

Appendix A

DRAFT

INFORMATION MANAGEMENT PLAN

**Pacific
Region
Identity
Protection
Project
“PRIPP”**

April 2004

Forum Eyes Only

ABBREVIATIONS

Throughout this report the following abbreviations will be utilised:

| | |
|-----------------|--|
| AIPR | Australian Identity Protection Registers |
| FIU | Financial Intelligence Unit |
| IMP | Information Management Plan |
| PRIPP | Pacific Region Identity Protection Project |
| PTCCC | Pacific Transnational Crime Coordinating Centre |
| TCU | Transnational Crime Unit |
| The “Registers” | The PRIPP will be divided into five identity fraud specific registers with a sixth register - the Pacific Fraud Centre |
| NFD | National Fraud Desk (Australia) |
| The “Project” | refers to PRIPP |

ABSTRACT

This IMP details to participating agencies and jurisdictions the process of transferring identity fraud intelligence from participating organisations to the PRIPP. This plan also details how that intelligence will be managed from the collection phase through to dissemination.

This document should be read in conjunction with the PRIPP Memorandum of Understanding and other documentation relating to this project. This documentation has already been disseminated to jurisdictions and participating agencies.

The IMP specifically deals with four important sections of information and intelligence management, which will assist in the promotion of sharing and exchanging identity fraud intelligence between jurisdictions and agencies. The four areas cover:

- The role and objectives of the PRIPP, the data collection philosophy and types of information and intelligence sought for the “Registers” (Part A);
- The methodology for identity crime intelligence to be transferred from the relevant organisation to the PRIPP for publication on the SplexNet or web page, dissemination to participating agencies and other relevant issues (Part B); and
- An explanation of the search methodology to ensure accurate and timely retrieval to assist investigators and analysts to retrieve identity crime intelligence from the “Registers” (Part C); and

- General IMP provisions relating to access and training; data integrity and security; quality control; the “Registers” and PRIPP (Part D)

An electronic version of this IMP can be provided on request.

INTRODUCTION

The PRIPP is an initiative of the Pacific Islands Forum Secretariat under direction of the Forum Regional Security Committee (FRSC). The PRIPP promotes and facilitates the exchange of identity fraud and general fraud intelligence between jurisdictions, and agencies, and provides a central repository of fraud-related information.

The PRIPP facilitates the exchange of fraud intelligence via Splexnet or a web page and provides a dedicated fraud registers to support regional, and national, operational requirements. The Project Manager of the PRIPP at the PTCCC manages these functions.

The Australian authorities, through their counterpart mechanisms the National Fraud Desk (NFD) and the Australian Identity Protection Register (AIPR), have identified a significant shortfall in the intelligence process relating to fraudulent identities. Many Commonwealth Government Agencies and financial institutions are regularly experiencing losses caused by the use and creation of fraudulent identities which are generally produced to obtain a financial benefit or gain. Law enforcement agencies then attempt to investigate these offences and are hindered by a lack of coordination of this intelligence between the victim agencies and the jurisdictions.

Many of the victim organisations make an effort to maintain their own intelligence on fraudulent identities encountered by their agency, in an attempt to identify future claims for benefits or services by known fraudulent identities. In some cases, this intelligence is shared on a limited basis. The cost of identity fraud is a significant issue. It can be argued that identity fraud is a driving force for most fraud and is used to avoid detection and launder the proceeds of crime.

The PRIPP is seeking to provide law enforcement and participating agencies with a regional response, and to improve the intelligence holdings relating to, identity fraud specifically and fraud in general.

The PRIPP will be hosted on Splexnet or own web page. The “Registers” will record suspected fraudulent identities used to obtain a benefit from various organisations and details of victims of identity theft. Registers also contain information about lost/stolen documents of identity, images of authentic documents and the Pacific Fraud Centre.

This will assist investigators to reduce the surge in identity fraud by maintaining a central register of such information.

ABOUT THE IMP

This IMP documents the methodology for transferring identity fraud intelligence holdings onto the “Registers” located on Splenet or web page.

To assist with the management of identity fraud intelligence, the PRIPP has designed a template to submit the required intelligence for the register. This template is annexed to the concept paper and can be made available electronically on request from PRIPP. Agencies that do not have access to the Splenet or web page will be provided with their own electronic copy of the template for the electronic submission of intelligence.

