The Egmont Group
of Financial Intelligence Units

Egmont Cases

Financial Analysis Cases 2011 - 2013

The Egmont Group has made every reasonable effort to ensure that the information in this publication is accurate. The information is provided on the basis that all persons accessing it undertake responsibility for assessing its relevance, usefulness, and accuracy. The information does not constitute legal, professional or commercial advice. Anyone contemplating reliance on the information contained in this publication should seek independent or appropriate professional advice prior to doing so. The Egmont Group does not guarantee, and accepts no legal liability or responsibility in this publication to any loss or damage suffered arising from, or in connection with, the accuracy, currency, completeness or usefulness of the information in this document.

This publication is copyright. No part of this publication may be reproduced by any process without prior written permission from the Egmont Group Secretariat. Applications for permission to reproduce all of part of this publication should be made to:

The Egmont Group Secretariat
Suite 910, 2200 Yonge Street
Toronto, Ontario M4S 2C6
CANADA
Tel: + 1-416-355-5670
Fax: + 1-416-929-0619
E-mail: mail@egmontsecretariat.org
Website: www.egmontgroup.org

Copyright © 2014 by the Egmont Group

The Egmont Group of Financial Intelligence Units

Map of contributing Egmont Group Financial Intelligence Units

Egmont Cases

Financial Analysis Cases 2011 - 2013

Preface

This is a very timely book. Money laundering and terrorist financing are hidden crimes and only concrete examples how proceeds of serious crimes are laundered and how terrorists fund their operations, will shed light on these activities. This book will serve to better understand how money laundering and terrorist financing works and what the role of FIUs is to prevent and combat these forms of crime.

The objective of the Training Working Group (TWG) is to provide a forum for Egmont Group Financial Intelligence Units (FIUs), and International Organisations, to increase the effectiveness of its members and other FIUs by offering opportunities to enhance skills, knowledge and expertise through broad based training initiatives. An important instrument to achieve this goal is the Best Egmont Case Award (BECA) held annually as part of the Egmont Plenary programme. In the last years, a large number of contributions have been received. I am very grateful for my Vice-Chair, Mr Phil Hunkin, and his team to analyse all contributions, select the most relevant ones and compile them in this publication. This book is hoped to contribute to making anti-money laundering and combatting terrorist financing a functioning, effective and valuable tool.

January 2015
Daniel Thelesklaf
Chair Training Working Group

Contents

Introduction

The Best Egmont Case Award (BECA) is an initiative of the Egmont Group of Financial Intelligence Units (FIUs). The Awards have been developed and championed by the Training Working Group (TWG).

The TWG identifies training needs and opportunities for FIUs and their personnel and conducts training seminars for Egmont members as well as for non-Egmont members' jurisdictions.

In 1999, the Egmont TWG undertook an initiative to draw together a compilation of sanitised cases which describe the fight against money laundering, undertaken by Egmont Group member FIUs. The compilation was to reflect in part the Egmont Group's fifth anniversary in 2000. The publication was entitled 'FIU's in action 100 sanitised cases'. This publication has provided invaluable assistance in identifying the components of money laundering cases. In addition to this publication the TWG created a database of sanitised cases that was available to FIUs through the Egmont Secure Web (ESW). Until 2012 this database was regularly updated with new sanitised cases.

Some ten years after the original 100 cases were published, the TWG identified that there was a need to try to develop and improve this concept. The TWG canvassed the opinions of colleagues to identify what improvements could be achieved. A key finding from this research was a desire from FIUs to be able to learn from and see "real life" examples of unsanitized cases that had already been successfully prosecuted and were publically reported. The benefit of this would be for analysts and investigators to learn from positive outcomes already achieved. The TWG believed that this would complement the existing sanitised cases and enhance the material through the increased relevance of the case examples. The challenge now facing the TWG was how to identify suitable cases.

During the working group meeting in Mauritius in 2010 the concept of a competition of the best money laundering cases was originally discussed. The initial idea was first tabled by FINTRAC and was further developed by the TWG at the Colombia Plenary. By the time the Working Group met in Moldova, a concept had been agreed and the first competition was launched in 2011. The competition would be judged at the plenary meeting in Yerevan, Armenia in July 2011. The Vice Chair of the TWG, Phil Hunkin of FIS Guernsey, accepted the role of BECA champion.

The concept of the competition was to provide the plenary with a more relaxed focus after a long working week, with a competitive edge! A panel of five judges would determine the best two cases, which would be marked against a set of criteria. The finalist FIUs would

then be invited to present their case to the plenary in no more than 12 minutes. The Heads of FIU would be asked to vote for the case that they considered to be the "best case" and the winners would be awarded the BECA trophy in addition to receiving a replica award for display within their own FIU. The winning FIU would receive international recognition of a job done particularly well and all the kudos that would follow.

The outcome for the TWG was to have several cases that they could use for the benefit of FIUs and the wider AML/CTF community.

In February 2011, immediately after the Aruba Working Group meetings, the first call letter for the BECAs was sent to all Egmont FIUs. The letter called for both sanitised and unsanitised cases with an emphasis on presenting unsanitised cases that had been through the court process.

There was a fantastic response to the call letter and a total of 47 cases were submitted in the first competition. At this stage, I would like to take an opportunity to thank the judges for their time and efforts in judging the first four BECA competitions.

2011 BECA panel of judges:

Sasha Behari	MOT (FIU-Aruba)
René Bruelhart	EFFI (FIU-Liechtenstein)
Mark Hammond	Egmont Secretariat
Phil Hunkin	FIS (FIU-Guernsey)
Nischal Mewalal	FIC (FIU-South Africa)

2012 BECA panel of judges:

Sasha Behari	MOT (FIU-Aruba)
Henry Komansky	FIA (FIU-Bermuda)
Phil Hunkin	FIS (FIU-Guernsey)
Phuttipong Chantrawadee	AMLO (FIU-Thailand)
Nischal Mewalall	FIC (FIU-South Africa)
Daniel Thelesklaf	EFFI (FIU-Liechtenstein)

2013 BECA panel of Judges:

Fuad Aliyev	FMS (FIU-Azerbaijan)
Henry Komansky	FIA (FIU-Bermuda)
Olivier Lenert	FIU-LUX (FIU-Luxembourg)
Alejandra Medina	(FIU-Mexico)
Phuttipong Chantrawadee	AMLO (FIU-Thailand)

2014 BECA panel of Judges:

Sasha Behari	MOT (FIU-Aruba)
Sinclair White	FIA (FIU-Bermuda)
Amar Salihodzic	EFFI (FIU-Liechtenstein)
Nischal Mewalall	FIC (FIU-South Africa)
Stefan Lundberg	NFIS (FIU-Sweden)

There were a number of excellent cases submitted, the judging panel had a difficult task and ultimately could not separate the best three cases submitted by Fiji, Finland, and the Turks and Caicos Islands. As a consequence all three jurisdictions were invited to present at the Armenian Plenary. After a very close vote, the Finnish FIU was judged to be the inaugural winners of the BECA.

RAP - Finland receiving the BECA plaque from Mr Boudewijn Verhelst, Chair of the Egmont Group in Yerevan, Armenia 2011.

A review of the competition and its benefits was conducted at the Manila plenary meeting in January 2012 and it was concluded that the first competition was a success. The TWG decided that the competition would continue. In an attempt to develop the quality of the cases and to ensure that the submissions followed a structured format, new criteria were devised and included in the 2012 call letter.

18 cases in total were submitted for the 2012 BECA and our analysis identified that the new criteria had resulted in a better quality of case submission. The two winning entries were AMLC Philippines and Rosfinmonitoring Russia. The cases were presented at the St. Petersburg Plenary and again after a very close vote, Russia were crowned champions of BECA 2012.

In 2013, the TWG again reviewed the BECA and concluded that it was successful, beneficial and should continue. The BECA champion identified that we would need to identify how we could share the cases with the wider AML/CFT community. With the help of the Egmont Group Secretariat, all of the cases submitted in the two previous competitions were made available to all Egmont FIUs via the ESW. It was decided that a publication would be the most effective way to highlight the best of

Mr. Chikhanchin Head of FIU Rosfinmonitoring Russia takes the honours at the Plenary in St. Petersburg

the BECAs, the aim was to have as many of the cases as possible in an unsanitised format. Factual information would provide the greatest clarity for applicability to the wider AML/ CFT community.

Another solid entry of eighteen cases was submitted in 2013, they were judged in the same manner and the two winners were a joint submission from Nigeria and South Africa, and Colombia. The Sun City plenary enjoyed two fantastic presentations and the Heads of FIUs voted the Colombian case as the winner of the 2013 BECA.

In April 2014, thirteen cases were received from 12 of the 139 member FIUs. The two winners were a joint submission from Mexico and the United States and a case from Australia. Both contenders provided very strong presentations at the 2014 Egmont Group Plenary in Lima, Peru and the Heads of FIUs voted the joint case from Mexico and the United States as the winner of the 2014 BECA.

It was agreed at the working group meetings in Budapest in 2014 that as testament to the success of the BECA competition, the TWG would compile this publication.

I hope you enjoy reading these excellent case examples and benefit from the experience and impressive cases investigated by the contributing jurisdictions.

Acknowledgements

I would like to take this opportunity to acknowledge the work and effort undertaken in the publishing of the BECA book by the following people:

Michelle Watson (Consultant) and Kelly Woosley (FIS – Guernsey) who have worked together, on opposite sides of the world, to bring this professional publication together, within a very short time frame.

The TWG project team who have contributed and driven the publication of the book; Amar Salihodzic EFFI (FIU-Liechtenstein), Stefan Lundberg (NFIS –Sweden), Stacey Clermont (Egmont Secretariat), Sasha Behari MOT (FIU-Aruba), Alejandra Fabiola Medina Carrillo and Guillermo Alejandro Hernandez Rodriguez (FIU-Mexico) and Evgeny Volovik (Rosfinmonitoring Russia).

Liechtenstein (EFFI) FIU for providing the financial support that allowed for the compilation of the document and the availability of printed copies for Egmont members.

The Egmont Group Secretariat for their ongoing support and advice.

FinCEN for their creative input in preparing this book for publication.

All BECA entrants and the contributing countries.

Phil Hunkin – Head of FIU Guernsey and BECA Champion

The role of financial analysis in the BECAs

The evolution of analysis

Financial analysis plays an important role in the BECA cases, and the Egmont Training Working Group (TWG) was keen to determine how analysis has evolved since the inception of the BECAs in 2011. It is acknowledged that it will always be difficult to assess the cases for this purpose, given that they were written with a unique aim in mind, that is, as an entry for the BECA awards.

This publication comprises of twenty two cases which have been included to provide examples of a financial investigation and the analytical processes demonstrated by the various FIUs in their work.

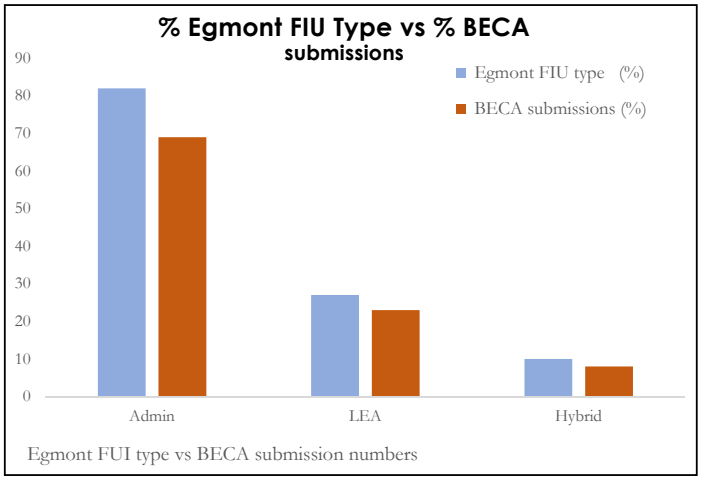
A key objective of this publication is to produce a valuable reference for our FIUs, enabling the financial crime prevention community the opportunity to share and learn from experience. The following cases show how investigations were initiated and progressed through to successful money laundering cases. They demonstrate how FIUs developed their investigation from available information to produce an intelligence product and valuable evidence to support a prosecution.

Analytical knowledge

In trying to determine the role of financial analysis, it was necessary to assess the evidence of analytical knowledge and understanding as well the range of different analysis types used wherever possible. The cases selected showed elements of planning and tasking, the collection, collation and evaluation of information as well as structured analysis, well presented findings and appropriate dissemination.

Emphasis was placed on the analytic argument and the development of analytic conclusions. In many cases there was clear progression from the development of initial premises which were progressed to inferences, before drawing well supported conclusions. Analysis types were classified as either comparative, dynamic, environmental, cross matching or time related. It should be noted that judgment of the analysis itself was outside of the scope of this project.

Submission numbers



Egmont FUI type vs BECA submission numbers

Over the past 3 years the majority of BECA submissions were received from Administrative FIUs. There are just 27 Law Enforcement and 10 Hybrid style FIUs compared with the 82 FIUs that operate as an administrative organisation. Given that the majority (69 %) of Egmont FIUs are administrative, it is not surprising that they have submitted a higher percentage (82%) of the total number of cases. Law Enforcement FIUs represent 23% of Egmont members although contributed just 12% of the BECA cases with the remaining 8% of hybrid FIUs who contributed 6% of cases. These results show that Law Enforcement FIUs are underrepresented in the BECAs and further work is needed to understand why.

Quality of analysis vs. High Development Index

The majority of member FIUs are situated within countries classified as having a High Development Index (HDI) score. The HDI is a statistic compiled from various sources of data including life expectancy, education, and income indices, to rank countries into four tiers of human development. These tiers have been used to categorise both the participation and quality of analysis undertaken in an attempt to determine whether changes are better understood against the backdrop of social factors.

Countries with a medium HDI have shown the most significant increase in the use of analysis despite being represented by a lower number of FIUs. Submissions from countries with a very high and high HDI show a consistent, to decreasing trend in demonstrating analysis within submissions entered. These patterns may reflect the training and experience of the developed very high and high HDI countries where existing analytical practises are more likely to be already in place. The apparent increase in analytic capabilities demonstrated by medium HDI countries could be considered to reflect the support and training extended to this demographic.

Conclusion

In conclusion, from the cases submitted in the BECA competition have been useful in determining a crude baseline assessment of the role financial analysis plays within an FIU. The opportunity to share such valuable information between FIUs could also be used to capture a more definitive measure of excellent analysis undertaken by the member FIUs.

While there is not a definitive set of products that can be used to conduct financial analysis, it is important to fully understand the process, the analytical products used and the reasons why. This will provide a greater measure of accuracy for determining analytical acumen, well founded judgments and strong lines of analytical argument.

Revealing the inner workings of the analysis undertaken within the Egmont community will serve to help identify not only the cases which have been deemed to be good examples of financial analysis but will also demonstrate the 'how' and 'why'.

Bribery and Corruption

Bribery and Corruption is endemic in a great number of countries and has a significant impact on the economic and social welfare of a country. Corruption undermines the democratic institutions, reduces economic development and contributes to government instability. It also erodes the social fabric of society as it undermines people's trust in the political system, in its institutions and its leadership.

Corruption is generally considered to be the abuse of power for private gain. It can occur at all levels and is usually facilitated by the provision of services or the payment of a bribe. Grand corruption consists of acts committed at a high level of government that distort policies or the central functioning of the state, enabling leaders to benefit at the expense of the public good. Petty corruption occurs at a smaller scale and takes place when low- to mid-level public officials interact directly with the public who are often trying to access basic goods or services in places like hospitals, schools, police departments and other agencies.[1] Petty corruption has also been called 'survival corruption' as it is particularly common in countries where public servants are grossly underpaid.

Although petty corruption involves relatively small amounts of money it hurts the poorest members of society who cannot afford to pay the bribes.[2] Grand corruption however has a significant impact on a society.

Grand corruption is usually undertaken by senior members of government who use public assets to invest in projects that benefit themselves rather than the community at large or accept bribes for personal gain. Bribes are often paid by the private sector in order to win a contract. These bribes can be significant in amounts and often come from foreign companies and investors. These corrupt officials need to establish arrangements to receive bribes without attracting undo attention. They are often linked to methods that have been established to launder the proceeds.

The most common methods used to launder the proceeds of corruption include the use of corporate vehicles and trusts, gate keepers, domestic financial institutions, offshore/foreign jurisdictions, use of nominees such as trusted associates and family members, and the use of cash. The money is then used to support a lavish life style and purchase assets. Such assets may include monies in bank accounts, real estate, vehicles, arts and artifacts, and precious metals.

1. Transparency International FAQs on Corruption http://www.transparency.org/whoweare/organisation/faqs_on_corruption/2
2. Regional Anti-Corruption Initiative http://www.rai-see.org/

Chapter 5 of the United Nations Convention against Corruption (UNCAC) 2003 states clearly that asset recovery is an international priority in the fight against corruption. It provides a framework for the return of stolen assets that requires countries to take measures to restrain, seize, confiscate and return the proceeds of corruption.[3]

The FIU plays a vital role within this process as demonstrated in the following two cases. The first describes a significant case where a senior official was obtaining public assets through corrupt practices to fund terrorist activity. The second case is an example of how the FIU was able to work the judicial system to trace financial flows and determine the links between people and assets. Both cases, are waiting on the completion of court proceedings and have therefore needed to be sanitized.

Indicators

- Abnormal or large cash payments
- Large cash withdrawals
- Purchase of high value items with cash
- Pressure exerted for payments to be made urgently or ahead of schedule
- Payments being made through a third party country - for example; goods or services supplied to country 'A' but payment made, usually to a shell company in country 'B'
- Abnormally high commission percentage being paid to a particular agency. This may be split into two accounts for the same agent, often in different jurisdictions
- An employee of a financial institution who never takes time off even if ill, on holiday, and insists on dealing with specific customers themselves
- Invoices being agreed in excess of the contract without reasonable cause
- Payment of, or making funds available for, high value expenses or school fees (or similar) on behalf of others
- Use of offshore companies
- Politically Exposed Person

3. Asset Recovery Handbook – A Guide for Practitioners 2011 The International Bank for Reconstruction and Development https://www.unodc.org/documents/corruption/Publications/StAR/StAR_Publication_-_Asset_Recovery_Handbook.pdf

1. Corruption, Money Laundering, and Terrorist Resourcing in the Middle East (FID, Bahrain)

Introduction

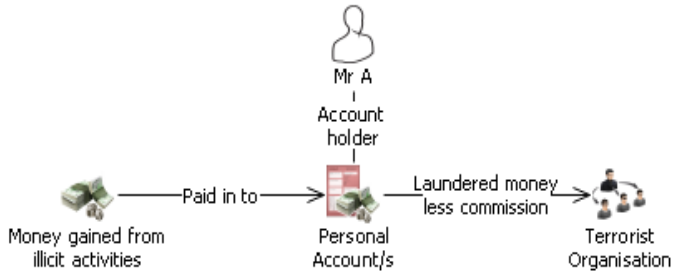
This case study concerns a high profile Bahraini Publicly Exposed Person 'A' and a female business associate who, along with one other person, are awaiting trial in Bahrain , and one other Middle Eastern country.

A Suspicious Transaction Report (STR) triggered initial investigation into the case which commenced three years ago when information was received by the FIU from a local bank. The Anti- Economic Crime Directorate noticed a variety of suspicious activities and began to closely monitor person 'A's accounts, meetings with businesses, associates and communications with various people in different countries.

The Investigation

In early 2008, the Financial Intelligence Unit (FIU) received information concerning 'A'. The information clearly indicated that 'A' was abusing his public position and violating his duty in the political community through improper means. There was a clear indication that he was involved in bribery locally, corruption and carrying out money laundering operations to hide the nature of those illegal activities. Additionally, the money laundering operations were being performed to aid terrorist organisations which were using new channels to launder money following international sanctions on their assets.

