revealed that the transactions were being conducted with what was suspected to be stolen credit cards identity from foreign jurisdictions.

The case was disseminated to the relevant law enforcement agency.

Possible Offence:

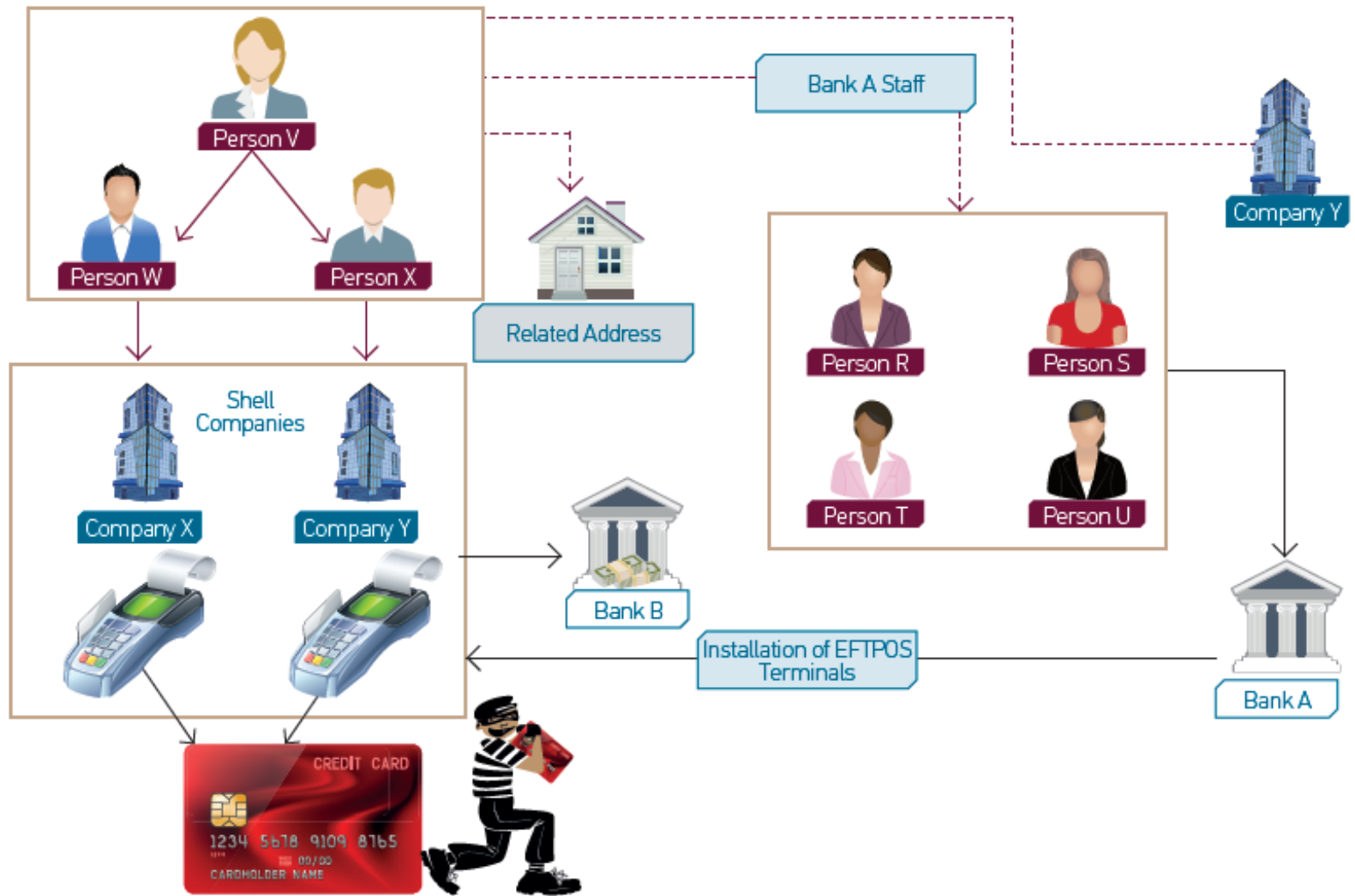
- Money Laundering
- Credit Card Fraud

Indicators

- Using fake documentation to open business accounts
- Set up of shell companies to facilitate credit card transactions
- Conducting several fraudulent transactions from a newly installed EFTPOS terminal