Part A

- Outline the role and objectives of the PRIPP, the data collection philosophy and the nature and extent of information and intelligence required (Part A);

PRIPP the “Registers” - Role, Aims and Objectives

The role of the PRIPP is to:

Capture identity fraud intelligence relating to the use of fraudulent and stolen identities from law enforcement and government agencies. The PRIPP will centralise and facilitate the exchange of this intelligence on a regional basis between participating agencies and jurisdictions.

The objectives of the PRIPP are to:

- understand the extent of the impact of identity fraud on participating agencies;
- assist investigators to reduce the surge in identity fraud by maintaining a central register of fraudulent and stolen identities that will assist in early detection and prosecution;
- facilitate co-operation and co-ordinate the exchange of identity fraud intelligence between participating agencies in accordance with privacy legislation;
- utilise identity fraud intelligence as an impetus for investigations, recovery of losses due to fraud, identifying the proceeds of crime and intelligence analysis;

The purpose of the PRIPP “Registers” is to:

- a) assist in protecting genuine identities;
- b) assist investigators to reduce the incidence of identity fraud and theft; assist victims of identity fraud and theft; identify fraudulent and stolen identities;
- c) facilitate cooperation and coordinate the exchange of identity fraud information and intelligence between agencies for the purposes of law enforcement, protection of the public revenue and assist in forming relevant administrative decisions, and
- d) use identity fraud information and intelligence as an impetus for investigations, recovery of losses due to fraud, and intelligence analysis.

Data collection for the PRIPP

Suspected Fraudulent Identity Register/Victims of Identity Theft Register

The PRIPP has specifically designed a template for the submission of fraudulent and stolen identity details to the PRIPP. This template will be electronically provided to the participating agencies or for those agencies with Splixnet or web page access, the template can be made available electronically on request.

The same template will be used for fraudulent identities and victims of identity theft. This information will be differentiated from the fraudulent identity intelligence by selecting a drop down menu in the first box which allows the selection of "Fraudulent Identity Details" or "Stolen Identity Details". By selecting this drop down menu, the title in the first box on the template will automatically change to reflect your selection.

The PRIPP seeks the following types of intelligence and information from jurisdictions and participating agencies on the provided template:

- Name, address and date of birth of the fraudulent identity;
- Type of identity, for example is a name completely fictitious, partially fictitious or legitimate.
- Type of fraudulent document produced and any corresponding numbers on the document, for example, a Driver's Licence, number 12345678;
- Origin of document produced, for example a Driver's Licence that may be fraudulently manufactured or legitimately obtained through deception.
- The type of criminal offence committed or the type of benefit sought and value of that benefit;
- Details of the suspect (if known);
- A free text field to detail the circumstances in which the fraudulent document was produced or other matters of interest which may assist subsequent investigations or inquiries;
- The name, contact details and agency of the person submitting the template, to assist in any subsequent inquiries surrounding the fraudulent identity.

How to complete this template

Intelligence for the “Registers” will only be accepted on the template provided. The person completing the template should follow these basic instructions:

At the top of the template, the date of compiling the report (or date created) must be inserted. The month must be selected from a drop down field to ensure consistent reporting. Tab into the next field which requests the date the information was received by your organisation (if known) and if different from the date of completing the form. Then tab to the heading of “Fraudulent Identity Details” in the first text box.

Identity and Document Rating System

In the first text box the user must select the Identity and Document type from the drop down menu. This clearly indicates the type of identity and document being submitted.

Fraudulent/Stolen Identity Details

The user must select either “Fraudulent Identity” or “Stolen Identity” from the drop down menu located next to this title. This selection will determine the title of the second text box, which will automatically change after the selection is highlighted in the drop down menu. Then using the tab key, move the cursor to each data field in the first text box, typing in all of the required details. The fraudulent surname, given name and date of birth are mandatory fields. The field requesting the Country relating to the fraudulent address is a drop down menu. Simply select the relevant Country and it will automatically be inserted.

Then tab to the third text box which details the type and number of the fraudulent documents utilised to support the fraudulent name, or the type of documents used in the identity theft. The type of fraudulent document is a mandatory field.

If you are entering a victim of identity theft, then please enter the victim’s details in the text fields provided and ensure that the title at the top of this text box reflects the data you are submitting. If the person submitting the fraudulent identity has supplied a phone number, then these details are to be submitted in the specified phone number fields in the “Suspect’s Details” section of the template.