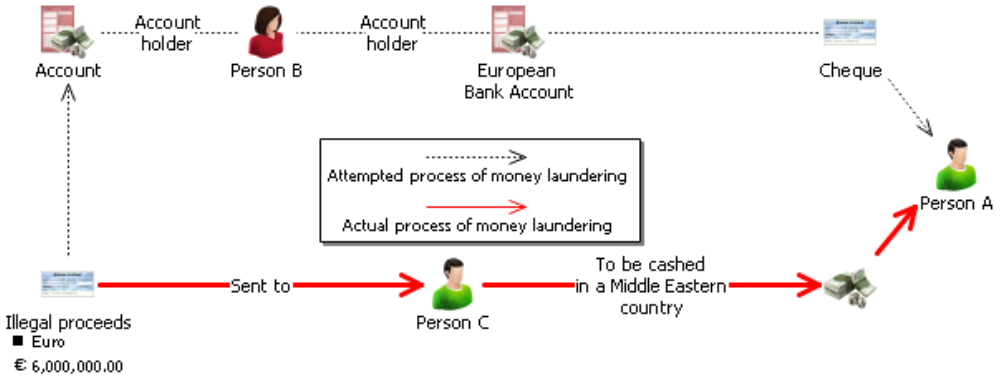
The Anti- Economic Crime Directorate's investigation substantiated that 'A' had local and international associations and affiliations with terrorist organisations. It was established that dirty money would be deposited into his personal accounts, he would take his commission and then transfer it on to a terrorist organisation.



The case was referred to the Public Prosecution Department for the authority to investigate 'A''s bank accounts and also those of family members. Authority was also given to monitor telephone conversations involving all suspects.

The investigation indicated, via taped telephone conversations that 'A' had agreed with a Middle Eastern female 'B' a deal where she would cash a European Bank cheque and transfer monies to 'A' in the value of EUR 6,000,000. It was suspected this had been gained from illegal activities.

When 'B' was unable to cash the cheque in Bahrain, 'A' enlisted the help of one of his employees 'C' and told him to cash it in a Middle Eastern country.



Throughout, 'A' utilized the help of many associates in order to ease and simplify the money laundering activities by assigning them to find other people who were trying to launder their illegal money.

Determined to take a strong stance, the Bahrain FIU sent a qualified team of investigators to a Middle Eastern country to collect substantial information and evidence concerning 'B' and to retrieve any other information that might be relevant to the case.

'A' was subsequently arrested and his house and office were searched. Suspicious evidence was found which indicated that 'A' was involved in money laundering activities. Among the evidence found in his possession were contacts of people connected to terrorist organisations and numerous cheques. Using modern technology, 'A''s mobile phone usage was analyzed further, which further confirmed his contact with known terrorist organisations.

The case was transferred to Public Prosecution however 'A' denied all the charges against him and rejected any link or knowledge of the cheque worth EUR€ 6,000,000 and the alleged accomplices. 'B' claimed that she was interested in starting a business in Bahrain with the help of 'A'. Further, she denied having or playing any role in the money laundering scheme or having prior knowledge about the EUR 6,000,000 cheque.

FIU Action

1) Ask permission from the Public Prosecution to reserve and expose the entire moveable and non-moveable, local and international properties that belong to 'A' and his family members. This was of high importance because it established that there were connections in their bank accounts and movement of money between them.

2) In pursuance of the Public Prosecution Order, we obtained 'A''s and his family members', bank statements which corroborated earlier suspicions.

Evolution of the case

The case took a year to investigate before the arrest of any suspects. Methods adopted included gathering, collating and analysing information received from Interpol, General Directorate of Traffic, Customs, Ministry of Industry and Commerce, Central Bank of Bahrain and other governmental organisations as well as through other international organisations, such as the Egmont Group.

1. Financial analysis enabled the investigators to establish that there was a vast amount of money, from an unknown source, in 'A''s private account.
2. Funds were moved between 'A''s family members and his own bank accounts, there were also links between 'A''s corporate accounts and his own private accounts.
3. There was no correlation between the money moving between A's bank accounts and his corporate earnings. This indicated that A's money was from an unknown source.

Indicators relevant to this case

- Large cash transactions were a regular occurrence: - all transactions were done either by cash or cheques. In some months, there were one hundred transactions while in others there were very few. The company accounts were recording financial input but there had been no company business generated. There was no logical movement of funds between company, family and personal bank accounts.
- Large and rapid movement of funds: the total number of the deposits into 'A''s private account was 458, but the total number of withdrawals was 4,563. The money deposited into 'A''s bank accounts was from an unknown source. Additionally, large amounts of money were being transferred to other countries.
- Unrealistic wealth compared to Client Profile 'A''s income, clearly exceeded his earning potential from genuine companies.
- The creation of shell companies to cover the source of various monies. The companies did not have any significant assets or operations. The majority of the companies have been created with the same address.
- 'A''s companies were issued without having any significant assets or operation procedures to his bank accounts, his family members or by his companies' bank accounts.
- Some companies had not declared their owner to the Ministry of Industry and Commerce. At the same time these companies had bank accounts which were personally managed by 'A'.

Collectively, the above indicators raised suspicions that 'A' had abused his position and intended to hide the funds using various money laundering activities.

Outcome

After his arrest, 'A' continued to deny all allegations in interview despite the additional evidence obtained as a result of searches undertaken at his home address and work premises.

The case was transferred to the Public Prosecutor's office and 'A' now awaits trial having been charged with offences relating to money laundering, bribery and corruption. Since 'A''s arrest and pending completion of court proceedings, his assets remain frozen.

The case has yet to complete the judicial process.

2. Money Laundering, Corruption and the importance of international exchange (UIF, Argentina)

Introduction

This case was selected as it constituted and still constitutes an enormous challenge for our Unit, considering the level of complexity of the schemes involved, the various instruments used and the facts related to the perpetration of corruption crimes with the participation of Politically Exposed Persons (PEPs).

The assistance provided by counterpart Financial Intelligence Units (FIUs) who are members of the Egmont Group, allowed UIF-Argentina (UIF) to indentify shell structures used for money laundering schemes.

This case describes how a PEP was able to enjoy the proceeds of corruption through the purchase of property using a complex network of shell companies spanning multiple jurisdictions, including countries with zero or low tax rates also known as Tax Havens. Large financial institutions and legal gatekeepers were used to give the appearance of legitimacy and credibility.

Since this case is currently in the judicial system and no final judgment has been rendered, it has been necessary to sanitise the case.

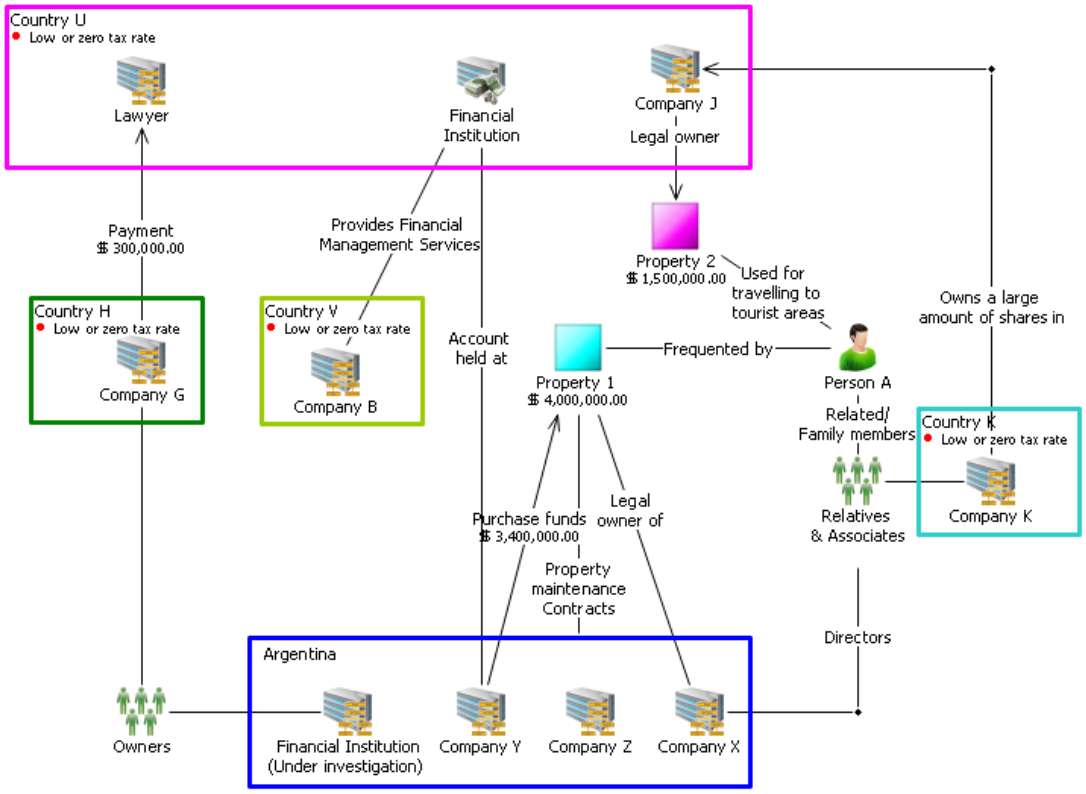
Development of the Case

It was brought to the attention of the Argentinian courts that a PEP was enjoying a questionable lifestyle and one beyond their expected financial means. Searches of Argentinian property registries conducted by the Courts revealed that properties used by the subject (Person T), were in fact, owned by other individuals.

At the same time, UIF-Argentina received a voluntary disclosure from a foreign FIU in Country (R). The disclosure stated that in a media release, a link had been established between Person (A) and the directors of Company (A) which was registered in that foreign country. It stated that Company (A) owned one of the properties (Property AV) enjoyed by Person (T).

As a result, UIF-Argentina conducted an in-depth analysis of the partners of Company (A) to find that the two partners, Person (J) and (E) were close relatives of an associate (Person M) of Person (T).

As a result of this information, the court requested UIF-Argentina to conduct a more detailed analysis and it was discovered that there were three properties enjoyed by Person (T) but owned by persons other than this person.



Property AV

UIF-Argentina focused on establishing a connection between Person (T) and the companies that were created for the purpose of purchasing this property. It was found that payments for the purchase of the property were made via a significant financial institution (F) from a foreign country (U).

An information request was sent to Country (F) requesting details of the transactions that were conducted as payment for Property (AV). The information revealed that the property

was purchased by Company (A). The names of the directors were also provided. Funds for the purchase were provided as a loan from Company (B), a company established in a country (V) known as a Tax Haven. The loan was for the sum of USD$ 3,400,000.00 which represented 85% of the value of the property. The remaining USD$ 600,000.00 was paid in cash. It was also found that the financial institution (F) in Country U managed the financial affairs of Company (B).

Additionally, services necessary for using and maintaining Property (AV), were contracted by companies (Y) and (Z). Companies (Y) and (Z) were incorporated in Argentina and were linked to Person (J) who was a relative of an associate (Person M) of Person (A). Foreign information requests were sent to 10 FIUs requesting information on all of the above persons.

The information provided by one of the foreign FIUs allowed UIF-Argentina to establish that one of the relatives of Person (T)'s associate transferred USD 300,000 to the bank account of a law firm located in Country (U). The money was transferred from the account of Company (G), which was also located in a country known to be a tax haven. It was assumed that this was part payment for purchasing Property (AV).

The law firm used for this transaction is internationally renowned for actively participating in money laundering schemes on behalf of foreign PEPs.

The foreign FIU was also able to confirm that the directors of Company (G) were also the owners of a significant financial institution located in the Argentine Republic. The investigation is still ongoing to determine whether this financial institution was involved in any payment for Property (AV). The owners of this financial institution are also under investigation.

Property YT

Information provided by the relevant government agency showed that a politically exposed person and his close friends and associates travelled to tourist spots using Property (YT). Investigation showed that this property was purchased for the sum of USD 1,500,000 by Company (J), which was a company established in a country known as a tax haven. A large amount of shares in the company were owned by Company (K), which was established in third country also known as a tax haven. Information provided by a foreign FIU established a link between Company (J) and Company (K). Company (K) was controlled by a close associate of Person (T).

Property DT

In the beginning of 2012, a reporting entity reported to UIF, the purchase of Property (DT) in cash for the sum of USD 450,000 in year 2009. The purchaser was Company (X), who justified the origin of the funds through a loan for consumption. This loan was never verified.

Intelligence tasks performed revealed that Person (T) enjoyed the use of this property. UIF conducted a comprehensive analysis. Information gained from the Legal Persons Registry indicated that Company (X) was incorporated during the first 2009 quarter by two individuals. On further investigation, UIF established that these individuals were without sufficient means to afford such a property.

Shortly before purchasing the property, these individuals transferred the block of shares to another two individuals who were closely related to Person (T).

In addition, further information requested from other reporting parties revealed that Company (X) appeared to have no legitimate function given that it was not registered with the Federal Administration of Public Revenue, had not filed any tax returns, does not hold any bank accounts and has not made any foreign exchange transactions.

Conclusion

The analysis of this case was made possible due to information provided by Egmont member FIUs. This information allowed for the identification of shell companies as well as linkages between individuals.

At the time of publication, the financial institution that was used to undertake financial transactions remains under investigation.

Indicators relevant to this case

- Company owned by individuals with insufficient financial means
- Property owned by person who is not the occupant
- Purchase of property with cash
- Companies established in offshore jurisdictions
- Companies established in jurisdictions known to be tax havens
- Company with no legitimate function (Shell company)
- Politically Exposed Person (PEP)
- Utilization of law firm with known history of money laundering

3. Corruption in the Civil Service (PPATK, Indonesia)

Gayus Tambunan (GT) (Tambunan), was a tax officer at the ministry of finance and was in charge of tax objections and appeals.

Analysis conducted by the Indonesia Financial Transaction Reports and Analysis Centre (INTRAC) revealed that Tambunan's wealth did not match his economic profile as a civil servant. INTRAC developed their analysis by asking for additional information from the reporting parties. Based on the information received, INTRAC established that Tambunan had received funds from various entities; corporations, tax consultants as well as other third parties. INTRAC identified from the intelligence that Tambunan's transactions may be related to bribery and corruption.

INTRAC's analysis also revealed that Tambunan had received 'SAT' Corporation's tax appeal in spite of the existing regulations in place. State losses were estimated to be USD 53,000. In addition, Tambunan also received money from the 'MT' and 'MJ' Corporations which totaled USD 41,000 in tax payments. However, instead of the money being returned to the State Treasury, Tambunan deposited the money into his own account, along with money received from individual tax consultants.

Tambunan concealed the proceeds of his crime by purchasing high value goods including two cars, precious metals, shares as well as real estate. Money was also withdrawn in cash, deposited in a cash deposit box and transferred to legal entities as well as to people in his close personal network. INTRAC's collaboration with international Law Enforcement Agencies (LEA) led to the discovery of money held within the safe deposit box.

INTRAC joined an informal inter-departmental task force consisting of the Indonesia National Police, Tax Office and State Audit Agency to investigate the case. The joint investigation concluded that Tambunan should also be charged with bribing various LEA officials, identity theft and forgery in addition to corruption and embezzlement.

In August 2009, while the case was under investigation by the Police, Tambunan bribed 'AE', an assistant Police Superintendent who accepted USD 6,600 in bribes along with a Harley Davidson motorbike which was gifted by an associate of 'GT'. He also paid USD 110,000 to 'AK' to admit that the money was his.

The investigation established that the public prosecutor 'CS' was also under the influence of Tambunan. 'CS' manipulated Tambunan' prosecution plan from a 1 year prison sentence to a 1 year trial in return for payment. On January 13, 2010, Tambunan's case was presented to the District Court. The judge, 'MA', chaired the panel of judges and was also under the influence of Tambunan. It was evidenced that on March 9, 2010, they met at 'MA''s official

residence. Tambunan proposed to gift the judge and the Panel of Judges USD 20,000. Just before reading the court decision on March 11, 2010, 'MA' requested additional funds by text and received USD 40,000 the following day.

Tambunan's influence continued following his prosecution and whilst awaiting sentencing was photographed by a newspaper photographer in Bali. It was later discovered that Tambunan had bribed a number of prison guards to be able to slip out of jail to visit to various places. Tambunan paid approximately USD 33,000 plus weekly payment s of USD 166 to eight people.

When operating his financial accounts Tambunan was found to use three different identities, two of which were forged. Both Tambunan and his wife also acquired fake passport documents in order to travel to Singapore, Malaysia, and Macau. The passports were provided by an American citizen; 'JJG'. Tambunan paid USD 100,000 (plus USD 1,000 for the broker) in order to obtain Republic of Guiana's passports. This evidence was uncovered through working with four other international FIU's.

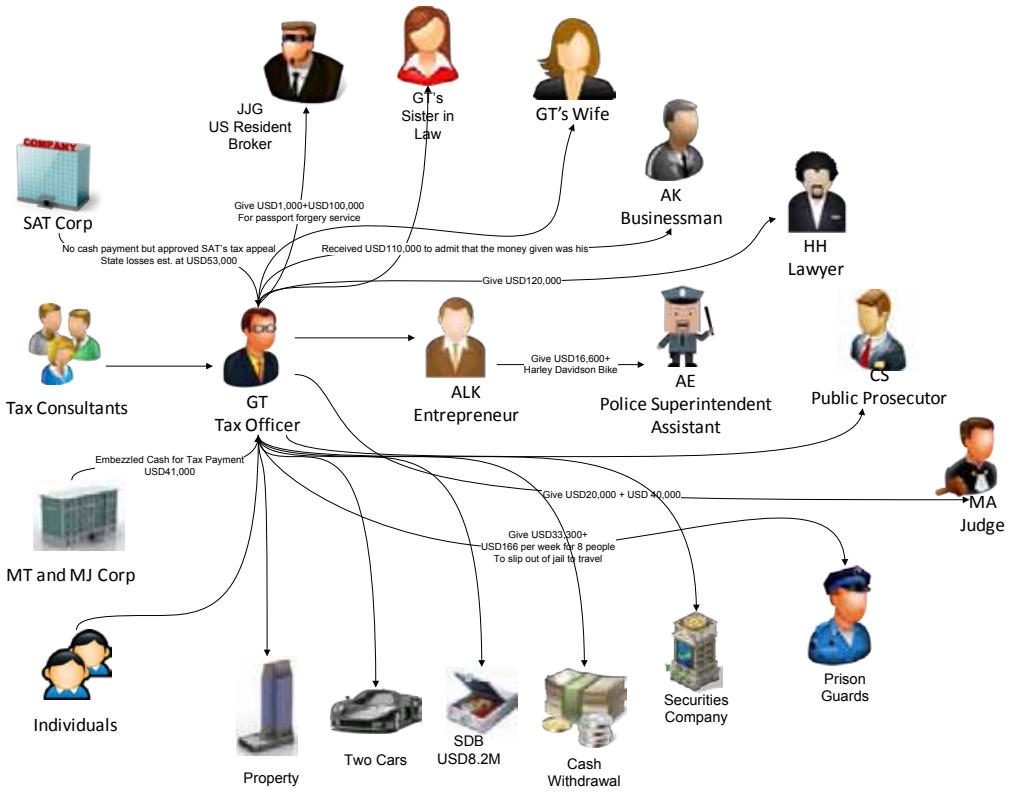
State losses were estimated as USD 11,300,000 and Tambunan was found guilty of corruption, embezzlement, bribery, identity and passport forging, as well as money laundering. He was sentenced to seven years imprisonment and fined USD 33,000 by the District Court on January 2011. Tambunan appealed his case and surprisingly, received a further ten years imprisonment by the High Court on April 2011.

Tambunan's accomplices also received custodial sentences ranging from two to seven years in addition to fines. 'JJG', the fake passport provider, now appears on the International Criminal police organisation 'INTERPOL' red notice list of subjects wanted for extradition or unlawful action.