Link Chart showing the parties involved in the EFTPOS terminal fraud



CASE STUDY 3: ATM SKIMMING



ATM SKIMMING

- ✓ On 4 December 2015, 6 Chinese nationals arrived into Fiji from Hong Kong on flight FJ392.
- ✓ On 6 December 2015, the Lautoka Police arrested the Chinese nationals following tip-off from a taxi driver.
- ✓ On 6 December 2015, between 6.00pm-7.30pm, unusual activity was noted at the ANZ branch ATM in Lautoka.
- ✓ A taxi driver witnessed the Chinese nationals conducting several suspicious withdrawals at the ANZ branch ATM.



FijiFIU

Fiji Financial Intelligence Unit



ATM SKIMMING

- ✓ On 7 December 2015, BANK B staff during routine checks at the BANKB Lautoka City Mall ATM detected 2 captured cards. The cards were unique in design and did not resemble normal bank handy cards. The front of the card was black in color and rear of the card had PIN number pasted on it.
- ✓ The Lautoka Police officials uncovered an ATM scam involving the 6 Chinese nationals mentioned above. The Chinese nationals were found in possession with a number of ATM cards. 384 plastic cards of similar nature were confiscated by the Lautoka Police.



FijiFIU

Fiji Financial Intelligence Unit



ATM SKIMMING

- ✓ It was noted that the Personal Identification Numbers (PIN) were pasted on the back of the cards. It was difficult to determine which cards belonged to which bank and which customer accounts were compromised. A card reader was used by BANK A to determine the card holders.
- ✓ On 28 December 2015, the Lautoka Police officials seized additional 104 ATM cards and a card making device. The card making device was reportedly hidden in a sofa at Galaxy Hotel in Nadi. A sum of \$22,807.00 was also recovered from the suspects.



FijiFIU

Fiji Financial Intelligence Unit



ATM SKIMMING

- ✓ The Magistrates Court in Lautoka handed a two-year and 11 months prison terms to the six Chinese nationals on 27 June 2016;
- ✓ charged with **theft and dishonestly dealing in personal financial information.**

Prison terms for six Chinese nationals

Shayal Devi
Monday, June 27, 2016

THE Magistrates Court in Lautoka has handed a two-year 11 months prison terms to six Chinese nationals charged with theft and dishonestly dealing in personal financial information.

Appearing before Magistrate Raramasi Salakubou on Monday were Sanlin Xie, Changbao Xie, Liu Jinling, Zhong Chenhua, Weiqiang Liu and Yanyan Yang.

The court heard the men were apprehended in different locales throughout Lautoka last December.

They had arrived in the country as tourists and were found making suspicious withdrawals at an ANZ ATM in Lautoka.

Upon capture, police found more than 400 ATM cards on the men.

While delivering the sentence last week, Mr Salakubou said he had taken into account the seven months the men had spent in remand.

He said the men had shown remorse for their crimes and had co-operated with police.



[+ Enlarge this image](#)

Some of the Chinese nationals outside court. Picture: REPEKA NASIKO



FijiFIU

Fiji Financial Intelligence Unit



6 Chinese nationals charged in relation to alleged ATM scam appear in court

By Swastika Singh

Thursday 21/01/2016

Share



The six Chinese nationals who are charged in relation to the alleged ATM scam in Lautoka, appeared in the Lautoka Magistrates Court today.

The six have been charged with four counts of theft and four counts of dishonestly obtaining or dealing with personal financial information.

Magistrate Salakubou Raramasi remanded them in custody upon the request by the Prosecution.