Fraudulent Document Type

The tab should now be on the document type next to number 1. Using the cursor, press on the arrow and a drop down menu will appear. Select the type of document in the drop down menu. The type of document will automatically be inserted into this field. The cursor should now appear in the “Country” field. In this

field, select the drop down menu and select the relevant country that applies to the type of document. For example, you can select a Driver's Licence as the fraudulent document type and then select "International" to submit a fraudulent International Driver's Licence to the "Registers".

The cursor should now be on the "Number" field that corresponds to the document type just entered. This is where the number associated with the document must be entered.

The cursor should now be on the Type of Date associated with the document. A drop down menu allows you to choose an Issue Date or an Expiry Date. Select the appropriate date type and then enter either the issue or expiry date of the fraudulent document (if known) into the date field. If the expiry date only has a month and year, such as a Medical Card which expires on 10/2007 then only enter the month and year.

The template can accommodate four fraudulent documents or types of identity used to takeover the identity of the individual. In the rare event that more than four fraudulent documents are known and associated with one fraudulent name, the additional details should be entered in the free text field under "Circumstances", located in the sixth text box.

Every different fraudulent identity, even though the difference may only be a slight spelling change of the name, requires its own template document.

Offence Details

After detailing the types of documents, tab down to the fourth text box. This is a free text field where you may enter the offence that has been committed. If a series of offences have been committed, then please enter the most serious offence. Then tab to the next fields, which allows you to enter the amount obtained or sought to be obtained and the date of the offence or the period of time in which the offences were committed.

Suspect's Details

If the submitting agency has a suspect for the fraudulent identity being submitted on this template, then please enter the suspect's details in the allocated fields. This text box is completed by following the same instructions as the "Fraudulent Identity Details" text box. The text field titled "Reference" allows the submitting agency to insert a criminal history number, or an investigation number, that may be relevant to the internal numbering of your agency.

Circumstances

The sixth text box allows the author to detail the circumstances of the fraudulent identity being produced. This may include a narrative such as, "*The offender*

produced the fraudulent documents to the XYZ Bank, in order to open a bank account to obtain a credit card and left phone number 123456. No other details are known as to the true identity of the offender”. The free text field allows you to enter as much detail as necessary and is designed to assist other agencies and investigators who may be investigating the same fraudulent names which have been produced in different circumstances.

Financial Transactions Reports Information

If any of the information contained in the template is derived from Financial Transactions Reports Information then the user must select “Yes” from the drop down box at the end of this question. This will indicate to the Collator/Analyst that the information is to be treated differently from general identity fraud information, due to the constraints imposed from the various Transactions Reports regimes in the region.

Contact Details

The final text box provides for the contact details of the person submitting the template. These details include the name of the agency, the Country, Town or Region (if applicable), the name of the person to contact and the contact phone number and e-mail. The contact name and agency name are mandatory fields.

Persons completing the template must be aware that these basic details will be added to the “Registers” and may be provided to other agencies participating in the project. Any person who does not wish for their details to be added to the register or provided to other agencies should not complete the template.

Definition of fraudulent identity

For the purposes of the PRIPP the definition of a ‘fraudulent identity’ is an identity that has had at least two of the following four identity characteristics fraudulently created:

- a) Given name(s)
- b) Surname or family name
- c) Date of birth
- d) Address

and

this identity must appear on a proof of identity type document irrespective of whether that document is fraudulently manufactured or legitimately issued.

The PRIPP will not accept simple aliases. Therefore a person applying for a benefit with the surname of CLARK instead of CLARKE will not be accepted as a fraudulent identity, unless another identity characteristic has been changed, such as the first name or date of birth, and the identity is supported by proof of identity

document. This indicates that the person has taken some affirmative action to try and remove themselves from their legitimate identity.

Similarly, the PRIPP will not accept details where a person has lawfully changed their name and uses the new name to commit fraud.

Deceased Persons

Often the identity of a deceased person is adopted for the purpose of assuming another identity to obtain some type of benefit. The PRIPP will accept the details of deceased persons where the name and date of birth of the deceased person has been transformed into fraudulent documents for the purposes of deceit. For example, the details of a deceased Cook Islander appearing on a newly issued New Zealand Birth Certificate.