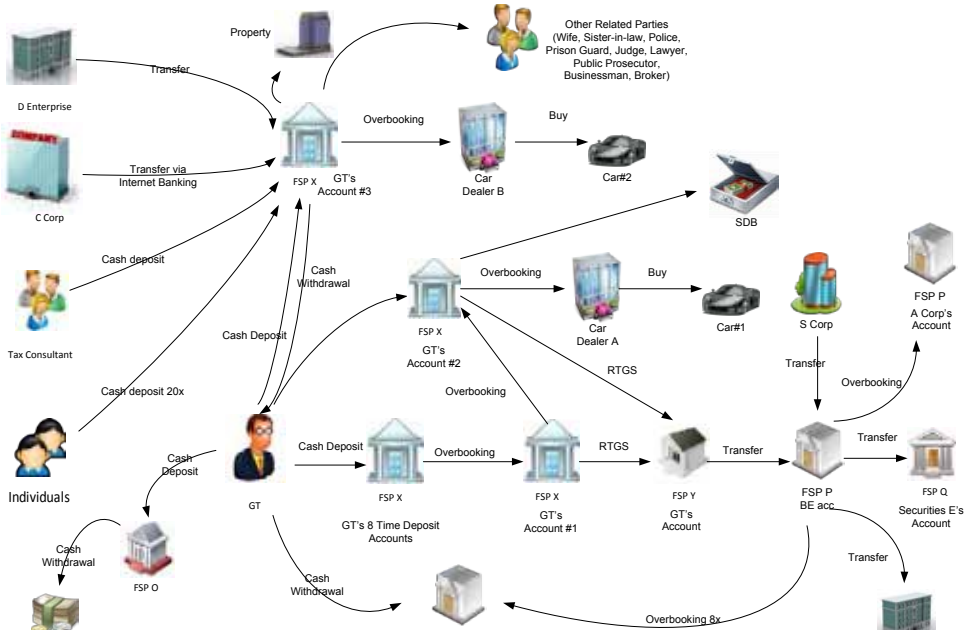
Indictors relevant to this case

- The use of nominees
- The use of fake documentation
- Account transactions with no clear rationale
- Appearance of transactions that form a structuring pattern
- Co-mingling of funds

Association Chart



Flow of Funds

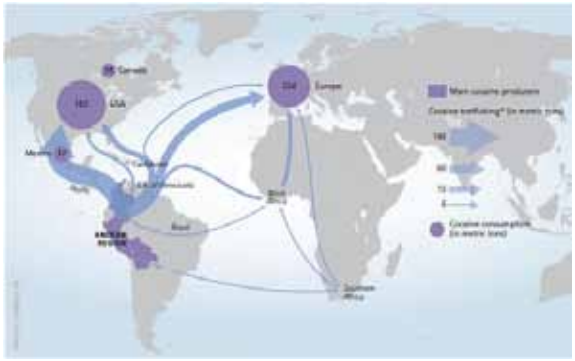


Drug Trafficking

Drug trafficking has become one of the most, if not, the most, profitable illegal business activity of criminal organisations, such as drug cartels, producing multi-billion dollar revenues annually. It involves the cultivation, manufacture, distribution and the sale of substances which are subject to drug prohibition laws.[4]

By definition, drug cartels operating from lower capacity countries will always seek to place their products in markets with a high purchasing power and a demand for their products. Drugs therefore, have to be smuggled first through various jurisdictions and often via routes that involve other low capacity jurisdictions with a lack of a rule of law.

Funds need to be provided to pay for services that facilitate this smuggling using various methods such as couriers, shipping, car/truck transport etc.These funds are often sent to individuals in small amounts via money service businesses. Informal money transfer systems and cash carriers are also used as payment methods making it even more difficult to trace the origin and destination of funds.



The actual payment for drugs is nearly always done with large sums of cash which must be moved and/or eventually integrated into the financial system so that they appear to be legitimate funds that can be used to support a lavish lifestyle or finance other business activities

Criminal groups are becoming more and more creative with their distribution and payment methods. The sale of synthetic drugs over the internet is a growing industry. On-line sites allow for the purchase of drugs using e-currency such as 'Bitcoin' which is a hard-to-trace virtual currency. These groups also work through software systems such as Tor networks which provide anonymity to users of the network.

The following cases describe the movement of money as a result of drug importation from South East Asia, Central Asia and Latin America.

4. United Nations Office on Drugs and Crime (UNODC) UNODC World Drug Report 2010 https://www.unodc.org/unodc/en/drug-trafficking/index.html

Through the analysis of financial transaction data FIUs were able to establish the origin and destination of the funds and establish links between different criminals groups that were previously unknown to law enforcement. Money was moved in a variety of ways including cash couriers and money service businesses. In one case, casinos were used as a method to provide a sense of authenticity with regards to the origin of the cash.

Indicators

- Transactions just below the reporting threshold
- Frequent/unusual use of night deposit drops or ATM machines for deposits
- Using multiple accounts to collect funds that are then transferred to the same foreign beneficiaries
- Reluctance or refusal of individuals to provide identifying information to bank employee
- Sudden, unexplained change in banking habits or activity
- Transfer of funds to a commercial account with no logical relationship or connection to the sender of the funds
- Use of third party bank accounts
- Links to known criminal organisations
- Transactions conducted in round figures
- Account activity inconsistent with customer profile
- The repeated use of transfer/deposit operations in a way that shows the breaking down of a large amount
- Sudden activity/movement in an inactive account, especially when done in large amounts
- Local transfers in large amounts followed by transfers overseas in different currencies
- Luxury living not matching economic status (especially if it was sudden)
- The purchase of real estate/cars/jewelry/other assets of high value
- Early repayment of loans (especially if it is paid in cash)
- Transfers in equal or close values for several persons in different countries, or to one beneficiary in several accounts

4. Multiple heroin importation syndicates dismantled (AUSTRAC, Australia)

Case Description

The following two inter-related cases show how AUSTRAC information and intelligence proved to be pivotal in uncovering links across a network of criminal syndicates that previously were not known to be connected. The combined effect of the two investigations, thanks partly to financial intelligence, was to dismantle a larger part of the network than might otherwise have been the case.

Introduction

Illicit drug importation continues to be a major focus for Australian law enforcement agencies. The strong Australian dollar has lowered the cost of imported drugs and precursors. Combined with strong demand and high criminal profits for most imported illicit drugs, Australia is an attractive criminal 'import/export' market for both domestic based and transnational crime groups.[5] In 2010-11, approximately AUD 85,000 illicit drug related arrests were made. In the same year, more than 9.3 tons of illicit drugs were seized. This reflects an increase of over 400 per cent in the weight of heroin seizures from the previous year and was the highest weight recorded in Australia since 2002-03.[6]

The following two cases, divided into Part A and B, describe the activities of two suspects who worked with other criminal syndicates to import heroin from Vietnam into Australia. The Australian Transaction Reports and Analysis Centre (AUSTRAC) information allowed law enforcement agencies to trace the syndicates' financial activity, identify syndicate members and establish links between them and a wider network of syndicates. It resulted in the disruption of a number of crime syndicates operating in different Australian states.

Part A describes how AUSTRAC information revealed to authorities one syndicate's money laundering methodology through an Australian casino. Part B demonstrates how AUSTRAC information and analysis used in a subsequent investigation revealed links among a network of drug trafficking crime syndicates that were also connected to the syndicate at the center of the case in Part A.

---

5. Jevtovic, P 2012, Organised crime and the high Australian dollar, media release, 27 November, Australian Crime Commission, Canberra, viewed 21 March 2013, < http://www.crimecommission.gov.au/media/organised-crime-high-australian-dollar>.
6. Australian Crime Commission 2012, Illicit drug data report 2010-11, Australian Crime Commission, Canberra, viewed 21 March 2013, <http://www.crimecommission.gov.au/publications/illicit-drug-data-report/illicit-drug-data-report-2010-11>.

Evolution of the Case

Part A and B are separate law enforcement investigations but connected due to links found between crime syndicates across the two cases. The two cases are presented together to demonstrate how AUSTRAC information revealed previously unknown links between suspects and some of the crime syndicates involved in each case. The investigation in Part A preceded the investigation in Part B.

Part A

AUSTRAC provided financial transaction reporting and associated analysis to law enforcement agencies which was instrumental in dismantling an international drug importation syndicate operating in Australia.

For a number of years, the syndicate had been importing heroin of the highest purity from Vietnam. Drug couriers brought the heroin into Australia through internal concealment.

The syndicate used a consistent methodology for recruiting drug couriers and smuggling the drugs into Australia:

- The syndicate generally recruited individuals of Vietnamese descent who were in some form of gambling-related financial difficulty
- The syndicate coerced these individuals into becoming couriers by providing them with loans until, eventually, they owed so much money to the syndicate they were forced to act as drug couriers to pay off their debts
- When a courier was recruited, the syndicate would seek approval from members of another interstate drug syndicate to undertake a drug importation
- Once the interstate syndicate approved, the main syndicate would give the newly recruited drug courier an advance of AUD 5,000
- Before the couriers flew out of Australia, the syndicate would provide them with a Vietnamese mobile telephone number and instructions on how to contact individuals on arrival in Vietnam
- Once the courier had obtained the drugs, they would smuggle the drugs internally back into Australia where they would be met by the main suspects who would assist with the removal of the drugs and then arrange distribution
- Couriers were also used to smuggle drugs within Australia, by transporting the drugs internally on domestic flights for delivery to syndicate members and other syndicates located interstate

AUSTRAC received several suspicious transaction reports (STRs) relating to the syndicate's activities at a casino. The STRs showed that the main suspects regularly provided gambling chips to the value of AUD 5,000 or AUD 10,000 to unidentified third parties. These third parties would then cash the chips after limited gambling activity. This activity indicated that the main suspects were using the third parties to launder illicit funds through the casino on their behalf or were using the casino as a venue to covertly pay members of the syndicate.

AUSTRAC found that, despite the high volume of funds the suspects had been moving through the casino, no cash threshold transaction reports (TTRs) had been submitted to it in relation to the syndicate's activities at the casino. This suggested to authorities that the syndicate had been 'structuring' its cash transactions into amounts of less than AUD 10,000 to avoid the threshold transaction reporting regime.

AUSTRAC information also included reports of a number of international funds transfer instructions (IFTIs) conducted by the main suspects to beneficiaries in Vietnam, totaling approximately AUD 27,000.

The investigation led to four suspects being arrested and charged with various drug offences and the seizure of an estimated AUD 5,000,000 worth of drugs. The suspects were convicted and sentenced to terms of imprisonment ranging from 3 to 11 years.

The Part A diagram in Annex B illustrates how the syndicate operated.

Part B

AUSTRAC information assisted an investigation by identifying previously unknown entities and links between the crime syndicate initially targeted at the start of the case and a network of other drug syndicates operating in different states in Australia. AUSTRAC information helped trace links back to the syndicate discussed in the case in Part A.

Similar to the activity in Part A, the primary syndicate in this case imported heroin from Vietnam to Australia using drug couriers concealing the drugs internally. This primary syndicate also sourced large amounts of heroin from a second drug syndicate, which operated in a different Australian State.

At the request of the investigating agencies, AUSTRAC produced a number of intelligence assessments which analyzed different aspects of the primary syndicate's financial activity. AUSTRAC information enabled law enforcement to identify and link Suspects A and B. Both these suspects were members of the second syndicate and major suppliers of drugs to the primary syndicate. Suspects A and B also had strong links to a third syndicate – the subject of the case in Part A.

AUSTRAC information showed that:

- Members of the primary syndicate made five international funds transfers (IFTIs) to entities in Vietnam, worth approximately AUD 35,000. The majority of funds were sent to Suspect A, who was also the beneficiary of several other IFTIs sent from Australia to Vietnam by other individuals linked to the drug syndicates. Suspect A was known to travel between Australia and Vietnam, with family members in Vietnam who were part of the operation
- AUSTRAC received a suspicious matter report (SMR) showing an unusually steep increase in the annual winnings at a casino by one of the main suspects who was a member of the primary syndicate. This unexplained wealth suggested the suspect was receiving additional income or funds from unknown sources
- Suspect A appeared to control a number of syndicates which were part of an extensive drug trafficking network. This included the primary syndicate and the third syndicate (which was analyzed in Part A)

As a result of the investigation, Suspects A and B were arrested and charged with drug offences. The Part B diagram in Annex B illustrates how the primary syndicate operated and interacted with the wider criminal network that was uncovered.

Conclusion

As of April 2013, there have been 12 suspects charged as a result of the investigations into the network of syndicates discussed in Part A and B. A number of these syndicates have been dismantled and the suspects charged with numerous drug related offences related to the importation and trafficking of an illicit drug.

AUSTRAC provided significant assistance to the investigations with analysis of financial data. AUSTRAC helped to establish the previously unknown key link between some of the drug syndicates in the network. AUSTRAC information and analysis also showed how these syndicates interacted financially.

The two cases highlight the critical intelligence value that transaction information can provide in identifying hidden networks and links among criminal entities and syndicates. With transnational crime groups operating more fluidly to exploit market opportunities, the ability to detect established or opportunistic links among crime syndicates based on financial intelligence as seen in these cases, is likely to increase in importance.

Indicator Tables

Part A

Offence	Drug trafficking
Customer	Individual
Industry	Banking (ADIs) Gambling services
Channel	Electronic Physical
Report type	IFTI SUSTR
Jurisdiction	International – Vietnam
Designated service	Account and deposit-taking services Gambling services
Indicators	• Gaming chips given to unidentified third parties who cash the chips following minimal gambling activity • High volumes of cash moving through accounts belonging to persons of interest at gaming venues • Individuals structuring funds when cashing chips to avoid reporting requirements • International funds transfers to countries and individuals of interest to authorities • Unusual gaming activity

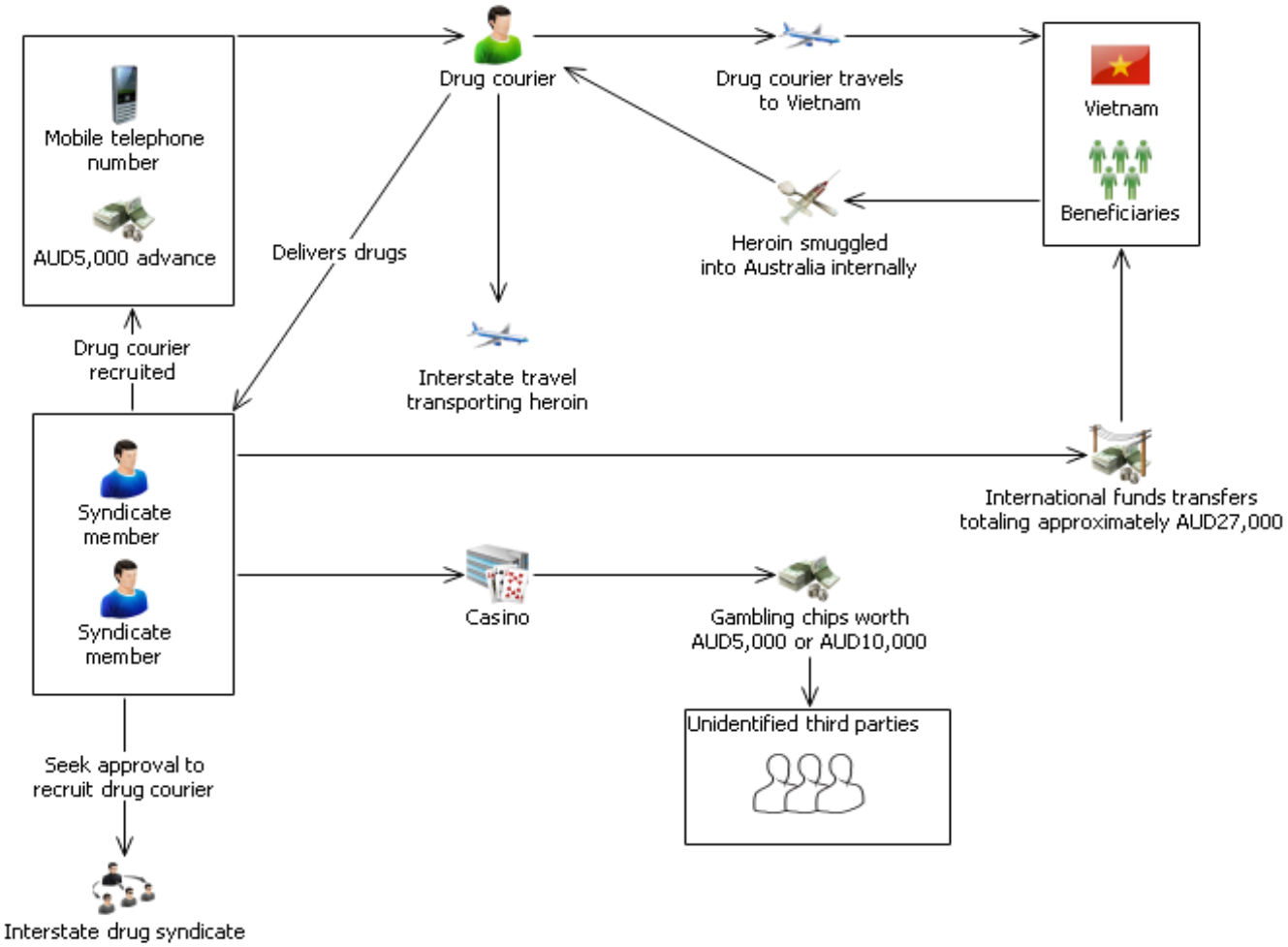
Part B

Offence	Drug importation
Customer	Individual
Industry	Banking (ADIs) International funds transfers
Channel	Electronic Physical
Report type	IFTI SMR
Jurisdiction	International – Vietnam
Designated service	Account and deposit-taking services

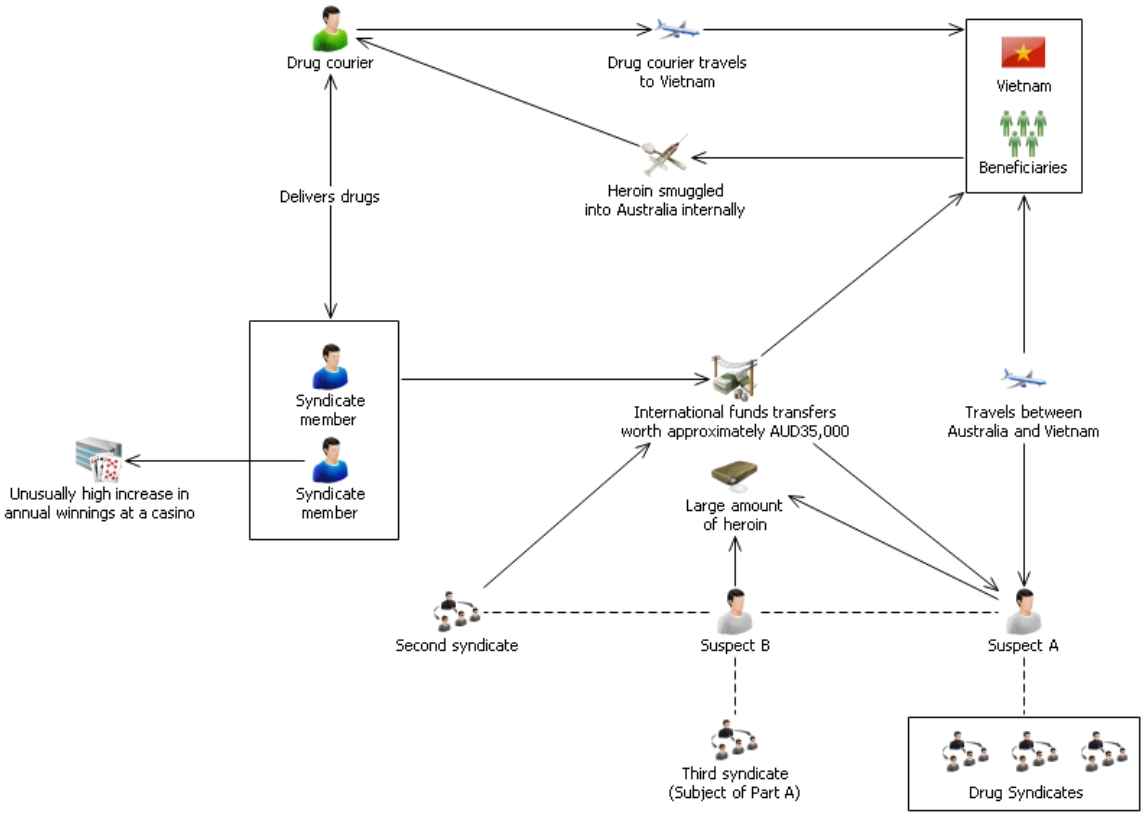
Indicators	• Customer involved with a high value of funds, which are inconsistent with expected/established financial activity for the customer (i.e. unexplained wealth) • Customer making regular international funds transfers of significant values to high-risk jurisdictions • Multiple customers conducting international funds transfers to the same overseas beneficiary • Unusually high increase in annual winnings from gaming activities

Analysis diagrams

Part A



Part B



5. Afghan Heroin (Rosfinmonitoring, Russian Federation)

Case description

The following case demonstrates how The Federal Financial Monitoring Service (Rosfinmonitoring) analysts and law enforcement investigators were able to reconstruct the scheme of a predicate offence based on fragmentary information in order to detect new criminal incidents and to reveal the scheme to launder criminally gained income. This case clearly demonstrates the benefits of an Financial Intelligence Unit (FIU) close cooperation with domestic agencies responsible for combating money laundering, as well as with foreign counterparts.

Introduction

The financial investigation case presented herein is noteworthy due to the complexity and serial repetition of the predicate offence and related money laundering, which were revealed by the FIU based on the information initially received from a law enforcement agency.

In the course of the investigation it was established that members of a criminal group had Organised large-scale smuggling of Afghan heroin to the Russian Federation with the aim of selling it in the Central and Northwestern Federal Districts. The illegal selling of drugs took place in 12 regions of the Russian Federation.