Assistant Superintendent of Police Anil Prasad informed the court that the six do not have a fixed residential address and they were to leave the country the day after the alleged withdrawals from different ATMs in Lautoka.

Prasad told the court that it is a serious matter and the

investigation is still ongoing.

Prasad informed the court that more charges are expected to be laid after the investigation is completed.

It is alleged that the six Chinese nationals made about 60 withdrawals from different ATMs last month.

Police say a tip was received from a taxi driver at the Lautoka Police Station that a group was seen conducting several suspicious withdrawals in the area.

They were also found with a number of ATM cards.

6 Chinese nationals in custody over major ATM scam

By Vijay Narayan

Thursday 10/12/2015



Police are now investigating a major ATM scam involving a few individuals.

Six Chinese nationals are in police custody after they were found in possession with a number of ATM cards over the weekend.

Police Chief of Intelligence and Investigations, ACP Henry Brown says a tip was received from a taxi driver on Sunday at the Lautoka Police Station that a group of Chinese nationals were seen conducting several suspicious withdrawals in the area.

Role of the FIU

- ✓ Linked up with the commercial banks (Bank A , B & others) involved as the Fiji FIU received STRs.
- ✓ Fiji FIU attended the Association of Banks in Fiji (ABIF) special meetings on this case.
- ✓ Fiji FIU linked the FPF investigators with the commercial banks.

Fraudulent cards being used to scam ATMs - McCarthy

By Ana Ravulo

Friday 11/12/2015

Share 7



Kevin McCarthy

The Association of Banks of Fiji says that the perpetrators who are scamming the ATMs are using fraudulent cards with real customers card details to withdraw money.

Chairman Kevin McCarthy says these people are using a skimming device either attached to an ATM or via a hand held card reader device.

McCarthy says these transactions can affect all bank customers but mostly limited to customers of ANZ, BSP and Westpac due to their larger ATM reach and interchange capabilities.

He adds that it is important for customers to understand that when a fraudulent transaction has been identified, these fraudulent transactions will be refunded to the customers once appropriate investigations have been completed.

The association is currently assisting the Police and the Finance Intelligence Unit of the Reserve Bank of Fiji to determine the apprehended criminals.

Six Chinese nationals who made about 80 withdrawals with a number of cards are expected to be charged later today.

CASE STUDY 4:

TRADE BASED MONEY LAUNDERING



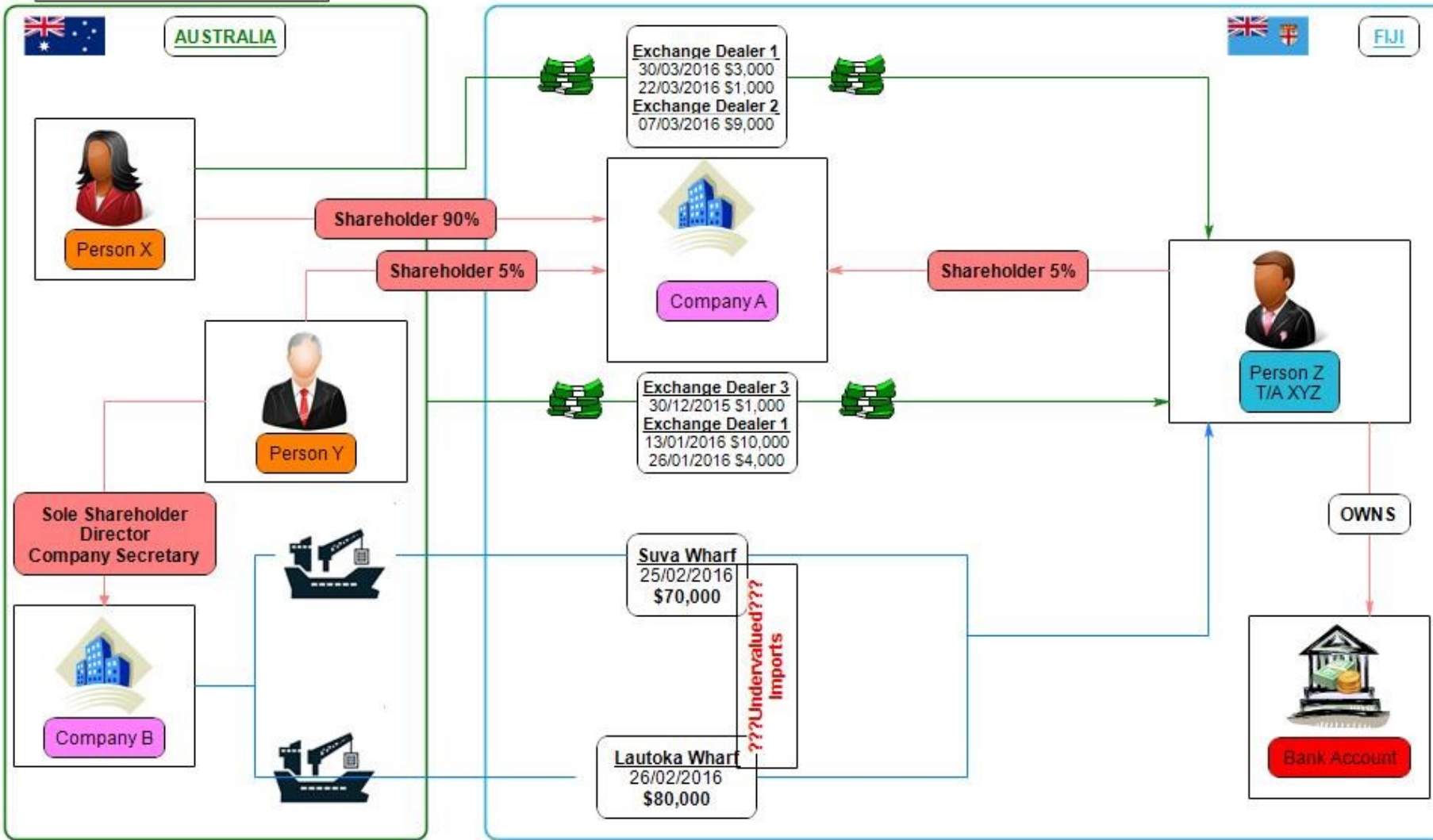
FijiFIU
Fiji Financial Intelligence Unit





ALLEGED TRADE BASED ML

Fij FIU Confidential Report



ALLEGED TRADE BASED ML

- ✓ STR: Reported by Member of the Public.
- ✓ Person X & Y (foreigners) were reportedly using Person Z to set up a “construction company”, Company A in Fiji.
- ✓ The name of the company Person Z was trading as (XYZ) was similar to Company A.
- ✓ The Fiji FIU conducted financial checks and established that Person X & Y were sending funds via three separate FX dealers to Person Z between Dec 2015 and March 2016.
- ✓ The Fiji FIU conducted checks with FRCA Customs and established that two excavators were sent from “Company B” in Australia to Person Z (T/A Company XYZ) in Fiji.



FijiFIU

Fiji Financial Intelligence Unit



ALLEGED TRADE BASED ML

- ✓ FRCA Customs interviewed Person Z and established that there may have been possible undervaluation of invoices for the excavators.
- ✓ Moreover, Fiji FIU established that the excavators were intended to be used for Company A's operations.
- ✓ Fiji FIU established that Company A was not yet registered with Investment Fiji & Registrar of Companies. It was only registered after the excavators came in the country and funds were exchanged between the parties.
- ✓ Suspicion: **“Business transactions were conducted between the foreigners and Person Z without proper business registration”**.