The PRIPP will not accept details of deceased persons where relatives or associates of the deceased person have failed to notify an agency of the death of that person and continue to receive some type of benefit.

Caution when completing templates and submitting intelligence

Agencies submitting the intelligence must have made sufficient inquiries regarding the fraudulent identity to be satisfied on the balance of probabilities that the identity details are fraudulent and therefore of sufficient value to be added to the “Registers”. These inquiries may include confirming that a driver’s licence number does not exist, or the document produced does not have sufficient security features to satisfy the agency that it is a legitimate proof of identity document.

A suspected fraudulent identity should not be submitted until these inquiries have been conducted and the agency can justify its submission if required.

The parties to the MOU for the PRIPP “Registers” should acknowledge that any information provided is compiled from a variety of sources, which may not necessarily be reliable (particularly in relation to criminal intelligence). Accordingly, the parties do not warrant or represent that the information is free from errors or omissions. Whilst every care has been exercised in the provision of the information, neither party is liable to the other for any consequences arising from such errors or omissions, including any loss which may be incurred as a result of reliance on the accuracy or completeness of the information.

Privacy

The submitting agency must ensure that their submissions to the PRIPP are lawful. Agencies must be cognisant of legislation that may bind their organisation to share or not to share certain types of information and also adhere to and comply to relevant privacy legislation and principles.

Part B and C

- The methodology for identity crime intelligence to be transferred from the relevant organisation to the PRIPP for publication on the SplexNet or web page and dissemination back to participating agencies and other relevant issues (Part B);
- An explanation of the search methodology to ensure accurate and timely retrieval to assist investigators and analysts to retrieve identity crime intelligence from the “Registers” (Part C)

To streamline the process of submitting intelligence, the PRIPP has developed standard templates which can be obtained directly from PRIPP or the Liaison Agency in the participating jurisdiction. This e-mail must also be **carbon copied** to the nominated participating agency liaison officer. A list of the nominated liaison officers for each participating agency, and participating jurisdiction, and their contact details will be available once confirmed.

Agencies that do not have access to Splexnet or web page will be provided with an electronic copy of the template. The template is a Microsoft Word document and does not contain any macros.

If an agency experiences difficulty in e-mailing the templates to the PRIPP please contact your jurisdiction’s liaison officer or PRIPP through:

- Shaun Evans, PIFS Law Enforcement Adviser by email at shaune@forumsec.org.fj or by phone (+679) 3312 600

Once the intelligence is received, the PRIPP Collator/Analyst will upload the template details onto the “Registers”.

Consent

Victims of identity theft must complete a standard consent form before their information can be added to the “Registers”. This form (see Appendix A) can be made available electronically to participating agencies and jurisdictions.

The consent form must detail the corresponding police investigation number allocated to the investigation. Therefore, every victim of identity fraud must first report the matter to his or her local police station before being eligible to be added to the “Registers”.

The consent form seeks the person to acknowledge and accept that their identity details will be added to the “Registers” and will be disseminated to the agencies participating in the “Project”.

Transfer of mass data

PRIPP will liaise with the agency and jurisdiction concerned should the transfer of mass data be required.

Jeopardising investigations

The discretion lies with the submitting agency to decide the timing of submitting identity fraud intelligence. If a particularly fraudulent identity is subject to an investigation, and dissemination of that identity to participating agencies is likely to jeopardise an investigation, then the donating agency should consider this issue before submitting the intelligence to the “Registers”.

Similarly, the submitting agency should also recognise that by not disseminating the intelligence to the participating agencies, they may be reducing the opportunity of discovering duplicate identities and offences with other participating agencies and the possibility of obtaining further evidence.

This decision rests entirely with the submitting agency. The “Project” will disseminate all fraudulent identities received.

Dissemination of identity fraud intelligence

Access to the “Registers” will require at minimum user name and password. User names and passwords will be allocated once the PRIPP is operational.

Those agencies and jurisdictions that may not be able to have access to the “Registers” will periodically receive a CD-ROM. Each CD-ROM will contain an updated version of the data available on the “Registers”. This data can be interrogated and searched. The PRIPP recognises that on line access is desired by participating agencies but respects the fact that this may not be practical for some agencies and jurisdictions.