The Russian Rouble cash proceeds were exchanged for foreign currency and partially transferred to other countries, including transfers in favor of the drug trafficking kingpin's relatives. Another portion of the cash money was transported out of Russia by couriers.

Our financial investigation detected the "finance manager" residing in Country A, who was closely associated with the gang's leader. The funds gained from drug trafficking were transferred by the criminal group members and their relatives to the accounts of a "finance manager". The investigation also established the identity of a person who was coordinating the delivery of drugs.

Case development

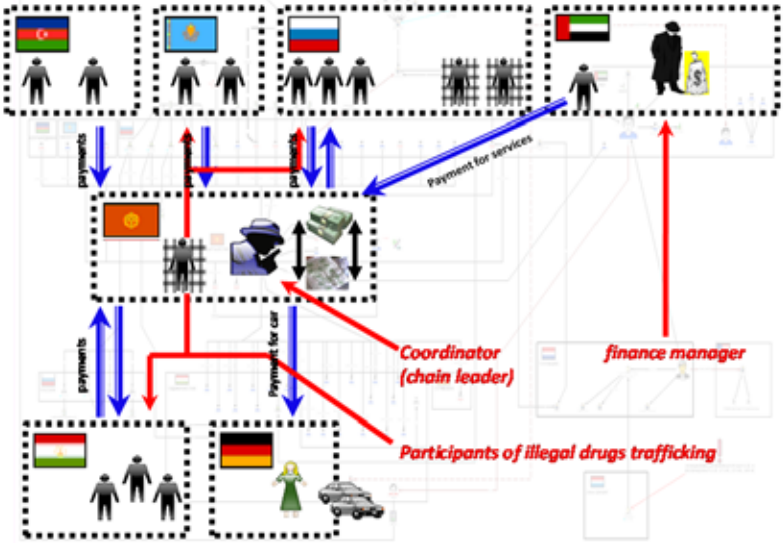
Initial detection

In 2011, law enforcement authorities requested one of the Rosfimonitoring territorial subdivisions for information on several individuals allegedly involved in drug trafficking in St. Petersburg. Initial case development was conducted by a territorial subdivision of Rosfinmonitoring but due to the interregional and international nature of the criminal activities, the case was forwarded to the headquarters for further financial investigation.

Role of the FIU analysis

We consider that the quick exposure of the criminal activities was as a direct result of the work undertaken by our FIU. Law enforcement officers were provided with information concerning the criminal activities of the persons involved, copies of documents obtained, references and financial link schemes.

At first, Rosfinmonitoring carried out a search of FIU data and cooperated with the territory of the Russian Federation to reveal the scheme of the predicate offence. After the criminal scheme had been revealed and the locations of the accumulated funds detected, further work was conducted to reconstruct the



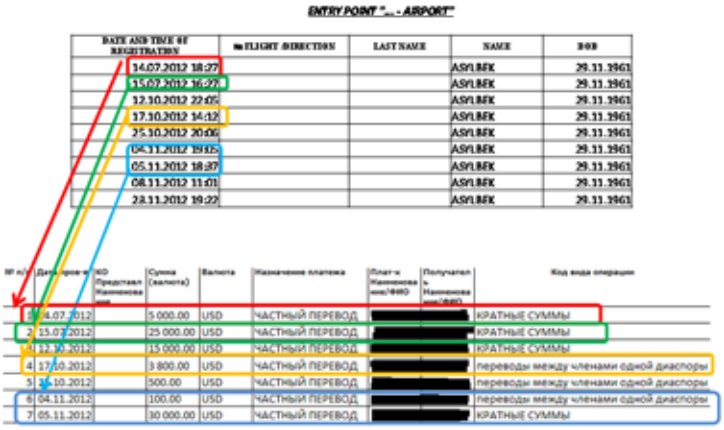
scheme that was developed in an attempt to make the criminally gained income appear legal, to track its final location and to identify persons benefiting from the specified criminal activities.

Rosfimonitoring's territorial subdivision in Northwestern Federal District and the headquarters in Moscow detected that funds gained from drug trafficking by the criminal group members and their relatives had been transferred to the foreign accounts of the gang leaders and their relatives. The facts around the purchase of expensive vehicles and real estate with the cash gained from the sale of heroin have also been revealed.

Rosfimonitoring used some innovative analysis techniques. The characteristics of payments made at different levels of the criminal scheme has revealed features pointing to the existence of other similar distribution chains, but with a different set of individuals. As a result, new criminal activities have been detected and further examined by law enforcement.

By comparing the routes of the domestic and cross-border flights made by the gang members with the suspicious money transfers that were conducted both within Russia and transferred to the accounts opened in some third countries, the FIU analysts succeeded in detecting previously unknown persons (participants of the scheme), means and destinations of the money transfers, as well as revealing the drug trafficking routes.

By identifying the features of the financial links that were associated with each level of the criminal group, we were able to identify their position in the Organised criminal group's hierarchy.



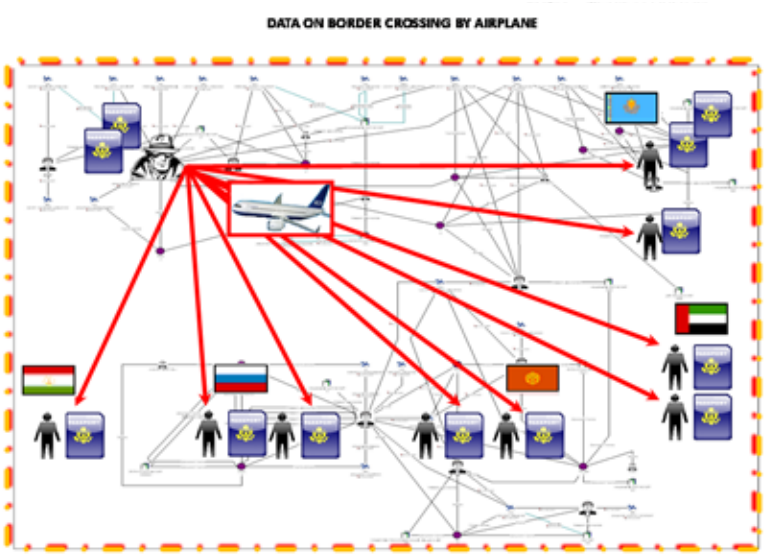
One of the key analytical findings, accomplished literally "on desk", was identifying the "finance manager", a professional in financial services who was accumulating, allocating and transferring funds for criminal purposes including money laundering.

Domestic/International cooperation

At all stages of the financial investigation, the FIU cooperated with Russian law enforcement authorities, with both investigative and operative officers, through the sharing of information and working place meetings. Rosfinmonitoring conducted financial investigations utilizing all available sources of information and by interacting with the Federal Tax Service, Federal Customs Service of Russia and Russian credit institutions. The

analysis of information received from the above-mentioned sources has revealed the scheme of payments for drugs and the laundering of this illicit income, and detected new predicate offence incidents and persons involved in criminal activity.

Having established the withdrawal of part of the funds abroad and the identity of external partners involved, we started actively approaching our counterparts. In particular, we cooperated with FIUs of the USA, the UAE, Tajikistan, Kazakhstan, Uzbekistan, Afghanistan, Kyrgyzstan, Germany, Lithuania, China (PRC) and the Netherlands. Directly through interaction with foreign FIUs we have obtained valuable information concerning the suspects under the criminal investigation. Rosfinmonitoring's coordination efforts and the exchange of information with foreign FIUs resulted in the identification of the accounts opened with the foreign banks and financial institutions, which were or could have been used to launder the drug trafficking revenues.



Purely as a result of FIU-to-FIU interaction have we been able to reveal the identity of the person who was previously unknown to the law enforcement bodies, and is residing in the territory of Country B and who is presumably the regional coordinator for the smuggling of heroin from Afghanistan to Russia through the territory of neighboring countries. He also controlled the cross-border transportation and the distribution of money for the purchase of vehicles which were used to deliver the heroin. He also paid individuals for their role in the drug trafficking scheme.

The person responsible for laundering the money generated from the importation of heroin to Russia was also identified. We also traced their contacts in the territory of Country A and some third countries. Specifically, we have detected investments in professional football clubs who were allegedly involved in the money laundering scheme.

As a result of the FIU-to-FIU interaction, the movement of the proceeds of the drug trade both through the accounts of the persons involved in the crime as well as the movement of money outside the Russian Federation was detected.

In particular, international cooperation has made it possible to reveal a money laundering scheme worth nearly USD 1,000,000 and to determine assets of the individuals involved persons and/or their relatives abroad.

Dissemination to law enforcement authorities

The results of financial investigation were forwarded to the Federal Drug Control Service of Russia, which was in charge of the criminal investigation based on the Criminal Code of the Russian Federation (CCRF) articles related to illegal drug trafficking and proceeds of crime legalization (laundering).

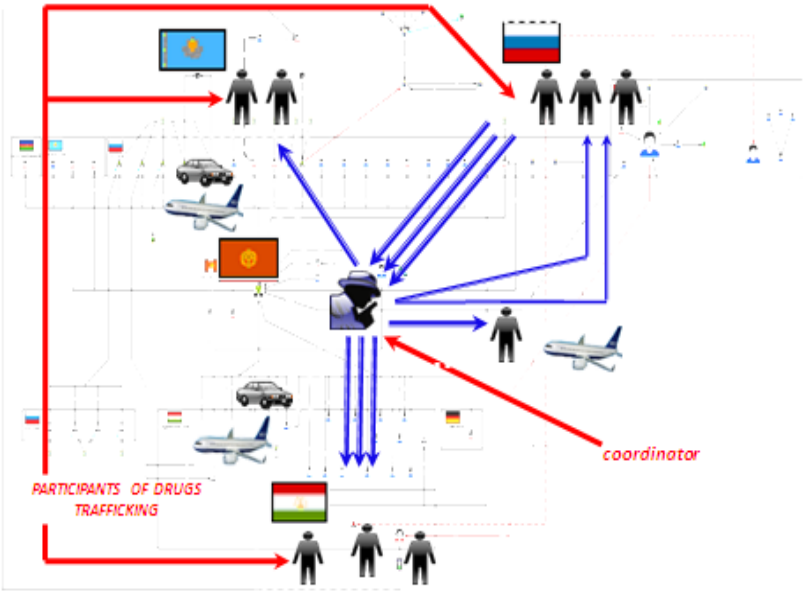
As a result of further investigation and search activities, including those based on materials received from Rosfinmonitoring, the location of the drug trafficking kingpin in Country A was identified and his extradition to Russia was accomplished. He was charged with drug trafficking, organisation of a criminal network and money laundering under the CC RF.

Through cooperation between Rosfinmonitoring and FIUs of certain Central Asian countries some new activities have been detected and persons affiliated with Organised criminal groups identified. The information obtained with regards to their activities and links was passed to Federal Drug Control Service of Russia.

As a result of investigation and search activities, several members of the group were detained, with some 170 kg of heroin seized from them. They were charged with drug trafficking and money laundering under the CCRF.

Due to cooperation between Rosfinmonitoring and the Central Asian FIUs several other individuals linked to heroin smuggling channels were also identified.

Relying on the collected data one of the Central Asian FIUs launched its own financial investigation, which was further investigated by local law enforcement agencies and resulted in the detention of one of the gang members and the seizure of approximately 10 kg of heroin.



Case closure

The total volume of seized heroin was about 250 kg.

The results of the criminal economic assessment, carried out by the Russian Federal Drug Control Service, has revealed the laundering of about USD 3,000,000. The criminal economic assessment has still to be completed. The estimated total amount of money laundered could be around USD 10,000,000.

Conclusion

We believe that our FIU's contribution has made it possible to quickly recover the chain of settlements and transactions related to the predicate offence. Only successful cooperation with national law enforcement authorities, credit institutions and other entities enabled us to reconstruct the complete money laundering scheme. Single informational databases did not contain the data necessary to compile a complete picture of all criminal activites related to the initial case.

This experience has allowed us to develop additional criteria for the proactive selection of financial and other links of individuals involved in drug trafficking and money laundering schemes.

Indicators relevant to this case

- Intelligence indicating links to drug trafficking
- Purchase of real estate and expensive vehicles with cash
- Transfer to criminal group members and family in other countries
- Use of a gatekeeper
- Use of cash couriers
- Transfer of funds to countries with known links to drug trafficking
- Conversion of Russian Roubles for foreign currency

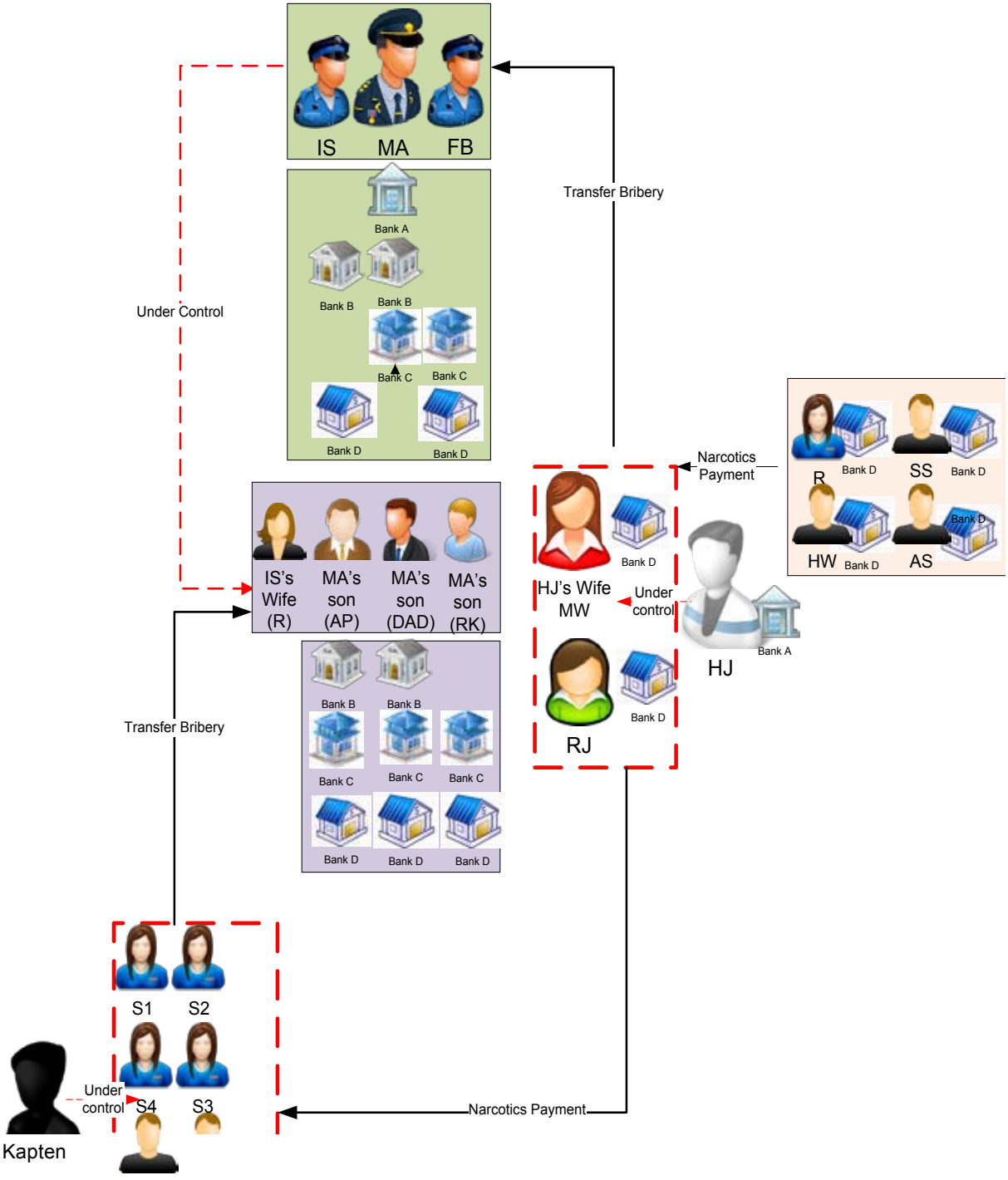
6. The Illegal supply of drugs into Nusakambangan Prison (PPATK, Indonesia)

The case illustrates how the Indonesia Financial Transaction Reports and Analysis Centre (INTRAC) investigated a drugs syndicate which was controlled from within one of the biggest and most isolated prisons in Indonesia, known as Nusakambangan Narcotics Prison (NNP)

The National Narcotics Board (NNB) is the independent law enforcement agency responsible for the prevention of drug crime within Indonesia. In early March 2011, the NNB succeeded in apprehending Marwan Adli (AMA), the warden of NNP along with two other prison officers; Fob Budhiyono (AFB) and Iwan Syaefudin (AIS). Together, they were suspected of providing privileges to prisoner Hartoni Jaya Buana (HJ) so that he could conduct his narcotics business both inside and outside the prison.

INTRAC's involvement in the case began after receiving information from the Ministry of Justice and Human Rights, the government organisation with overall responsibility for managing NNP. The information confirmed that 3 officers employed at NNP had been arrested and provided a list of names, profiles and date of birth details for the officers as well as family members.

INTRAC commenced an investigation and undertook financial analysis. This process revealed that some of the names on the list were connected to several accounts and when compared and contrasted with additional information relating to "MW", the wife of HJ; INTRAC were able to summarize the flow of the money as shown on the following association chart:


IS
MA
FB
Transfer Bribery
Under Control
Bank A
Bank B
Bank B
Bank C
Bank C
Bank D
Bank D
Narcotics Payment
R
Bank D
SS
Bank D
HW
Bank D
Bank D
AS
HJ's Wife MW
Bank D
Under control
HJ
Bank A
RJ
Bank D
IS's Wife (R)
MA's son (AP)
MA's son (DAD)
MA's son (RK)
Transfer Bribery
Bank B
Bank B
Bank C
Bank C
Bank C
Bank D
Bank D
Bank D
S1
S2
S4
S3
Under control
Kapten
Narcotics Payment

Evolution of the case

The two main drug dealers within NNP were HJ and Kapten. They controlled their syndicate from inside the prison and controlled bank accounts held in the names of third parties.

Narcotics payments were deposited into two separate bank accounts held by MW and RJ but which remained under HJ's control. Money had also been transferred to the prison warden and officers as well as to members of their families.

Kapten also controlled accounts in the names of many individuals which also received illicit income from MW and RJ's accounts. Money was transferred from these accounts to accounts under the control of the prison staff.

The analysis concluded that the transfers, both directly and indirectly, from HJ and Kapten to the prison staff demonstrated their involvement in the syndicate. The use of the third party accounts also indicated that they were attempting to conceal and disguise the identities of the senders and beneficiaries as well as the underlying transactions (drug deals) that were made by the syndicate.

Within less than a week from receipt of the initial information from the Ministry of Justice and Human Rights, INTRAC successfully collected the syndicate's financial information from reporting entities and disseminated the financial intelligence to NNB. INTRAC's analysis assisted the NNB investigation by using a 'follow the money approach', especially when it came to identifying related parties who were involved in the syndicate. INTRAC also made recommendations to the Ministry of Justice and Human Rights relating to the internal supervision of the correctional institution.

INTRAC also provided another significant role as a money laundering legal expert witness for the NNB during the investigation phase and for the prosecutor at court trial phase.

The NNP officers and their families were convicted of money laundering both as active and passive offenders. The court trial revealed that the use of the NNP officers' and their relatives bank accounts were a part of the money laundering activity in which these individuals received or controlled the placement, transfer or payment of funds which originated from proceeds of narcotics crime.

Conclusion

This is the first money laundering case which was enacted under Article 5 of Indonesian Anti money Laundering (AML) Law, which is dedicated to punishing passive money laundering offenders. This case will set a precedence for similar cases in the future.