FijiFIU

Fiji Financial Intelligence Unit



ALLEGED TRADE BASED ML

Indicators:

- ✓ Use of Person Z as a mule to facilitate alleged trade based ML.
- ✓ Engaging in alleged tax/vat evasion by Person Z and Company XYZ as funds sent from Australia to Person Z via FX Dealers could be business funds which were not remitted to the bank account of Person Z.
- ✓ Possible manipulation of invoices by understating the value of the machinery.



FijiFIU

Fiji Financial Intelligence Unit



TERRORISM

FS: 20/8/16

ISIS: Sydney Court Denies Bail To Tongan-Australian

Australian Police stated she was found with a hunting knife and flag in her handbag as well as instructions for making a bomb detonator

Tongan-Australian teenager and Muslim convert Alo-Bridget Namoa, 19, was denied bail by a Sydney court over terrorism charges on August 5.

Australian news media reported bizarre behaviour exhibited by Alo-Bridget in court, reporting that she was laughing and pulling faces during proceedings.

Namoa's barrister Mr Kahn told the Sydney court that Alo-Bridget was suffering from schizophrenia and hallucinations.

She is formally charged with possessing an item connected to a terrorist act and recklessly collecting documents connected to a terrorist act.

Namoa along with her husband Sameh Bayda, 19, was arrested in February this year after Australian Police alleged the teenage couple were collecting information on how to carry out a terrorist attack.



Alo-Bridget Namoa.

Australian Police stated she was found with a hunting knife and an ISIS flag in her handbag as well as instructions for making a bomb detonator.

Videos of real life executions and beheadings were also discovered on her mobile phone. Crown barrister Michelle English told the court there was a "wealth of extremist material on her phone".

Prosecutor David Anderson stated "Rather than simply being influ-

enced by Mr Bayda, she's thinking for herself.....There is a concern she is a supporter of ISIS.

"The accused was up to her eyeballs in what her husband was up to."

In her defence, Namoa's barrister Mr Kahn argued that Alo-Bridget was suffering from mental health problems and that her mental health had been deteriorating while she was in custody.

The court heard that she was being kept in permanent isolation with limited health care, spending 22 hours a day in a single cell and two hours a day in an isolated caged exercise yard.

The court also heard that she had told prison doctors "I hear voices. It tells me to hurt people but I don't" and "the toilet talks to me, it makes me laugh".

According to local reports, former classmates and friends were baffled by Namoa who was originally a Catholic but had undergone a conversion to Islam during High School.

According to *The Daily Telegraph* one of her friends stated "I'm just so shocked, I can't believe what's happened to her, I would never in a million years have picked it."

Matangi Tonga

Feedback: jyotip@fijisun.com.fj



FijiFIU

Fiji Financial Intelligence Unit





FOREIGN TERRORIST FIGHTERS

UNSCR 2178 Definition:

Individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict.

FOREIGN TERRORIST FIGHTERS: CASE STUDY

Deleted content



FijiFIU
Fiji Financial Intelligence Unit



FOREIGN TERRORIST FIGHTERS: CASE STUDY

Deleted content



FijiFIU
Fiji Financial Intelligence Unit



FOREIGN TERRORIST FIGHTERS: CASE STUDY

Deleted content



FOREIGN TERRORIST FIGHTERS: Legislative Reforms

BILL NO. 23 OF 2016 A BILL

FOR AN ACT TO AMEND THE PUBLIC ORDER ACT (CAP. 20)

ENACTED by the Parliament of the Republic of Fiji—

Short title and commencement

- 1.—(1) This Act may be cited as the Public Order (Amendment) Act 2016.
- (2) This Act comes into force on the date or dates of its publication in the Gazette.
- (3) The Public Order Act (Cap. 20) is referred to as the “Principal Act”.