Actions of agencies regarding identity theft inquiries

The situation may arise in which a participating agency matches an identification document being produced by a customer to a stolen identity collected by the PRIPP. The action to be taken by the agency greatly depends on the circumstances. However, the PRIPP cautions agencies to take particular care and exhaust all available avenues of inquiry before taking any action with the person producing the identification document. Agencies must consider that the person producing the identification may be the victim of the identity takeover and not the offender.

Agencies act at their own risk having regard to civil liability and the PRIPP is not liable for any actions taken by the participating agency.

Summary of PRIPP Registers Intelligence Management

- The “Registers” will be located on a specifically designed area of Splexnet or web page;
- The PRIPP will collect all information and intelligence relating to fraudulent identities on a template (annexed to this IMP) which is to be completed by the submitting agency;
- The template is to be attached to an e-mail and forwarded to the PRIPP by email and carbon copying the e-mail to the nominated liaison person for that agency. The liaison person will then retain a hard copy (or file) of the template to assist with their reporting process.
- The Collator/Analyst at the PRIPP will upload the intelligence from the template onto the “Registers”. Collation, data entry and analysis will be coordinated by the PRIPP at the PTCCC.
- The PRIPP will promote the submission of intelligence and information through close liaison with law enforcement agencies and participating government agencies; and
- The PRIPP will report back to the contact person in each participating jurisdiction on the progress of the “Project” and will continue to promote and facilitate the exchange of identity and general fraud intelligence.

Part D

- General IMP provisions relating to access and training; data integrity and security; quality control of the “Registers” and PRIPP (Part D)

The following policy concerning caveats and security will apply:

- Information entered on the template and e-mailed over the Internet or over the secure network for submission to the “Registers” must be either classified as “In Confidence” or “Unclassified”. Participating agencies that do not have access to secure e-mail and need to submit intelligence at this level will have to forward the templates on floppy disc. The PRIPP does not anticipate receiving intelligence for the purposes of the register which exceeds these classifications. Caveats should not be placed on documents relating to the “Registers”.
- Information submitted by the jurisdiction/agency remains the property of the submitting organisation
- All information submitted to the PRIPP will be securely and confidentially handled.

Data Integrity

Data integrity is imperative. Forms are to be completed by the submitting person in the jurisdiction/agency in a comprehensive manner ensuring that all data fields are accurately completed.

Quality Control

Documents submitted for the PRIPP will be subject to quality control checks by the Collator/Analyst managing the data.

If a quality control issue is identified, then the Collator/Analyst will contact the submitting agency highlighting the deficiency and return the template for amendment before resubmission.

Complaints

Any complaints about actions of officers of the PRIPP may be investigated by the most appropriate authority.

In addressing complaints, the PRIPP shall work in accordance with its internal procedures for dealing with complaints and consult where necessary with the relevant authorities.

PRIPP and PFC Services and Support

The PRIPP will provide support to participating agencies and jurisdictions for the “Project”. Initially all inquiries should be forwarded to:

- Shaun Evans, PIFS Law Enforcement Adviser by email at shaune@forumsec.org.fj or by phone (+679) 3312 600

Appendix A

Pacific Region Identity Protection Project

Consent form for victims of identity theft

I of
.....

(full name) (full address)
have reported my identity being stolen to the (Country) Police
located at (full address). The
corresponding police report number is (official police report number).

I hereby consent to adding my personal details to the Victims of Identity Theft Register, (a component of the Pacific Region Identity Protection Project) being operated by the "Project" and by consenting acknowledge the following:

- that my name, address, date of birth, identity document type(s) and corresponding number(s), and the circumstances surrounding the theft of my identity will be added to the "Registers";
- that this personal information will be shared and accessed by all participating agencies which fall into the categories of all Pacific law enforcement agencies, foreign law enforcement agencies, government departments and agencies and statutory authorities;
- that the purpose of sharing my information with these agencies is to prevent my identity being used to commit offences and attempt to apprehend the offender(s);
- that I may experience some inconvenience when dealing with these agencies as they may have to take extra steps to verify my identity to ensure they are not dealing with the offender(s) who have stolen my identity;
- that my information cannot be used for any other purpose beyond the investigation of the theft of my identity;
- that I may have my details corrected or removed from the "Registers" by writing to Project Manager PRIPP.

.....
(signature) (date)
WITNESS:
(Police Officer taking the report)

.....
(signature) (date) (print witness name)
Completed forms are to be faxed to Pacific Region Identity Protection Project.