Thanks to the effective coordination and cooperation between INTRAC and its stakeholders; NNB, Ministry of Justice and Human Rights and the prosecutor, this case resulted in the identification of a drug syndicate within the NNP and the following penal sentences:

- Hartoni Jaya Buana (HJ) received a 20 year prison sentence and IDR 10,000,000,000 fine with a 1 year subsidiary prison sentence for money laundering and narcotics offences as an active offender
- Syafrudin alias "Isap", "Kapten" received the death penalty in relation to narcotics offences
- Marwan Adli (MA) received a 13 year prison sentence and IDR 10,000,000,000 fine with subsidiary of 8 months imprisonment
- RK received a 1 year prison sentence and IDR 200,000,000 fine with subsidiary of 2 months imprisonment
- AP received a 2 year prison sentence and IDR 50,000,000 fine with subsidiary of 2 months imprisonment
- DAD received a 18 month prison sentence IDR 100,000,000 million fine with subsidiary of 6 months imprisonment
- FOB Budiyono received a 7 year prison sentence and IDR 1,000,000,000 fine with subsidiary of 8 month imprisonment
- Iwan Syaefudin received a 5 year prison sentence and IDR 10,000,000,000 fine with subsidiary of 8 months imprisonment
- RJ, received a 2 year, 6 month prison sentence and IDR 250 million fine with subsidiary of 6 months imprisonment
- MW received a 2 year, 6 month prison sentence and IDR 250 million fine with subsidiary of 6 months imprisonment

Fraud

Fraud is a global threat and a widespread problem! Significant numbers of people each year fall victim to fraudulent acts. Several surveys have shown that fraud levels are on the increase and that there are a wide range of techniques used to commit frauds.

Fraud is described as a deception deliberately practiced to secure an unlawful gain by providing false or misleading information, or by concealing what should have been disclosed.

Efraim Diveroli, an American arms dealer who was convicted of fraud in 2011

There are a number of fraudulent activities embezzlement, insider trading, the sale of fraudulent products, bribery, cheque fraud, credit card fraud and confidence tricks to name a few, all of which can produce large profits. Criminals are always looking for easy ways to make large sums of money and their methods are constantly becoming more creative and sophisticated.

The internet provides the ideal tool to conduct fraudulent activities given the anonymity that it provides and also the ability to reach a large, transnational community. Scams are a popular type of fraud that frequently make use of the internet.

Advance fee fraud involves an unsolicited invitation to potential victims to invest funds, usually with the promise of significant financial returns. The scams lure potential victims by offering them a range of benefits. These may include money, prizes, gifts or employment - none of which actually exist.[7]

'Boiler room' scams involve high pressure selling of low value shares with the promise of growth. As the number of investors increase, so does the value of the shares which often encourages more investors. Once the shares reach a significantly higher value, the fraudster sells their portion of the shares enjoying the large profits. This results in a crash of the share sale price with significant losses to the victim investors.[8]

The following cases are a selection of the best examples on a wide variety of fraud cases detected with the help of FIUs in recent years.

What we learn from these cases is that fraud is not necessarily always a large scheme but it is usually difficult to detect. It often starts small and it is not until a large number of victims are involved that warning signs start flashing. While many instances of fraud go undetected,

7. AUSTRAC typologies and case study report 2011 http://www.austrac.gov.au/files/typ_rpt11_typol.pdf
8. AUSTRAC typologies and case study report 2011 http://www.austrac.gov.au/files/typ_rpt11_typol.pdf

learning how to identify the warning signs early may help to mitigate the loss caused by frauds or substantially reduce "fraudulent acts". From these cases we also learn that the detection of fraudulent activities often requires the analysis of massive amounts of data, and that analytic methods alone are not sufficient. At all stages of financial fraud investigation, successful domestic and international cooperation of key stakeholders is crucial.

Indicators

- Money being transferred to another account soon after being deposited
- Transfer of funds to countries known for fraudulent schemes
- Difficulty in verifying customer identification information
- Schemes that offer unusually large returns on investment
- Multiple customers sending international funds transfers to the same overseas beneficiary
- Multiple international funds transfers sent to the same beneficiary in one day
- High-value international funds transfers
- U-turn transactions, involving funds being transferred out of the country and then part of those funds being transferred straight back into the same country
- Series of low value international funds transfers
- Transfer of funds to recipients in countries where the recipient's name is not traditionally associated with that country

7. Efraim Diveroli/AEY Investigation – The supply of banned arms (FinCEN, United States)

Introduction

As its name implies, the United States Financial Crimes Enforcement Network (FinCEN) serves to coordinate a vast array of information among regulators, law enforcement entities, and the financial sector. This approach allows stakeholders, especially law enforcement agencies, to leverage their own expertise while drawing upon information provided by the financial sector. FinCEN, in turn, provides guidance so investigators can benefit from information collected from both domestic and foreign sources. FinCEN also provides subject matter expertise as needed for certain investigations.

This information sharing, through FinCEN's resources, proved instrumental in the investigation and successful prosecution of an arms dealer accused of serious fraud. Several investigative agencies, all with strong ties to FinCEN and direct access to FinCEN records, formed a task force to coordinate actions on the case.

FinCEN's assistance included proactively identifying records related to the case and leveraging its links to the domestic financial community and Egmont Group for more information.

FinCEN further strengthens information sharing by housing representatives from federal law enforcement agencies to work side by side with FinCEN personnel. Some of the larger agencies send two or three representatives for full-time details, while smaller agencies use FinCEN space and resources as investigations warrant. This not only enhances cooperation between FinCEN and individual agencies, but it also improves communication among the agency representatives detailed to FinCEN as well.

The arms dealer, Efraim Diveroli, is the president of AEY, a munitions supplier with offices in Miami Beach, Florida. When the then 19-year old Diveroli began his career in 2005, AEY would bid on smaller contracts for numerous U.S. government agencies.

Soon after, AEY was juggling dozens of contracts, but its performance deficits went undetected by overextended Defence Department auditors. By the end of AEY's first year, they had won 149 contracts worth an estimated USD 10,500,000, mostly with the Defence Department or the State Department.

AEY had a mixed record on fulfilling government contracts. In fact, officials withdrew at least 11 jobs from AEY because of poor performance. The reasons for terminating the contracts included providing potentially unsafe helmets, failing to deliver at least 10,000 pistols, and shipping poor quality ammunition to U.S. Specials such as "damaged goods", "junk" weapons, and other equipment in "the reject category".

These officials complained on several occasions that AEY was "hurting the mission," had "endangered the performance" of government agencies, "failed to deliver acceptable goods," "provided no notice of an excusable delay," and "provided inadequate assurance of future performance." One contracting officer reported that AEY repeatedly engaged in "bait and switch" tactics by substituting nonconforming goods in place of those required by the contract. However, AEY continued to be awarded contracts by underbidding the competitors.

In contrast to most government contractors, Diveroli bid on contracts without a secured source for the products, attempted to locate suppliers and goods after the contracts were awarded, and provided nonconforming substitute products when unable to locate the required goods.

In 2006, the Department of the Army issued a solicitation requesting bids on a contract to provide various types of ammunition to the Islamic Republic of Afghanistan. AEY was one of the bidders, but was competing against at least 10 well-established companies. The army awarded the contract to AEY for its low bid of USD 298,000,000 on January 2007, making AEY the main supplier of ammunitions to Afghanistan's army and police force.

Under the terms of the contract, AEY was required to certify that it was providing serviceable and safe ammunition. The contract required that the ammunition must be "serviceable and issuable to all units without qualification." It also prohibited delivery of ammunition acquired, directly or indirectly, from certain countries.

Diveroli purchased the ammunition in Albania, but this ammunition was originally manufactured in a different country which was a prohibited source. To effectuate the scheme and hide the ammunition's origins, Diveroli and his co-conspirators would direct others to repackage the ammunition. Diveroli hired a businessman in Albania to bundle millions of bullets into new plastic bags and place them in cardboard boxes in order to conceal the true origins of the ammunition and save money on airfreight.

With each shipment, AEY falsely certified the Certificate of Conformance to state that the supplied ammunition conformed to the contract requirements, and that its manufacturer and point of origin were from a legitimate source. Based on these false submissions, the army paid AEY millions of dollars for 35 shipments of prohibited ammunition.

These submissions and resulting payments to AEY are the basis for charging all defendants with procurement fraud against the United States. This fraud cost taxpayers millions of dollars and resulted in the supply of substandard ammunition for foreign security forces.

Evolution of the case

Initial Detection

Homeland Security Investigations (HSI) began the investigation of Diveroli after receiving allegations of licensing violations by an arms dealer who frequently bid on U.S. Government contracts. In the course of the investigation, HSI discovered evidence of contract fraud and sought collaboration with other agencies. Soon after, the prosecutor's office, the United States Attorney for the Southern District of Florida, established a working group for all agencies involved in the investigation. These agencies accessed FinCEN's records and requested additional assistance from FinCEN as the case developed.

Role of the FIU and Analysis

This case highlights the multiple ways FinCEN provides law enforcement support. First, FinCEN gives law enforcement direct access to more than 150 million records it has collected under the Bank Secrecy Act (BSA), including more than a million Suspicious Activity Reports

(SARs) it collects yearly. FinCEN manages all aspects of this access including issuance of passwords, training, and the monitoring of BSA data security. Second, FinCEN can, upon request, provide extensive BSA analysis and apply advanced querying techniques in support of open investigations. Third, FinCEN assists law enforcement agencies in obtaining information from Egmont Group FIUs and manages a specialized communication channel with the financial sector, known as the 314(a) program.

In 2005, a representative from the Defence Criminal Investigative Service (DCIS) queried Diveroli in the BSA database, but met with negative results. However, this query created a record in FinCEN's case management system that later proved useful for networking, de-confliction and case history management. DCIS noted on the case record that HSI was participating in the investigation.

In 2006, a financial institution filed the first SAR on AEY for suspected money laundering between February and March 2006, involving more than USD 2,700,000. The bank reported that Diveroli was transferring large sums between his personal savings account, money market account, business, and personal checking accounts. When the bank questioned Diveroli about his business, he closed his accounts and refused to provide further information.

In October 2007, an Army-CID special agent, who is detailed to FinCEN, performed a number of searches, including the BSA records. Among the records retrieved was the 2006 SAR that clearly indicated that Diveroli had accounts in other banks.

In November 2007, Army-CID again reached out to FinCEN and filed a USA PATRIOT Act Section 314(a) request. This section of the Act allows law enforcement agencies to request that U.S. financial institutions search their records for subjects in terror financing and significant money laundering investigations. This search helps investigators identify previously unknown accounts. The request by Army-CID was submitted because Diveroli had made large deposits in several bank accounts in the U.S. and was suspected to have accounts overseas wherein he could deposit monies from the unlawful activity. Investigative activity had already disclosed the purchase of negotiable instruments and internal transfers in various accounts opened by Diveroli in excess of USD 10,000. The case agent reported that the 314(a) request did indeed provide previously unknown account information.

As often happens, the 314(a) request generated additional SARs as financial institutions reviewed their records and discovered transactions related to Diveroli and AEY. These SARs revealed international and domestic account information previously unknown to investigators. Several international wire transfers led investigators to foreign bank accounts owned by AEY, and indicated the use of a shell corporation. Moreover, the 314(a) served as a "red flag" and financial institutions began monitoring accounts belonging to AEY and its associates.

By December 2007, both HSI and Army-CID were regularly interrogating BSA records for more information on AEY and Diveroli. Subsequent SARs noted suspected money laundering occurring between March 2007 and January 2008. During that period, 58 wire transfers totalling USD 44,115,457 were received by Diveroli, and 189 wire transfers totalling USD 48,258,729 were sent by Diveroli. Many of the outgoing transfers were sent internationally.

A New York Times investigative article on Diveroli and the illicit ammunition deals published in March 2008 prompted FinCEN to proactively search the BSA data for Diveroli and his associates. Analysts located several SARs and referred them to the HSI liaison detailed to FinCEN, and coordinated its findings with the other agencies investigating AEY.

In April 2008, a bank filed a SAR after it was contacted by the Army-CID case agent. The SAR described a series of transactions including a suspicious wire transfer in June 2007 for more than USD 500,000 from AEY to a bank in Cyprus.

In June 2008, U.S. Army-CID requested all account activity on Diveroli and his associates from three European Egmont Group members. Army-CID had received information that Diveroli allegedly paid bribes to several individuals in these countries. Diveroli was paid approximately USD 69,000,000 of the USD 298,000,000 contract, but a review of his assets in the U.S. did not account for these expenditures. FinCEN requested detailed account information and activity, personal and business identifiers, and any Suspicious Transaction Reports (STRs) filed in these three jurisdictions.

As FinCEN was reviewing and processing the request, an analyst conducted additional research on the BSA database. The FinCEN analyst found other identifiers for Diveroli and more BSA information not known by Army-CID investigators. This additional FinCEN research greatly assisted Army-CID. In fact, the Army-CID agent, who is physically located close to FinCEN, is one of the most proficient and experienced users of BSA data in the country. FinCEN personnel often use their advanced knowledge to supplement the work of senior analysts and investigators.

The requests made through the Egmont Group returned information from a jurisdiction on Evdin Ltd, a firm that did business with AEY. In addition, another European FIU reported a previously unknown bank account. The Army-CID case agent reported that "the European FIU was very cooperative and helpful in the investigation". The Egmont data helped significantly in this case making connections between Diveroli and Evdin Ltd. and located international accounts in two countries. Through FinCEN's assistance, and especially with the use of STRs, investigators learned that Evdin Ltd and its President Ralph Merrill were connected to Efraim Diveroli. The Army-CID agent assigned to FinCEN said the Egmont Group Financial Intelligence Unit (FIU) information was vital to their investigation, and that this case returned the best results they have ever received back from Egmont Group FIUs. FinCEN's contribution to this case included coordinating the flow of information from the financial sector, the Egmont Group FIUs and other law enforcement agencies. Moreover,

law enforcement agencies were not only able to obtain this information through FinCEN, but FinCEN added value by having its experts in these areas review requests and responses to ensure that every possible lead was completely researched and analysed. Finally, FinCEN also conducted a unique post-case analysis of the use of the BSA and FinCEN resources in select cases. This analysis occurs after arrest or indictments, and serves as a broad platform to share information on how law enforcement agencies use BSA data. The collected analyses are posted on FinCEN's secure portal for law enforcement, and sanitised versions are available on FinCEN's public web page.

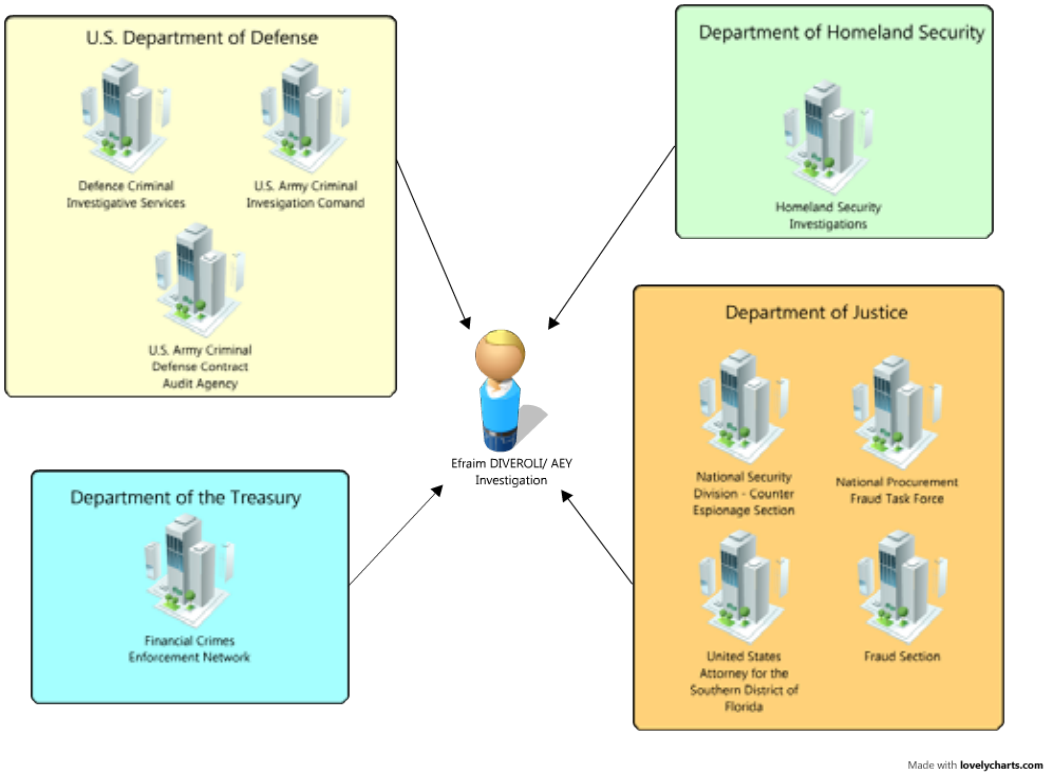
Domestic/International Cooperation

As noted above, HSI initiated an investigation of Diveroli and AEY for suspected contract fraud and numerous violations of the Arms Export Control Act. Competitors alleged a variety of offenses including corruption and illegal quality and origins of weapons and munitions. Although investigators found that many of the accusations were false, or the accusations were never proved, AEY became known to law enforcement and other government agencies as an entity requiring enhanced scrutiny.

In April 2006, the U.S. Department of State put AEY and Diveroli on its Arms Trafficking Watch List because of the HSI investigation. HSI works closely with the state department to ensure enforcement of licensing procedures. The state department listed all the primary actors in AEY's business as potential arms traffickers including an intermediary and one of its major suppliers located in Albania.

Investigators discovered the contract fraud in August 2007, when HSI and DCIS agents served a search warrant at AEY's offices in Miami Beach, Florida in support of the licensing violations investigation. During the search, agents recovered company e-mails about the army contract and the conspiracy to use prohibited ammunition and falsify the records. With evidence of the contract fraud, HSI notified Army-CID about the potential illegal activity. In October of 2007, Army-CID started its own investigation of Diveroli and AEY. The U.S. Attorney's Office in Miami, Florida assisted the investigation by giving HSI, DCIS, Army-CID, and the Defence Contract Auditing Agency space in their office for a task force to meet and share information. On March 25, 2008, the defence department suspended Diveroli and AEY from contracting with any agency in the executive branch of the United States government.

The department of defence cited the shipments of prohibited ammunition and the false claims that Diveroli made by attributing the munitions to a permitted source. On the same day that the New York Times published its article on AEY, the United States House of Representatives Committee on Oversight and Government Reform opened an investigation to establish the scope of AEY's contracts with the defence department in their efforts to investigate allegations of legal violations by AEY. As noted above, FinCEN outreach to the Egmont Community proved very beneficial to this investigation. Case investigators repeatedly acknowledged that months of time was saved by the foreign FIUs' cooperation.



Disclosure to Law Enforcement

Since its founding, FinCEN has worked closely with law enforcement to ensure that its information is readily available for criminal investigations. Agency representatives have always been housed at FinCEN, and FinCEN has provided over 300 agencies with direct access to its data. In this case, the major investigative agencies not only had direct access to FinCEN data, but had representatives located at FinCEN. This allowed unparalleled collaboration as the task force participants in Miami also had colleagues working side by side at FinCEN.

Case Closure

On June 19, 2008, a federal grand jury in Miami, Florida, returned a 71-count indictment against AEY, Efraim Diveroli, Ralph Merrill, and two AEY officers for Conspiracy to Commit Offenses against the United States, and Major Fraud against the United States. At the time of the indictment, Efraim Diveroli was only 21 years old.

In 2009, Diveroli pleaded guilty to Conspiracy to Commit Offences against the U.S. In return for pleading to one conspiracy count of making false statements to the government, the U.S. Attorney's Office agreed to drop 84 other procurement charges and a forfeiture allegation. AEY also pleaded guilty to the same count. On February 2, 2011, Efraim Diveroli was sentenced to 48 months in prison, 3 years supervised release, 200 hours of community

service, 90 days home detention, USD 149,279 in restitution, and a USD 250,000 fine. Ralph Merrill was sentenced to 48 months in prison, 3 years supervised release, and a USD 150,000 fine after being convicted of Conspiracy to Commit Offences against the U.S., Major Fraud, and Wire Fraud. For their cooperation, the two AEY officers that aided in the investigation received probation, and each had to pay almost USD 150,000 in restitution. AEY and all the individuals involved in this case have been debarred from federal contracting for 14 years.

Conclusion

FinCEN's approach is to provide law enforcement agencies with their own access to financial reports required by the Bank Secrecy Act and provide expertise for higher level research and analysis. In addition, FinCEN provides important links to the domestic financial sector and Egmont members across the globe. This approach is facilitated by having law enforcement agencies physically located at FinCEN. In the investigation of Diveroli and AEY, the various law enforcement agencies queried FinCEN's records at different times in the investigation and were able to gain access to records as financial institutions filed them. These records in turn provided leads for investigations to follow both domestically and internationally. FinCEN provided the links and processes that enabled investigators to gather more evidence from these sources. At various stages in the investigation, FinCEN conducted additional research and analysis, coordinated the flow of information and provided guidance and expertise when investigators sought information from the financial sector or Egmont members.