PARTS inserted

2. The Principal Act is amended by—

Foreign terrorist fighters

12X. Any person who—

- (a) finances, recruits, organises, transports or equips individuals who travel abroad or to Fiji for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training;
- (b) travels or attempts to travel abroad, or, travels or attempts to travel to Fiji, for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts, or the providing or receiving of terrorist training;
- (c) wilfully provides or collects, by any means, directly or indirectly, funds with the intention that the funds should be used, or in the knowledge that they are to be used, in order to finance the travel of individuals who travel abroad or to Fiji for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training;
- (d) wilfully organises, facilitates, plans, supports, including acts of recruitment, by any means, the travel of individuals abroad or to Fiji for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training; or
- (e) participates in, facilitates, organises, or supports acts prohibited under the United Nations Security Council Resolution 2178 and subsequent resolutions,


commits an indictable offence and is liable upon conviction to a fine not exceeding \$150,000 or imprisonment for a term not exceeding 20 years, or to both.”




FijiFIU
Fiji Financial Intelligence Unit




CASE STUDY 6: IMPERSONATION: SOCIAL MEDIA


 People

 **Barry Whiteside** + Add Friend ...

Lives in Suva, Fiji

 **Barry Whiteside** + Add Friend ...

Governor at Reserve Bank of Fiji
Studied at University of the South Pacific
From Suva, Fiji

 **Barry Whiteside**

Listens to Emily Jennings - Soprano
Likes Rugby (sport)

[See more](#)



CASE STUDY 6:

IMPERSONATION: SOCIAL MEDIA

Fake Facebook profiles

- ✓ Cybercriminals/scammers have created several fake *Facebook* profiles of “Barry Whiteside”, Governor of the RBF.
- ✓ The Governor **does not have any *Facebook* profile** under his name.
- ✓ Cases have been brought to the attention of the FIU and the RBF that these false personations were used to provide fake RBF approvals for victims to remit funds to secure proceeds of fake lotteries, investments and loans.



FijiFIU

Fiji Financial Intelligence Unit



CASE STUDY 6:

IMPERSONATION: SOCIAL MEDIA

Scam Emails

- ✓ A number of incidents of scam emails have also surfaced claiming to be from Governor Whiteside with fake messages and documents.



CASE STUDY 6:

IMPERSONATION: SOCIAL MEDIA

Bogus Loans and Grants

- ✓ The letterhead and logo of the RBF has been used by criminals on documents purporting to offer loans and grants to victims who began to correspond with the criminals using fake social media profiles and emails.



CASE STUDY 6: IMPERSONATION: SOCIAL MEDIA

FIJI SUN | FRIDAY, AUGUST 19, 2016 | FIJISUN.COM.FJ

6 BUSINESS

SCAM

RBF cautions over fake Facebook account of Governor, transactions

CENTRAL BANK: GOVERNOR DOESN'T HAVE FACEBOOK PROFILE UNDER HIS NAME, CYBERCRIMINALS CREATE FAKE ACCOUNT

Members of the public have been cautioned on recent cases of fake Facebook profiles, scam emails and bogus loans involving the Reserve Bank of Fiji. The caution has come from the Financial Intelligence Unit (FIU) and the Reserve Bank of Fiji.

Cybercriminals have created several fake Facebook profiles of "Barry Whiteside", Governor of the RBF although the Governor does not have any Facebook profile under his name.

Cases have been brought to the attention of the FIU and the RBF that these false impersonations were used to provide fake RBF approvals for victims to remit funds to secure proceeds of fake lotteries, investments and loans.

Mr Whiteside said the RBF and its staff do not communicate with anyone via Facebook or other social media on official business matters.

He said anyone who receives any communication or document purporting to be sent from him or any staff of the RBF must immediately refer it to the RBF and FIU for verification and further investigation.

Scam Emails and bogus loans

A number of incidents of scam emails have also surfaced claiming to be from Governor Whiteside with fake messages and documents.

Members of the public and stakeholders of the RBF are advised to exercise extreme caution when they receive unsolicited emails or lookalike emails without the official RBF domain @rbf.gov.fj.



RBF highlighted all official emails from RBF have the domain @rbf.gov.fj.

viding personal or commercial loans.

The victims should immediately cease communication with the criminals.

Members of the public are warned not to provide any personal and financial information on the fake loan documents.