The results helped collaborating agencies work more efficiently and stop a major fraud as it was occurring. The successful conclusion of this case saved taxpayers millions of dollars and stopped the issuance of unsafe and substandard ammunition to Afghani security forces. Moreover, leads uncovered in the investigation led to additional inquiries in foreign countries.

Background

Diveroli

Efraim Diveroli started off in the world of arms procurement at a young age. Diveroli left school in the ninth grade and soon became an apprentice arms dealer working for his father's and uncle's arms companies. He was traveling the country selling weapons by the age of 16. His father, Michael Diveroli, incorporated AEY in 1999 as a label-printing business and passed the company onto his 19 year old son in 2005 by listing him as President. Efraim Diveroli also owns LOW LLC, Advanced Munitions, Pinnacle Minerals Corp. and Ammoworks.

David Packouz gave up his career as a massage therapist and joined AEY in 2005 when he was twenty-three years old. At the time, Packouz was looking for something to do and his long-time acquaintance Diveroli was looking for a partner. Soon after, Packouz got married and a month after AEY was awarded the contract his daughter was born. Packouz eventually

quit AEY before the indictment because he was never paid for his work. He then started his own ammunitions company, Dynacore. Today he has returned to massage therapy and is also an aspiring pop-star. He produced a music album with humanitarian themes, called MicroCOSM. The songs are "meant to tell a story of love spanning outwards."

Alexander Podrizki, another friend of Diveroli's that he had made at the synagogue, was also 23 years old when he joined AEY. He served as a company agent who worked in Albania directing in the repackaging of the ammunition. Packouz and Podrizki came forward during the investigation and helped investigators put Diveroli behind bars. Both received probation and a large fine.

The Albania Connection

The United States International Defence Threat Reduction Agency (DTRA) offers incentives to countries for destroying ammunition caches that are over fifty years old. DTRA compensated Albania for destroying the ammunition that it had. But in actuality, the prime minister was taking their money, and then increasing his profit by selling the old ammunition to companies like AEY. Diveroli never planned on purchasing the ammunitions legally and needed a go between to shield AEY's arms transactions from U.S. government scrutiny. Rather than buy the ammunition directly from Albania, Diveroli chose to go through an arms company in Cyprus called Evdin Ltd, owned by Swiss arms dealer Heinrich Thomet. As a broker, Thomet created an array of shell companies and offshore accounts to Diveroli from Albania's national arms-export company (MEICO). Evdin bought the ammunition from MEICO for USD 22 per 1,000 rounds then sold it to AEY for much more.

It is suspected that Evdin's purpose was to divert money to Albanian officials such as Ylli Pinari, the head of the arms export agency, and the defence minister Fatmir Mediu. When Diveroli realised that the ammunition actually originated from a prohibited source, he directed others to repackage the ammunition and hide its true origins so they would not get caught violating the contract prohibitions. Diveroli hired an Albanian businessman named Kosta Trebicka to bundle millions of bullets into new plastic bags and place them in cardboard boxes in order to conceal the origins and save money on airfreight. With each shipment, AEY would falsely certify in a Certificate of Conformance that the ammunition being furnished conformed to the contract requirements, and that the manufacturer and point of origin of the ammunition was MEICO in Tirana, Albania. Due to high level pressure from Ylli Pinari, Diveroli eventually fired Trebicka and hired Pinari's own man, Milhal Delijorgji.

In June 2007, a jaded Kosta Trebicka recorded a phone conversation with Diveroli where Diveroli conceded that he believed Ylli Pinari was linked to organised crime, and that the chain may lead all the way up to the Prime Minister. Trebicka contacted an Albanian-American anti-corruption activist who contacted the U.S. Department of Justice and Defense, as well as the New York Times, which happened to be investigating arms dealing in Eastern Europe.

In March 2008, an explosion in Gerdec at an ammunition disassembly warehouse overseen by Delijorgji killed twenty-six people, injured at least 300 others, and destroyed hundreds of homes. This focused global attention on Albania's surplus arms industry. Two weeks after that, the New York Times published a report on AEY and Diveroli, exposing the origins of the bullets and alleging that many cartridges were more than forty years old.

Once the explosion occurred, Albanian investigators took over the case regarding the Albanian officials and MEICO's involvement with AEY. The investigation of the Albanian connection by American investigators stopped there. When the case against AEY went to trial, Kosta Trebicka was working with investigators from the U.S. Justice Department and another congressional oversight committee as a witness against AEY. He was also acting as a witness in the Albanian investigation into the explosion in Gerdec. Mr. Trebicka provided the Committee with ledgers from the repackaging process that identifies the country of origin for the ammunition. He thereafter became afraid for his life and fled. On September 12, 2008 his body was found on a remote road in Albania.

Three individuals were arrested for negligence in the investigation into the munitions trading and the explosion at the disassembly plant; a defence ministry official, and the owner and manager of the Albanian company tasked with dismantling the ammunition. The former defence minister, Fatmir Mediu, has been stripped of his immunity and all three individuals were convicted and sentenced to life in prison.

Indicators relevant to the case

- Multiple international wire transfers
- Multiple transfers of large sums of money between accounts
- Multiple accounts with no justification
- The type of business Diveroli is in and questions how he holds the position of arms dealer/president/supplier of AEY (all three positions)
- Company repeatedly engaged in "bait and switch" tactics by substituting nonconforming goods in place of those required by the contract
- Company continued to be awarded contracts by underbidding the competitors that were well established in the market
- Poor company performance despite continued business by winning bids
- Company falsely certified the Certificate of Conformance to hide the point of origin-contract falsification

- Transfer of large sums between personal savings account, money market account, business and personal checking accounts
- Closure of accounts and refusal to provide further information when financial institution requested additional 'Know You Customer' information
- Large deposits in several bank accounts in country of origin
- Use of foreign bank accounts
- Use of shell companies

8. Structuring in an effort to avoid tax (APML, Serbia)

Introduction

This case describes the use of multiple accounts established in a number of countries to enable intensive structuring activity. The ultimate aim was to distance the suspect from the original source of funds as a way to avoid the payment of taxes.

Evolution of the case

The Serbian FIU received a number of Suspicious Transaction Reports (STRs) from a bank, involving individuals A and O. The STRs stated that these individuals' accounts were frequently credited by different legal entities and individuals with the stated purpose "financial support". The funds were credited from various places including high-risk countries. Immediately after the crediting, the funds were withdrawn from the account.

Serbian FIU received information that a non-resident individual 'G' had transferred money to the bank accounts of a number of legal entities in different countries including the Philippines, Hong Kong, USA, Dubai and Pakistan.

The funds were then successively transferred from the bank accounts of these legal entities in the above countries to the individual bank accounts A and O held with two banks located in Serbia. The stated purpose of the transfers was "support", which added to the suspicion on the actual purpose of the transactions.

In the period 2006 – 2009, the foreign currency account of individual A was credited with a total of USD 880,000. The funds arrived from different legal entities. USD 300,000 was transferred by an exchange office from the Philippines. USD 200,000 by a number of individuals from Pakistan, which is considered a high-risk country, a total of USD 200,000 was transferred by a legal entity in the USA and USD 180,000 was transferred by a Hong Kong based legal entity. The stated purpose of these transactions was "support" to

individual A in the Republic of Serbia.

The foreign currency account of individual O is credited by a legal entity from the USA and by an exchange office from the Philippines under the same grounds, i.e. "support".

The Serbian FIU sent a request for information to the Philippines FIU concerning the legal entity transferring the funds to the bank accounts of the individuals in Serbia. The Philippines FIU replied that the legal entities were in fact exchange offices which had been under investigation in the Philippines. In addition, the individuals from the exchange offices in Serbia had also been under scrutiny. Namely, the exchange offices were being used as the channel to transfer funds associated with ransoms (kidnapping), as well as drug trafficking.

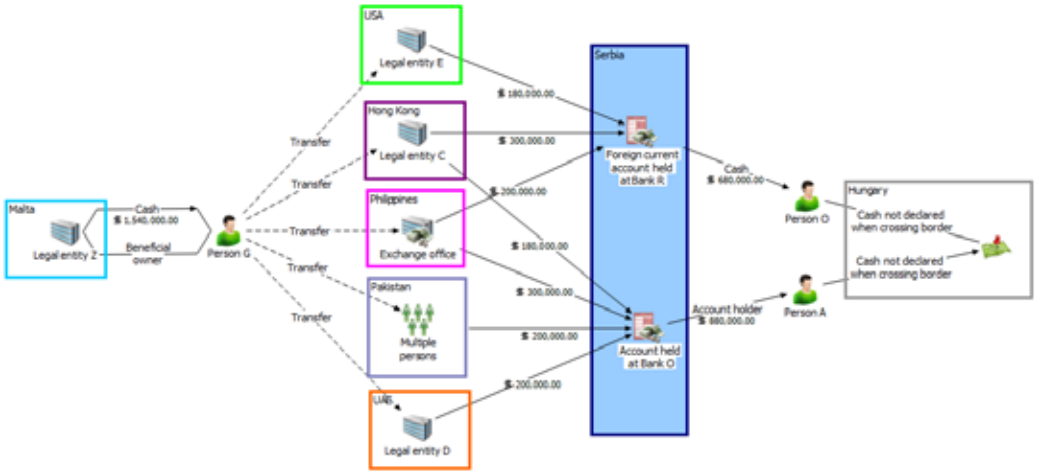
Other than the Philippines, most of the incoming transactions originated from the USA. At the request of Serbia FIU, FinCEN informed the Serbian FIU that the Miami-based City Bank NA had reported transactions carried out by individual G, totalling USD 297,942.00 as suspicious. The suspicion was triggered by wire transfers the individual sent to selected bank accounts in Serbia. Individual G had stated that the funds originated from car sales. In addition, individual G's bank account history showed numerous incoming and outgoing suspicious transactions to and from bank accounts of various persons at different locations, including Florida and Bolivia. The Miami-based bank sent STRs concerning individual G's suspected money laundering activity during the period 21 January 2009 – 16 June 2009. The Miami-based bank believed the activity of the legal entity transferring funds to individual G's bank account was suspicious, as it involved the use of cheques and wire transfers, as well as being involved in black-market peso exchange. In addition, the Miami bank was also provided with details concerning the legal entity crediting individual G's bank account. Namely, a withdrawal of funds was recorded in the bank account of the legal entity with no clear justification and no information about the expected expenditure.

In parallel, the Serbian FIU also sent a request for information concerning individual G to the FIU in Malta, who for their part also informed the Serbian FIU of suspicious activities being carried out by this person. Namely, in less than five months, individual G, who claimed to be the manager of a Malta-based legal entity, had carried out 28 transfers totalling €1,539,450. In addition, the FIU Malta also had information that the individual G withdrew money from his individual account in a Hong-Kong based bank totalling € 1,504,000. He justified all the transactions by claiming to be purchasing, allegedly, used electronic components in Hungary which he was paying for in cash and further selling in China, Hong Kong and United Arab Emirates.

The Serbian FIU sent a request to the competent Serbian authorities to obtain more detailed information on the above persons.

Further analysis undertaken by the Serbian FIU showed that the individuals involved had withdrawn the funds in cash and transported them across the Serbia-Hungary state border to the Republic of Hungary. Even though they had not declared any funds at the state border,

they claimed in a later statement to the Serbian authorities, that they transported the money to Hungary as the personal income tax obligations in Hungary were lower than in Serbia.



Given that individuals A and O did not report the frequent crediting of the individual bank accounts as income, they therefore also failed to report personal income tax. The Serbian FIU then sent a report to the Serbian Tax Administration about the incoming and outgoing transactions to/from individual bank accounts of the above individuals. In addition, in a statement to the officers of the competent Serbian authority, the individuals A and O also said that by receiving the transfers in their bank accounts and transporting the funds to Hungary, they were actually helping a friend of theirs, individual G, and that the funds had been generated from car sales in the USA. The above information obtained by the Serbian FIU, with regards to the above flows of money, i.e. the structuring and placement activities, added further to the suspicion of the stated origin of the funds.

Conclusion

The investigation resulted in the conclusion that the individuals A and O, as residents of Serbia, committed the crime of Tax Evasion. They paid a total of USD 344,000 in evaded tax.

Indicators relevant to this case

- Large cash withdrawals
- Non-resident transferring funds to foreign bank accounts
- Depositing of funds followed by quick transfer to other accounts
- Suspicious reason for transfer
- Frequent deposits by different legal entities/individuals
- Transfer of funds to various accounts in a number of countries from one account
- Suspicious description of transfer of funds

- Transfers from high-risk countries
- High quantity and volume of transactions in short period of time

9. Operation Arboria – A Ponzi Scheme (FIS, Guernsey)

Introduction

An investigation was carried out in Guernsey as a result of a joint investigation carried out by Guernsey, the United Kingdom and the United States of America with regards to a number of individuals who were associated with companies that had been providing financial investment opportunities to individuals. Individuals were initially provided with significant returns on their investment, though it was found that the companies in question had never invested the money.

It was found that the subjects under investigation were guilty of a high yield investment fraud, also known as a 'Ponzi Scheme'.

Background

TAYLOR is a local Chartered Insurer by profession, dealing in captive insurance, property transactions and risk management business in Guernsey. TAYLOR was, and still is the managing director and beneficial owner of the Jersey registered company entitled Quantum Resources Limited and the Seychelles registered company entitled Legend S.A. It was his use of these companies, together with his involvement with two additional companies; Vavasseur Corporation and Cotswold Trading Company Limited, that originally gave rise for concern.

In 1999, the Serious Fraud Office commenced an investigation into substantial and systematic frauds involving the UK resident, Michael Johns SUMMERS ('SUMMERS'). Related investigations by other UK Police Forces, in particular, Devon & Cornwall and Leicestershire Constabularies, plus the US Securities and Exchange Commission (SEC). Whilst Devon & Cornwall Constabulary focused on SUMMERS, the Leicestershire Constabulary investigation concerned a further investment fraud operated by a firm of certified accountants based in both Leicester and Nottingham, known as Dobb White & Co. This firm was operated by Shinder Singh GANGAR and Alan WHITE. The SEC investigation focused on yet another worldwide "Ponzi" scheme operated this time by Terence DOWDELL from within the United States.

Between 1999 and 2001 all three investigations overlapped, as it was discovered that proceeds from each fraudulent scheme passed through the same named accounts; Quantum Resources Limited, Legend S.A., Vavasseur Corp. and Cotswold Trading Company Limited. All the above accounts were operated under the control of TAYLOR.

With regard to the Serious Fraud Office investigation, SUMMERS obtained substantial funds from investment fraud victims. "Investors" were led to believe their funds were placed into high yield investment programs that bought and sold "Senior Bank Debentures" and "Medium Term Notes", supposedly producing returns of between 30% and 70% per annum. In reality no such deposits were ever undertaken and money obtained from the investors was used to pay returns on earlier deposits or commissions for those that introduced others to the scheme. The money was also directed to the personal use of SUMMERS and his associates, which in due course included TAYLOR.

Investigators from the Serious Fraud Office and Devon & Cornwall Constabulary travelled to Guernsey in May 2002 and interviewed TAYLOR with the original intention of using him as a witness against SUMMERS. A letter was subsequently sent by Guernsey Police to TAYLOR on 03 September 2002 concerning the money obtained by him and his companies through what he had described as the "interest free, open term loans" obtained from SUMMERS. TAYLOR was warned on both these occasions that as these funds were the proceeds of crime and he must not make any attempt to move them to other accounts or pay them away to any third party.

DOWDELL was tried in the USA and pleaded guilty to wire fraud and securities fraud on 24 June 2004 and sentenced to a total of 15 years imprisonment.

SUMMERS eventually pleaded guilty at Bristol Crown Court on 28 April 2006 to 33 counts of fraud in which he had obtained a total of USD 4,300,000. He was sentenced to a total of 4 years imprisonment.

The protracted trial of GANGAR and WHITE at Birmingham Crown Court concluded on 22 February 2008 when they were both found guilty of high yield investment fraud and on 11 April 2008 each was sentenced to 7 $^1/_2$ years' imprisonment.

The initial investigation in Guernsey focused on assisting the UK while US investigators put together their case for the 'Ponzi' scheme principals. Once the SUMMERS case had concluded, including Confiscation, a local money laundering investigation into the role played by TAYLOR in the above criminal enterprises was commenced, in particular into the movement of approximately USD 2,000,000 derived from the criminal activities of SUMMERS and others, which had passed through the Guernsey and Jersey accounts controlled by TAYLOR.

Guernsey FIU Investigation

In August 2009, the Guernsey Financial Investigation Unit began its investigation into the role played by TAYLOR in facilitating the 'Ponzi' schemes.

Following analysis of material already collated, multiple business bank accounts were identified that were used by TAYLOR to control SUMMERS' fraudulent schemes in Guernsey, Jersey and the UK. It was TAYLOR's relationship with SUMMERS that was

of particular interest, as well as the fact that TAYLOR received remuneration from SUMMERS. Once all the accounts were identified, production orders were then sworn and served on multiple local banking institutions.

A Letter of Request was sent to Jersey to request their assistance in obtaining bank statements and associated banking information evidentially. Assistance was also provided by Jersey Police Financial Crimes Unit with regards to a Jersey registered company.

Assistance was requested from the U.K. Serious Fraud Office, including access to vital papers attained during their investigation of SUMMERS. Additional assistance was also sought from other local agencies including Income Tax and the financial regulator, The Guernsey Financial Services Commission. TAYLOR was found to be the sole controller of companies registered in Guernsey, Jersey and Seychelles. A further letter of request was sent to United Kingdom Central Authority for bank account information.

Following the receipt of all information requested a full analysis was undertaken by the FIU. An offence of money laundering was identified and the case progressed with the Guernsey Law Officers of the Crown.

The FIU then applied for search warrants in November 2009 and on 15th December 2009, Customs and Police officers executed the warrants on TAYLOR's residential and business properties, led by FIU officers. Specialist IT forensic analysts were also brought in to assist with the multitude of computers and phones that were expected to be seized and also to deal with computer servers at business premises.

TAYLOR was arrested at his residential property, cautioned and interviewed on the day of the warrants. On 16th December 2009 he was charged with money laundering based on the information already gathered and what he said in interview.

The charge was amended in January 2010 from a single count of money laundering to 9 separate counts of money laundering.

TAYLOR pleaded 'not guilty' to the charges and a November 2010 trial date was set. In the interim the case was put together, which included statements and evidence being requested from overseas jurisdictions. Further production orders were served following the analysis of material seized during the warrants.

The Royal Court trial was heard over 10 days, with key evidence given by officers of the FIU, Serious Fraud Office, Devon & Cornwall Police, Guernsey Police and the Guernsey Financial Services Commission. TAYLOR was eventually found guilty on all 9 counts of Money Laundering, and sentenced in January 2011 to 2 ½ years imprisonment. This was a unanimous guilty verdict.

This was a landmark case for Guernsey as its first clear money laundering conviction. Judge Finch, residing in the case, stated the evidence was not just compelling, it was overwhelming. He stated "Guernsey is an international financial center and the subject of

continued scrutiny by worldwide regulatory bodies and any examples of fraudulent activity must be seen to be dealt with robustly." TAYLOR appealed the verdict, but the decision was upheld in the Court of Appeal in March 2011.

Confiscation work was then actioned in order to identify the benefit from TAYLOR's crimes, and Confiscation orders were initiated. This work is ongoing, however, overseas assistance has been requested from the Cypriot FIU by way of Letter of Request, all of which provided positive results. Further production orders and account monitoring orders have also been served during this process.

Indicators relevant to this case

- Using invested funds for personal use/purchases
- Moving funds from account to account without an apparent business purpose and without regard for administration costs
- Not maintaining a balance on an account to secure investor's interests
- High returns with little or no risk
- Unregistered investments
- Liberal use of investors funds for private gains
- Movement of funds from one bank account to another with no apparent business purpose, incurring charges and no profit
- Maintaining large cash balances at investment companies, while performing little to no trading
- High number of redemption requests from investors while not having enough financial means to satisfy requests
- Not being able to gain proper and timely access to investment funds
- Use of an email address as an important business address while it does not fit that of a business
- Use of a junior member in the organisation of a contract, inappropriate to the amount of money involved
- Use of false/fabricated documents and information
- Use of false email addresses and contact persons
- Use of fictitious account numbers and account balances

10. Money laundering and conspiracy to defraud – A Ponzi Scheme (FCU, Turks and Caicos Island)

Introduction

This case is about a substantial ponzi scheme[9] orchestrated and executed by Mr. David Smith where he encouraged his investors to invest into his high yielding investment scheme.