Abuse of social media

Razim Buksh, Director of the Financial Intelligence Unit said that the above incidents were not caused by any compromise to the RBF's website or Email servers.

He said that in the above-mentioned cases, cybercriminals have abused social media to impersonate Governor Whiteside and commit fraud.

Mr Buksh said members of the public should not open unsolicited and suspicious email messages.

Unsolicited email messages (that usually provide a website link or an attached document) could be infected with dangerous viruses that could compromise your email account, social media profiles, personal computers and mobile devices.

The Cybercrime Unit of the Fiji Police Force is currently investigating the matter.

Members of the public are advised to report suspected cases of impersonations and fraud to the Fiji Police Force or the FIU on phone number 322 3333 or email: info@fijifu.gov.fj.



FijiFIU

Fiji Financial Intelligence Unit



CASE STUDY 6: IMPERSONATION: SOCIAL MEDIA

Bogus Loans and Grants

RESERVE BANK OF FIJI
APPLICATION FORM

FORM RS-02



Internal loan Review				
Primary officer :		Prepared by :		
Date prepared :				
Loan request				
Borrower :				
Business information:	Form :			
	Organ date :			
	type :			
	Management :			
	Ownership :			
Guarantors : typically the owner of the business				
Request :				
Purpose :				
Terms :				
Type	Amount	Rate/fees	Term	Repayment



FijiFIU
Fiji Financial Intelligence Unit



CASE STUDY 6:

IMPERSONATION: SOCIAL MEDIA



PRESS RELEASE

Press Release No: 19/2016 Telephone: (679) 331 3611 / 322 3333
Facsimile: (679) 330 2094 / 331 6454
Date: 18 August 2016 E mail: info@rbf.gov.fj or
info@fijifu.gov.fj

FAKE FACEBOOK ACCOUNTS

The Financial Intelligence Unit (FIU) and the Reserve Bank of Fiji (RBF) would like to caution members of the public on recent cases of fake *Facebook* profiles, scam emails and bogus loans involving the Reserve Bank of Fiji.

Fake Facebook profiles

Cybercriminals have created several fake *Facebook* profiles of "Barry Whiteside", Governor of the RBF. The Governor does not have any *Facebook* profile under his name. Cases have been brought to the attention of the FIU and the RBF that these false personations were used to provide fake RBF approvals for victims to remit funds to secure proceeds of fake lotteries, investments and loans.

Governor Whiteside said that the RBF and its staff do not communicate with anyone via *Facebook* or other social media on official business matters. Governor Whiteside said that anyone who receives any communication or document purporting to be sent from him or any staff of the RBF must immediately refer it to the RBF and FIU for verification and further investigation.

Scam Emails

A number of incidents of scam emails have also surfaced claiming to be from Governor Whiteside with fake messages and documents. Members of the public and stakeholders of the RBF are advised to exercise extreme caution when they receive unsolicited emails or lookalike emails without the official RBF domain [@rbf.gov.fj](mailto:info@rbf.gov.fj).

Bogus Loans and Grants

The letterhead and logo of the RBF has been used by criminals on documents purporting to offer loans and grants to victims who began to correspond with the criminals using fake social media profiles and emails.



FijiFIU
Fiji Financial Intelligence Unit



Role of the FIU: Awareness

- ✓ Fiji FIU conducted background & credibility checks on the fake facebook profile of the Governor.
- ✓ Fiji FIU linked up with the relevant law enforcement officials.
- ✓ Fiji FIU issued a case dissemination report to the Fiji Police Force on 18 August 2016.
- ✓ Fiji FIU issued a joint press release with the Reserve Bank of Fiji on 18 August 2016.
- ✓ Disseminated widely to 6,000+ GOVNET users , 80+ AML compliance officers and their networks as well as to our partner law enforcement teams and their networks.