In September 2007 the Financial Crime Unit of the Royal Turks & Caicos Islands Police Force received information that Olint TCI Ltd, a company owned by David Smith, was operating a high value investment scheme out of the Turks and Caicos Islands. As a result of this information, the Financial Crime Unit of the Royal Turks & Caicos Islands Police Force initiated a proactive investigation into the affairs of Olint and its principal David Smith.

This proactive investigation was initiated with no complainants at the time as every one of Smith's investors believed in the scheme. The scheme was paying an average of 10% return per month.

During the investigation various USA agencies including the National Futures Association (NFA), IRS criminal investigation, Immigration Customs and Enforcement (ICE), Federal Bureaus of Investigations (F.B.I.) and Drug Enforcement Administration (D.E.A) were contacted and informed of our investigation. This led to the knowledge that Olint/ David Smith was the biggest Ponzi scheme outside the USA and until Bernard "Bernie" Madoff, perhaps the largest Ponzi scheme in the world.

Based on David Smith's own admission the total turnover of his scheme was in the region of USD 1,200,000,000 of which approximately USD 300,000,000 passed through the Turks and Caicos Islands (TCI).

With the assistance of the National Futures Association (NFA), investigators were able to establish the lack of trading activity and in some cases very little trading by David Smith. It was also established that the little trading done by Smith actually led to losses. Despite these findings, David Smith was consistently paying his investors an average of 10% return per month. These findings substantiated the initial belief that Olint/David Smith was a Ponzi scheme but there were still no complainants.

9. A Ponzi scheme is an investment fraud that appears to be actually paying high returns by paying the supposed returns out of victims' own capital. A typical Ponzi scheme promises investors a high rate of return in a short time. The money that is collected from investors is used to pay the return. This means the fraud can run for some time, because investors appear to be making the promised return. Early participants can profit.
   For example: Suppose the scheme promises a return of 10% a month. The fraudster simply takes investors' money and returns a tenth of it at the end of every month. The fact that investors appear to be getting the returns they were promised will encourage more people to put their money in the scheme, and even encourage the original wave of victims to reinvest. Eventually when there becomes a shortage of new investors, the scheme will run out of funds and will not be able to survive.

During the investigation it was also established that Mr. Smith was using investors' funds for his own private use. He purchased two homes and various plots of land. He also purchased a number of high value motor vehicles and had an extremely expensive and unprofitable gambling habit. Investigations also reveal that Mr. Smith instead of trading the investors' funds, was simply investing minimum amounts and moving the remaining funds from one account to another for no apparent business purpose. On one occasion USD 53,000,000 was transferred to a European Bank account over the course of a couple of days and back to the USA, simply incurring bank charges but not realising any profit.

During the investigations it was discovered that David Smith's scheme was made possible by the use of a US based Forex trading house (FX "A").

Evolution of the case

FX "A" is a futures commission merchant ("FCM") and a member of National Futures Association ("NFA") located in the USA. FX "A" was registered as an FCM on August 3, 2006 to act as counterparty to off-exchange foreign currency futures transactions with retail customers. FCMs that conduct this type of business are known as forex dealer members ("FDM") of NFA and are subject to specific rules and regulations regarding this business. Among these rules are specific capital requirements that must be met and records that must be maintained, as well as rules relating to fraud. Brokers employing FDMs to solicit retail FOREX accounts must register as associated persons ("APs") and the firm must provide NFA with a listing of all principals of the firm. Principals are defined as any officer or director; an individual who, directly or indirectly, owns 10% or more of the firm; or any individual who exercises a controlling influence over the firms operations.

On May 31, 2006 FX "A" had net capital of USD 612,000. At the time this was sufficient to meet the minimum capital requirement.

On July 31, 2006 NFA increased the capital requirements for FDMs from USD 250,000 to USD 1,000,000. Therefore FX "A" needed additional capital injected into their bank account to qualify for registration with the NFA. On August 2, 2006 FX "A" submitted a bank statement to the NFA which indicated that the firm had deposited sufficient capital to meet the new requirement. As part of the application process FX "A" submitted a Source of Assets Letter which indicated the source of capital deposited into the firm. This letter indicated that David Smith ("Smith") the owner of OLINT had deposited over USD 1,000,000 into the firm and that Smith was a 9% owner of FX "A". The Letter also named two other individuals whom each owned 45.5% of FX "A". Based on the audit conducted by the NFA it was clear that the firm's entire capital came from David Smith. NFA subsequently instructed FX "A" to list David Smith as a principal of the company due to his contribution to the capital.

Another account with FX "A" was Olint Corporation. The records for this company indicate that this company is owned by David Smith and that the funds on the account were from him. The account had approximately USD 20,000,000 with little or no trading in foreign exchange taking place. However despite the absence of trading, according to information received, Olint Corporation was still paying their customers an average of 10% return per month.

After the Olint Corporation account was questioned by the NFA the activities on the account decreased to the point where it appears to have closed. Further investigations revealed that a large amount of the funds from Olint Corporation were withdrawn from FX "A" and transferred to a new company that was formed by David Smith.

In March 31 2007, NFA changed its alternative minimum net capital requirement for FDMs from 1% of the notional value of open forex positions to 5% of the liabilities owed to customers. Considering this would encompass cash held at a FDM on behalf of the customer, in addition to positions in the customer's account, at the time of this new requirement, it appears FX "A" would be unable to meet the new capital requirement. Therefore FX "A" was contacted in late March 2007 and information was requested as to how they planned to meet the new capital requirements. FX "A" stated that David Smith had infused additional capital into the firm and that the two accounts owned by David Smith maintained large cash balances and that FX "A" would return the majority of the funds to the owners in order to decrease the firm's liability to customers. At that time these two accounts had a combined balance of USD 64,000,000.

Based on the documents and records that were reviewed, David Smith appeared to be the sole contributor of capital to FX "A". He made a contribution of over USD 100,000,000. However, according to the returns of FX "A" file with the NFA and with the Turks and Caicos Department of State Division of Corporations, David Smith was the owner of only 9% of the company.

On Thursday 26th June 2008, the financial crime unit received a Suspicious Transaction Report (STR) from a local bank in relation to Mr. Smith. According to the STR, the bank held an account in the name of a local financial institution for the benefit of Mr. Smith and his company Olint TCI. The bank and Mr. Smith had an agreement that the Olint account would maintain a minimum balance of USD 7,500,000 to protect the interest of investors. Mr. Smith subsequently requested the withdrawal of USD 5,000,000 thereby reducing the minimum account balance to USD 2,500,000. Mr. Smith informed the Bank that he needed the funds to facilitate redemptions to a number of club members who were pressing Olint for payment. The bank became concerned when it came to their attention that if there was a run on Olint the club members or investors would be unable to recover their investment. Mr. Smith then informed the Bank that he expected to receive in excess of USD 250,000,000 by the end of June 2008 to satisfy the high number of redemption requests. Mr. Smith further advised the bank that Olint had over USD 700,000,000 at a US-based forex trading firm (FX "B") that handled a large percentage of his trade. The bank became suspicious of how Olint/ Mr. Smith were unable to gain access to USD 250,000,000 out of over USD 700,000,000 in funds.

TCI Bank later received two email documentations from David Smith which he stated were sent to him by FX "B". These documentations were confirmation that Smith had indeed over USD 700,000,000 with FX "B" and that the due diligence process was delaying the receipt of the funds (USD 250 million) to repay investors.

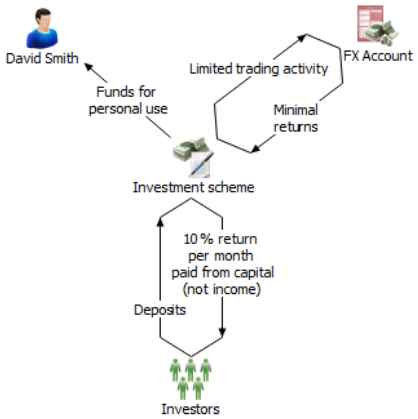
The Bank subsequently conducted due diligence on FX "B" as well as the documents they received and noticed that the email address did not fit that of a business. Also the level of person (help desk) who dealt with the matter was of a very low level within in the organisation especially considering the amount of money involved. The bank's first check revealed that the email address was not from FX "B" and eventually, with the assistance of the investigating officers, they were able to confirm that all documents were fabricated.

The financial crime unit also conducted their own enquiries as it relates to these documents and learned that FX "B" was a US registered company and that they were a registered Futures Commission Merchant with the USA Commodity Futures Trading Commission (CFTC) and a member of the National Futures Association (NFA) in the US.

The enquiries that were conducted with FX "B" revealed that the two documents in question did not originate from FX "B" and that both the account numbers and the account balance specified in those documents were fictitious.

On Friday 27th June 2008 the financial crime unit received another STR in relation to Mr. Smith from a local financial institution. This STR, indicated that Mr. Smith was the beneficial owner of Olint TCI Corporation Ltd, OLINT Corporation Ltd and Overseas Locket International Corp. This STR was repeating and confirming information in the previous STR that was received from the bank.

On Tuesday the 3rd July 2008, the financial crime unit obtained a copy of a complaint filed by the NFA against FX "A". This complaint also made reference to the findings of the audit conducted by the NFA in relation to Mr. Smith. In this complaint it was clear that Smith was doing low levels of trading activity, if any. It must be noted also that while David Smith was only making low levels of trading he was still paying consistent returns of 10% per month to investors. This type of return provided the perfect incentive for new investors to put their money into his investment scheme.



As a result of all the information gathered during the course of the investigation and the additional information received from the bank and the NFA, on the 11th July 2008 the investigating officers applied to the Supreme Court for restraint orders on the assets of Mr. Smith and his companies. USD 8,000,000 cash at the bank in the TCI and about USD 3,000,000 in properties was restrained. A further USD 6,000,000 was located in the USA.

Following the restraint order, production orders were served on all corporate entities that investigations revealed had conducted business with or on behalf of Mr. Smith.

On the 14th of July 2008 a search warrant was carried out at the home of Mr. Smith and a number of documents and computers were seized.

Mr. Smith was arrested on Thursday the 5th of February 2009. He declined to answer questions and was charged with offences as advised by counsel.

Conclusion

On the 23rd September 2010 Mr. Smith pleaded guilty to two counts of money laundering and two counts of conspiracy to defraud. He was sentenced to 6 1/2 years in prison following a plea agreement between the prosecution, the USA and Mr. Smith. He was convicted on the basis that he had defrauded and laundered over USD 230,000,000 involving over 6000 victims (mainly Jamaican) through the TCI.

Confiscation proceedings followed in January 2012.

Following his conviction, Mr. Smith was transported to the USA where he was indicted for similar offences and also pleaded guilty. He was subsequently sentence to 30 years in prison in the USA.

Indicators relevant to this case

- Higher than average return on investment
- Business funds used for private use
- Real estate and land purchases
- Lifestyle exceeds that expected with economic profile
- Movement of funds with no business rationale
- Lack of concern regarding banking fees where transactions have no rationale
- Account activity not in line with economic profile
- Use of false documentation

11. The Fiji Turtle Island Resort Case: Forgery, Fraud, Money Laundering, and Non-Conviction Based Forfeiture (FIU, Fiji)

Executive summary

The Fiji Turtle Island Resort case involves all aspects of an Anti-Money Laundering (AML)/ Counter Terrorist Financing (CFT) framework.

The case involves 84 cheque payments totalling FJD 840,000 that were subsequently laundered and as well as a range of tainted assets.

This case involved fraudulent activities conducted by Mr. Anand Kumar Prasad, the accountant of an Island Resort in Fiji from May 2006 to May 2007. Mr. Anand Kumar Prasad altered the resort's cheques which were written and authorised for payment of goods and services to the resorts' creditors.

To conceal the fraudent funds in this case, a shell company was established and cheques were paid into the account of that company. Other cheques were forged and paid into the accounts of family and friends.

The proceeds laundered from this crime were used to purchase six motor vehicles, a private property and cash which were ultimately seized.

Mr. Anand Kumar Prasad, his family members, and associates were convicted for conspiracy to defraud, forgery, uttering of forged documents, obtaining money by virtue of forged documents and money laundering.

Introduction

The Fiji Turtle Island case is a case that was reported to the Fiji Financial Inteliigence Unit (FIU) as a result of the Suspicious Transaction Reporting (STR) framework.

The case was initiated by the Fiji FIU when it received two STRs from two commercial banks. The FIU conducted its usual analysis and investigations. Within three days from receiving the STRs, the Fiji FIU disseminated its case report to the Anti-Money Laundering and Proceeds of Crime Unit of the Fiji Police Force .

Case study

Part 1- Relationship of parties involved in the STR and ultimately convicted

The fraud committed against SPOR (Fiji) Limited T/A Turtle Island Resort involved Mr. Anand Kumar Prasad and was facilitated by his family members and associates.

Family members of Mr. Anand Kumar Prasad:

- Ms. Shirley Sangeeta Singh - sister
- Mr. Arun Kumar Prasad – brother
- Ms. Bhagwati Prasad – mother

Associates of Mr. Anand Kumar Prasad:

- Mr. Deo Narayan Singh – owner of the shell company, Shahil & Shohil Grocery & Machinery Repairs
- Mrs. Atishma Kirti Singh – Wife of Mr. Deo Narayan Singh
- Mr. Reenal Rajneil Chandra – friend and brother of Mr. Reenal Praneel Chandra

Part 2 – The fraudulent scheme

Between May 2006 and January 2008, Mr. Anand Kumar Prasad (aged 27 at the time of the fraud) and the accountant at SPOR (Fiji) Ltd T/A Turtle Island Resort altered cheques that were being issued by the resort for the payment of its expenses.

A total of 84 cheques amounting to FJD 840,000 (equivalent of USD 478,000) was fraudulently converted and deposited at local commercial banks.

Mr. Anand Kumar Prasad was personally recommended by his sister, Ms. Shirley Sangeeta Singh, to the resort owner; Mr. Richard Evanson, for his employment at the resort.

Ms. Shirley Sangeeta Singh (aged 29 at the time of the fraud) was a senior prime banker at Commercial Bank A. She usually provided banking services to Mr. Richard Evanson because the business bank account of SPOR (Fiji) Ltd T/A Turtle Island Resort was held at Commercial Bank A.

Mr. Anand Kumar Prasad was a former employee of Commercial Bank A. The work experiences and knowledge of the banking system of Mr. Anand Kumar Prasad and his sister enabled them to circumvent controls at the commercial banks.

Mr. Anand Kumar Prasad was the main player in committing the fraudulent act, as well as the money laundering schemes. He had access to the cheque books and was aware that cheques for less than USD 10,000 would not be scrutinised. Mr. Richard Evanson stated that he had a lot of trust for his staff and therefore did not see the need to scrutinise cheques that were less than USD 10,000.

As part of the money laundering scheme, Mr. Anand Kumar Prasad also arranged with his friends to open bank accounts or to use existing accounts as a conduit for the altered cheques after he changed the payees' names and increased the sums payable.

Mr. Anand Kumar Prasad also had eight previous convictions for similar offences which show his crooked character.

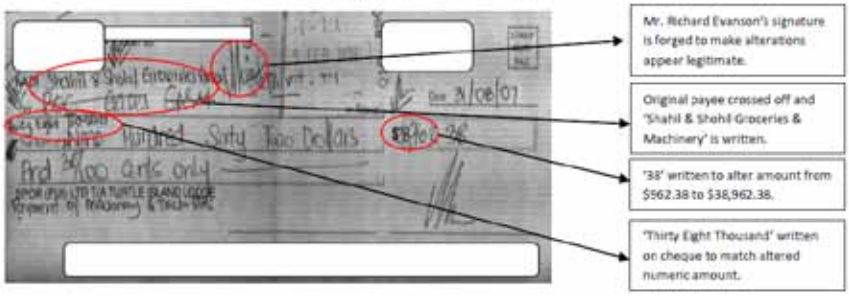
Forgery of cheques

Seventy five (75) cheques totalling USD 679,176.18 were fraudulently obtained by Mr. Anand Kumar Prasad and made payable to himself, his brother (Mr. Arun Kumar Prasad) and his associates (Mr. Deo Narayan Singh, Mr. Reenal Praneel Chandra and Mr. Reenal Rajneil Chandra). These Resort cheques were stolen by Mr. Anand Kumar Prasad and he forged the signature of Mr. Richard Evanson onto the cheques. The cheque amounts were between USD 3,000 to USD 10,000 but most of the figures were just below USD 10,000.

Alteration of the cheques

9 cheques that were written by the resort for the payment of general services were altered to the value of USD 152,719.58. These cheques were deposited into the business bank account of Shahil & Shohil Grocery & Machine Repairs.

Figure 1 – Copy of the Altered Cheque



Part 3 – The concealment

Use of a shell company

The money laundering scheme was carefully planned whereby the proceeds from the cheques were concealed through the establishment of a shell company namely, Shahil & Shohil Groceries & Machinery Repairs, on 6 February 2007. The primary business activity of this company was stated to be small groceries and machinery repairs.

Shahil & Shohil Groceries & Machinery Repairs' bank account was opened on 24 December 2007 at Commercial Bank A and 4 days later on 28 December 2007, the first fraudulent transaction was conducted on this account. The sole signatory to this business bank account was one Mr. Deo Narayan Singh (aged 39 at the time of the fraud), a former colleague of Mr. Anand Kumar Prasad at the resort.

An analysis of the business bank account of Shahil & Shohil Groceries & Machinery Repairs showed that the business was only receiving deposits (forged cheques) from SPOR (Fiji) Ltd T/A Turtle Island Resort. This confirmed that the business was established as a "shell company" to facilitate the money laundering activity.

Use of family members and associates

In addition to the proceeds from this altered cheque scheme being deposited into the business bank account of Shahil & Shohil Groceries & Machinery Repairs, the proceeds from the forged cheques were deposited into the personal bank accounts of Mr. Anand Kumar Prasad, his family members and associates.

Mr. Anand Kumar Prasad's family members and associates include:

- Mr. Arun Kumar Prasad (aged 39 at the time of the fraud) – brother 11 forged cheques = USD 105,955
- Mr. Reenal Praneel Chandra (aged 22 at the time of the fraud) – friend 9 forged cheques = USD 72,135.01
- Mr. Reenal Rajneil Chandra (aged 23 at the time of the fraud) – friend 4 forged cheques = USD 28,276.78
- Mr. Deo Narayan Singh (aged 39 at the time of the fraud) – associate 7 forged cheques = USD 63,182.44

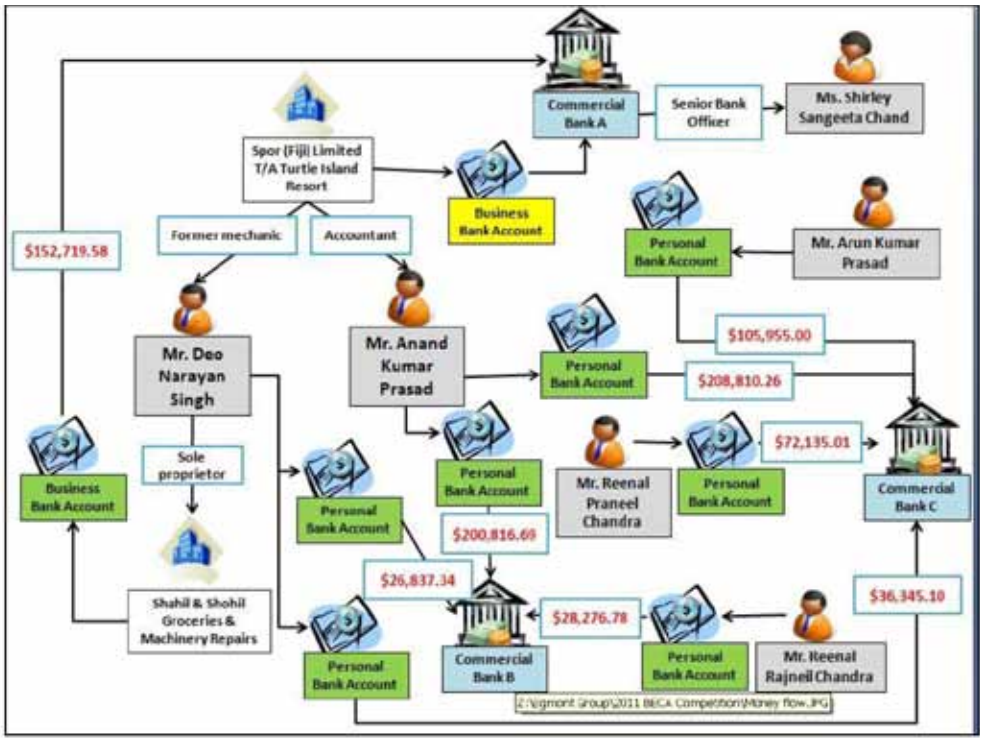
It was established by the Fiji Police that Mr. Reenal Rajneil Chandra and Mr. Reenal Praneel Chandra were friends of Mr. Anand Kumar Prasad. However during the court trial, Mr. Reenal Rajneil Chandra claimed that he only gave his account and ATM card to Mr. Anand Kumar Prasad and claimed that he knew nothing about the deposits and withdrawals from the account maintained under his name. There was no evidence to show that these two brothers directly benefitted from this forged cheques scheme.