FijiFIU

Fiji Financial Intelligence Unit



ML PROSECUTIONS & CONVICTIONS



FijiFIU
Fiji Financial Intelligence Unit



Money Laundering Prosecutions and Convictions

Date of Conviction/ Judgement	Case Reference No.	Amount Involved	Sentence
14 April 2011	State vs Anand Kumar Prasad, Reenal Praneel Chandra, Reenal Rajneil Chandra, Deo Narayan Singh, Shirley Sangeeta Chand and Atishma Kirti Singh Criminal Case No: 024 of 2010	\$840,00.00	Convicted and sentenced by the High Court as follows: <ul style="list-style-type: none"> • Anand Kumar Prasad 6 years • Deo Narayan Singh 4 years • Atishma Kirti Singh 2 years
14 December 2011	State vs Monika Monita Arora Criminal Case No: HAC125 of 2007	\$472,466.47 (ML); & \$10,000 : Corrupt Practices	Convicted and sentenced by the High Court to 7 years imprisonment
16 March 2012	State vs Deepak Rajneel Kapoor and Krishneel Khanaiya Bhola Nath Criminal Appeal No. HAC 042/2009	\$111,894.54	Mr Deepak Rajneel Kapoor pleaded guilty and was sentenced by the High Court to 16 months imprisonment
11 April 2012	State vs Johnny Albert Stephen Criminal Case No: HAC 088 of 2010	\$38,861.46	Convicted and sentenced by the High Court to 7 years imprisonment
1 November 2012	State vs Doreen Singh; Criminal Case No. HAC 086 of 2009	\$157,423.94	Convicted and sentenced by the High Court to 6 years imprisonment.
November 2012	State vs Nirmala Devi	\$1,095.00	Convicted and sentenced by the Magistrates Court to 1 year imprisonment suspended for 2 years.
27 September 2012	State vs Kapil Kushant Samy Criminal Case No. 325/2012	\$11,398.67	Convicted and sentenced by the Magistrates Court to 3 year suspended imprisonment



FijiFIU

Fiji Financial Intelligence Unit



Money Laundering Prosecutions and Convictions

Date of Conviction/ Judgement	Case Reference No.	Amount Involved	Sentence
31 July 2014	Sate vs Manoj Khera (Mahakali Jewellers)	\$44,611.00	Convicted and Sentenced by the High Court to 4 years imprisonment
21 April 2015	State vs Vikash Prakash Mehta	\$356,707.36	Convicted and Sentenced by the High Court to 5.5 years imprisonment
19 October 2015	State vs Savita Singh	\$2,400.00	Convicted and Sentenced by the High Court to 5 years imprisonment
12 November 2015	State vs Chris Ronil Singh	\$47,734.58	Convicted and Sentenced by the High Court to 4 years imprisonment.
27 January 2016	State vs FIU Katarine Gounden	\$15,628.33	Convicted and Sentenced by the Magistrates Court to 4 years imprisonment.
15 March 2016	State vs Fazeel Rasid Ali	\$110,00.00 (Theft) out of which \$82,787.95 (ML)	Convicted and Sentenced by the Magistrates Court to 34 months (2 years 8 months) imprisonment.



FijiFIU

Fiji Financial Intelligence Unit



Money Laundering Prosecutions and Convictions

Date of Conviction/ Judgement	Case Reference No.	Amount Involved	Sentence
18 March 2016	State vs Josefa Saqanavere, Tuimoala Raogo & Savenaca Batibawa	\$638,902.26	Convicted and Sentenced by the High Court to 13 years imprisonment for each.
6 June 2016	State vs Mukeshwar Narayan Singh	\$102,843.50	Convicted and Sentenced by the High Court to 7 years imprisonment.
6 June 2016	State vs Sakiusa Vakarewa	\$117,111.00	Convicted and Sentenced by the High Court to 6 years imprisonment.
8 July 2016	State v Nitesh Kumar	\$9,888.67	Convicted and Sentenced by the Magistrates Court to 2 years imprisonment, suspended for 3 years



FijiFIU

Fiji Financial Intelligence Unit





THANK YOU