Use of multiple bank accounts

Another important money laundering scheme was that the proceeds from the forged cheques amounting to USD 679,176.18 were deposited into multiple bank accounts maintained at Commercial Bank B and Commercial Bank C.

The use of personal bank accounts maintained at Commercial Banks B & C other than Commercial Bank A where the fraud was committed may have been a deliberate attempt by Mr. Anand Kumar Prasad to conceal the proceeds from the forged cheques.

Figure 2 – Diagram on the Money Flow into Personal Bank Accounts



Part 4 – The conversion

Money laundering

Details of case study provided in Parts 1-3 above shows various components to the well-planned money laundering scheme after commissioning of the cheque alteration and forgery.

The proceeds from this fraudulently converted cheques scheme were deposited into the personal bank accounts of Mr. Anand Kumar Prasad, his family members, associates and the business bank account of Shahil & Shohil Groceries & Machinery Repairs. The altered cheques were deposited through the involvement of Commercial Bank A's senior bank officer, Ms. Shirley Sangeeta Singh. Furthermore, she was personally involved in uplifting stop orders placed on the altered cheques by Mr. Richard Evanson. Ms. Shirley Sangeeta Singh did not hold the authority to do so.

The criminal proceeds that were credited to the respective Commercial Bank accounts were withdrawn immediately for similar credit values. These withdrawals were made in the form of cash and bank cheques to purchase six motor vehicles and a residential property.

Part 5 – The reporting of suspected fraud

This case was reported to the Fiji FIU through two STRs that were submitted by two commercial banks in Fiji. The first STR was raised on the grounds that Mr. Anand Kumar Prasad, "a self-employed individual" was depositing large amounts of cash into his personal bank account and it was believed to be sourced from his business. This STR was initially analysed for possible tax evasion related activities.

The second STR was raised on the grounds that a fraudulent scheme involving the alteration of business cheques was detected. This STR was categorised as a high priority. The Internal Fraud Investigations Team of Commercial Bank A had conducted their own investigations and detected a fraud conducted on one of their customer's bank accounts (Spor (Fiji) Limited T/A Turtle Island Resort) and the involvement of a staff member, Ms. Shirley Sangeeta Singh.

The Fiji FIU compiled a Case Report and disseminated it to the Anti-Money Laundering (AML) & Proceeds of Crime Unit of the Fiji Police Force.

Part 6 - Money laundering investigations & prosecutions

The Fiji Police Force obtained the original documents relating to the case from the relevant commercial banks. Investigations also included establishing the motor vehicle ownership records of Mr. Anand Kumar Prasad and others. Through this search, the Fiji Police were able to identify six motor vehicles that were registered under Mr. Anand Kumar Prasad and others. Investigations on the purchase of these vehicles revealed that the payments for the six motor vehicles were made by cash and bank cheques from the personal bank accounts of Mr. Anand Kumar Prasad and others.

Analysis of the personal bank accounts of Mr. Anand Kumar Prasad revealed that a bank cheque of USD 70,010 and USD 57,800 was issued to a local law firm for the purchase of a private property valued at USD 142,000. The Fiji Police Force conducted a search with the Registrar of Titles office and established that the private property was registered under Mr. Anand Kumar Prasad's mother, Mrs. Bhagwati Prasad and later transferred to Mr. Anand Kumar Prasad's friend.

Charges laid on persons involved

In 2009, charges were laid on Mr. Anand Kumar Prasad, his sister Ms. Shirley Sangeeta Singh, his brother Mr. Arun Kumar Prasad, Mr. Deo Narayan Singh, Mr. Reenal Praneel Chandra and Mr. Reenal Rajneil Chandra. The charges laid included forgery, causing payment of money by virtue of forged documents and money laundering.

Mr. Anand Kumar Prasad was sentenced for a term of six years for each money laundering offence to be served concurrently with the conspiracy sentence.

Successful restraining & forfeiture

Since a number of tainted assets had been identified, the Director of Public Prosecutions Office successfully filed a restraining order in April 2010 for seven vehicles, the sum of USD 5,191.01 which was maintained in a local bank account and a real estate property purchased for USD 142,000 that was subsequently registered under Mr. Anand Kumar Prasad's friend.

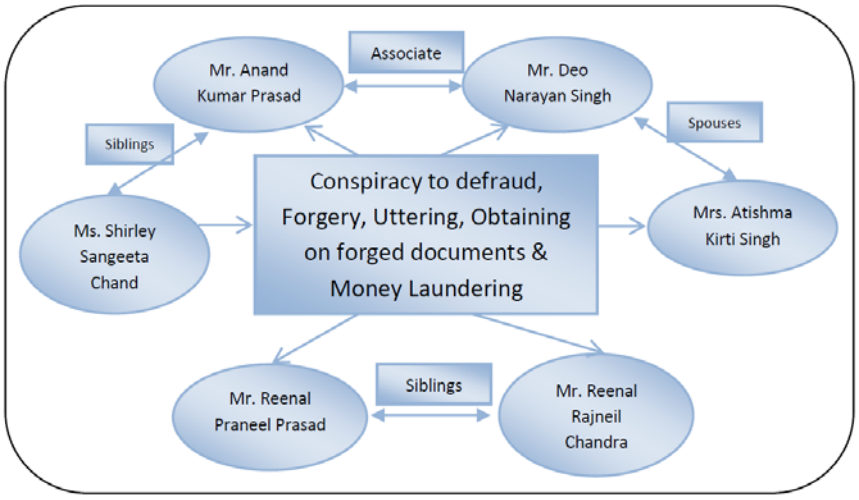
Money laundering conviction

On 15 April 2011, the court proceedings in the High Court of Fiji for the criminal case of Mr. Anand Kumar Prasad and others commenced.

On 19 April 2011, Mr. Anand Kumar Prasad, his sister Ms. Shirley Sangeeta Singh, two brothers, Mr. Reenal Praneel Prasad and Mr. Reenal Rajneil Chandra, Mr. Deo Narayan Singh and his wife, Mrs. Atishma Kirti Singh were convicted for conspiracy to defraud, forgery, uttering, obtaining on forged documents and money laundering.

The relationships between these convicted persons are shown in the diagram below:

Figure 3 – Illustration on Relationships between Convicted Persons



5. The role of Fiji FIU

Suspicious transaction reporting framework

The Fiji Turtle Island Resort case was initiated through the STR framework when only some of the fraudulent transactions that were conducted at Commercial Bank A were reported to the Fiji FIU:

- STR 1 - from Commercial Bank B on 6 November 2007 on the personal bank account of Mr. Anand Kumar Prasad.

- STR 2 - from Commercial Bank A on 3 March 2008 on the business bank account of Shahil & Shohil Groceries and Machinery Repairs Limited.

Upon receipt of this information, the investigations focused on the altered cheques from SPOR (Fiji) Ltd T/A Turtle Island Resort that were deposited into the business bank account of Shahil & Shohil Groceries and Machinery Repairs. The bank accounts of both business entities were maintained at Commercial Bank A. The Fiji FIU obtained information on this case from the other commercial banks and discovered that there were other SPOR (Fiji) Ltd T/A Turtle Island Resort cheques that were deposited into the personal bank accounts of Mr. Anand Kumar Prasad, Mr. Arun Kumar Prasad, Mr. Deo Narayan Singh, Mr. Reenal Praneel Chandra and Mr. Reenal Rajneil Chandra.

Obtain timely information from other financial institutions

The powers of the Fiji FIU under the Financial Transactions Reporting (FTR) Act to request for additional information from the financial institutions allowed timely access for investigators to proceed with the case. During the analysis of the STR, the FIU requested the other commercial banks to search for personal bank accounts maintained by the main suspects in this case, Mr. Anand Kumar Prasad and others.

The Fiji FIU was able to establish that additional stolen cheques with the forged signature of Mr. Richard Evanson were deposited into Mr. Anand Kumar Prasad and others bank accounts maintained at Commercial Banks, B & C.

This information further enhanced the scope of investigations undertaken by the AML & POC Unit of the Fiji Police Force.

Restriction placed on bank accounts

The personal bank accounts that were identified in this case all had minimal balances due to the immediate withdrawal of funds after an altered or forged cheque was deposited. However, the Fiji FIU was able to identify the personal bank account of Ms. Atisma Kirti Singh, the wife of Mr. Deo Narayan Singh maintaining an account balance of USD 17,000.

The Fiji FIU issued an "Instruction Notice" under section 25.1.h of the FTR Act to Commercial Bank B to "temporarily freeze" and to restrict any transactions conducted on her personal bank account.

The Fiji Police Force also executed a formal freezing order to restrict this bank account.

Obtain timely access to other information

The Fiji FIU has direct on-line access to the Births, Deaths and Marriages database (People National Registry System) from the Fiji FIU office. This was made possible through the signing of a Memorandum of Agreement (MOA) for information exchange between Fiji FIU and the Ministry of Justice, the line ministry for the Registrar of Births, Deaths and Marriages Office.

Having access to this database enabled Fiji FIU to establish the personal details of **Mr. Anand Kumar Prasad** and others which was vital at the intelligence development phase.

6. Domestic co-operation

Networking amongst both local and international partner agencies was essential to the successful completion of the case.

Fiji FIU & commercial banks

This money laundering scheme arising from the fraudulently converted cheques was brought to the attention of the Fiji FIU through the STR reporting of Commercial Bank A. The Fiji FIU then obtained information from other commercial banks on bank accounts maintained by the suspects. Furthermore, Commercial Bank B also complied with the Instruction Notice issued by Fiji FIU to restrict one of the suspect's bank account.

During the intelligence development process (in this case only 48 hours), the Fiji FIU was able to hold meetings with the commercial banks at very short notice.

The effective co-operation by all commercial banks was due to:

- The high level of awareness amongst financial institutions in Fiji on the role of Fiji FIU including the reporting of STRs and information exchange and
- The good working relationships that exists between Fiji FIU and commercial banks

Without the strong networking relationships between Fiji FIU and the commercial banks, the development of this case would have been limited.

Additional information that was requested by the Fiji FIU was provided by the commercial banks in a very timely manner.

Fiji FIU & law enforcement agencies

The co-operation and networking between Fiji FIU and AML & POC Unit of the Fiji Police Force resulted in effective dissemination of intelligence from the Fiji FIU on a timely basis which enabled the AML & POC Unit to act promptly on Fiji FIU's intelligence and case report.

It is also important to note that the signing of a Memorandum of Agreement (MOA) between Fiji Police Force and Fiji FIU in January 2008 enabled better information exchange and strengthened networking. The signing of the MOA also allowed for the secondment of a police officer to the Fiji FIU.

The Fiji FIU has direct access to the immigration database from the Fiji FIU office. The travel history of the suspects was obtained through this access.

The Fiji FIU has access to other databases of the Fiji Government and information on company registry, people national records etc. proved to be extremely beneficial in this case.

Law enforcement agency & office of the director & public prosecutions

While conducting investigations, the effective communication between AML & POC Unit of the Fiji Police Force and the Office of the Director of Public Prosecutions on laying of charges and the restraining and forfeiture of 'tainted properties' is commendable.

7. International co-operation

In addition to the efficient domestic co-operation amongst key stakeholders, there is a strong networking relationship between the AML & POC Unit and the New Zealand Police Force which was vital in this case.

Ms. Shirly Sangeeta Singh had boarded a flight that was bound for New Zealand with intention of absconding. The AML & POC Unit quickly communicated this to New Zealand Police Force and requested for their co-operation in deporting her back to Fiji. Within hours, the request was actioned. When she arrived at the airport in New Zealand she was put on the next return flight to Fiji on the same day. However, there were significant challenges faced by parties dealing with the case. The Fiji Turtle Island Resort case took almost three years for a successful conviction and there were certain impediments faced by the relevant agencies involved

Feedback to commercial banks

Commercial Bank A was acting on behalf of SPOR (Fiji) Ltd T/A Turtle Island Resort and was concerned with recovering the proceeds from the fraudulently converted cheque scheme.

There was a lack of feedback from the Fiji Police Force investigating officer to Commercial Bank A on the progress of the investigations. Commercial Bank A had to continuously follow up with AML Unit & POC Unit on the investigations since they were directly affected by the fraud.

Some reluctance in charging one suspect

During the early stages of the investigations, there was a setback experienced in the laying of charges against one of the key suspects, namely, Ms. Shirly Sangeeta Singh who was a key player in committing the fraud at Commercial Bank A. Infact there was some initial reluctance in charging Ms. Shirly Sangeeta Singh for "conspiracy to defraud" and for money laundering.

Non-conviction based forfeiture ruling & disposal of forfeited assets

This case involved the biggest number of tainted assets for any money laundering case and although these assets were successfully restrained, it was challenging to file a civil forfeiture order on these assets. Civil forfeiture was still fairly new to the State Prosecutors in 2008-2009, so there was some reluctance to apply for this order before the High Court which resulted in some delay of this process.

After the 'tainted properties' were restrained, there was no effective management of these assets because there were no standard operating procedures in place for orders successfully executed under the Proceeds of Crime Amendment Act 2005.

Indicators relevant to this case

- Signification alterations to cheques
  - Deposits from company account into personal accounts of family members
  - Deposits followed by immediate withdrawals
  - Deposits of large amounts of cash
  - Financial transactions inconsistent with employment status
  - Family member employed by financial institution
- Alteration of commercial cheques including original name payee transaction amount
- Knowledge of financial institution's procedures and regulations to circumvent control and supervision at commercial bank
- Lack of monitoring and internal control on financial matters by the account holder
- Lack of proper "Know your Employee" procedures, enabling the main suspect to repeat fraudulent actions for which he has been previously convicted
- Issuance of many cheques just below reporting threshold of USD 10,000

- Issuance of company cheques to self and direct relatives who have no clear business relation with the account holder
- Large cash deposits into personal bank account, with no clarification as to the source of the funds
- Use of shell company to deposit proceeds of cheques
- Concealment of criminal funds, by depositing criminal proceeds into multiple accounts held at multiple banks
- Use of an insider at a financial institution to uplift stop orders placed on the altered cheques by the account holder, while not having the authority to do so
- Immediate withdrawal of criminal funds that were just deposited in the form of cash and bank cheques
- Immediate withdrawal of criminal funds that were just deposited in the form of cash and bank cheques

12. Money laundering by fraudulent Western Union Agents (RAP, Finland)

Background

The following money laundering case was detected and investigated by FIU Finland in 2006-2007. The main targets of the investigation were two fraudulent Western Union agents who laundered the proceeds of hundreds of internet frauds by receiving and re-transmitting funds with fake identities.

Approximately EUR 1,000,000 was laundered by this criminal organisation and although the amount is not exceptionally high, the case itself was very interesting and quite challenging. The predicate offences took place in more than twenty different countries with indications of similar money laundering activities in an even greater number.

The case resulted in two high ranking members of the organised crime group being brought to justice within the interpretation of the law and coverage of the evidence playing a major role.

Predicate offences

The predicate offences were “traditional” internet frauds mostly related to cheap second hand car sales which were advertised on various internet sites. When the victims enquired about the vehicles they were told to pay (at least) the delivery costs in advance via Western Union to a “shipping agent” in Finland.

Once the victims had sent the agreed amount they reported the payment details (names, amounts, MTCN numbers) to the fraudsters. Often the fraudsters made excuses as to why the vehicle had not been delivered and the victims were asked for another pre-payment, for example; to cover logistics issues. Quite a few victims sent more money.

When the fraudsters were not able to "pump" any more money from the victims, the "seller" disappeared and contact could not be made.

Establishing the Money Laundering Network

The Romanian originated fraudsters co-operated with Nigerian originated criminals who handled the money flow of the fraud scheme. These "Money Logistic Managers" first contacted a Finnish citizen who was also Nigerian originated. This businessman ran his own company which provided cheap internet based international calls, an internet-cafe and Western Union services.

The fraudsters recruited the businessman to receive and send further money transfers. The transactions were undertaken according to the fraudster's instructions using false identities and attracted a 10% commission. They subsequently invited another Nigerian living in Finland to become a Western Union agent in order to participate in similar criminal activities.

Money transfers

Upon receipt of the payment information from the victims, the fraudsters forwarded the details to the "money logistic managers" who then gave instructions to the Western Union agents.

The instructions were transmitted by email or text messages and contained the sender's name, amount and MTCN number. Based on this information, the agents were able to find the individual transactions in the Western Union database and were able to withdraw the money with poor quality, falsified identity documents. Copies of the false identification (ID) documents were filed in the agents' archives to give the impression that the person has been seen and his ID checked.

The agents deducted their 10% commission and the "money logistics manager" provided further instructions on where to forward the funds. Once again, the amount and recipient name were sent by text to the agent, who then used a false identity to remit the funds to mainly Romanian recipients throughout Europe. These recipients are believed to act as "mules" for the real fraudsters.

It should be noted that the onward funds were divided into different amounts and sent to different recipients in order to make detection and tracing more difficult.

Detection

Western Union Nordic headquarters filed a Suspicious Transaction Report (STR) to Financial Intelligence Unit (FIU) Finland on 30th October 2006 as they had detected that one of their agents had been acting suspiciously since August 2006. The factors that lead to the suspicion were similar to indicators that had been identified in Denmark, including:

- Nigerian origin of the agent
- Significant change in the transaction pattern of the agent
- Large increase in the number of transactions
- Large increase in the average sum of transactions
- The most common source countries changed
- The most common destination countries changed

Western Union also received complaints from the fraud victims who claimed that the money they had sent had not been delivered to the right person. A couple of weeks later, Western Union also reported that another agent, who had just started in the business, was displaying similar behavior.

During the initial checks nothing relevant was found in either the FIU or police records. In order to clarify the situation, the FIU began collecting more information.

Gathering intelligence

Transactions

The information collection process commenced with a request of a list of all transactions carried out by the two agents. The transaction lists were used for two purposes. Firstly, to identify the senders and receivers of the funds in Finland and secondly, for statistical analysis to detect any potential changes in patterns. The FIU also asked Western Union Headquarters to provide copies of specific send/receive forms from the agents and deliver them to the FIU.

Senders/Receivers

There was a high number of transactions many of which included legitimate money transfers. This made detection quite challenging for the investigators as initially there was no way to separate the fraudulent transactions from the real ones, especially since it was not yet known for certain whether there were any fraudulent transactions.

The FIU checked national law enforcement and other databases and it became evident that in the majority of transactions the name and/or address details were not genuine. In a high number of transactions the persons' address was that of a hotel in Finland. The hotels were subsequently contacted but the identified names were not registered during the relevant time period. As a result of these enquiries it became evident that a lot of transactions had been made with fake identities. It was not known however, whether somebody was visiting the Western Union agents with fake identities or if the agents themselves were involved.

Statistical analysis

Statistical analysis was undertaken in order to establish the agents' activities. Initial interest was in the overall volume of the transactions:

- During the first half of 2006 the weekly total of agent one was approximately EUR 10,000 however, within couple of weeks it had increased to EUR 155,000.
- Agent two started his business from scratch and the weekly total amounted to tens of thousands of dollars almost immediately. Both figures were considered exceptionally large when compared to similar Western Union agents in Finland whose takings were normally EUR 200.

In addition, Western Union also detected a change in country pattern which was investigated further by the FIU. Activities in relation to the Congo, Gambia, the Philippines and Ghana remained steady which is considered consistent with normal legitimate transactions. For Nigeria however, transactions had doubled and the total amount of funds had tripled. Transactions to the USA had increased tenfold and Romanian transactions increased from nil to two hundred transactions and EUR 450,000.

In Finland, Western Union is typically used by immigrants to send relatively small amounts of money back to their families in their home countries. Against this background, the incoming and outgoing transactions shown above are exceptional. It was argued that "What came in went out immediately!" It was concluded that Finland was being used to rapidly funnel illegitimate money.

A change in due diligence processes correlated with the change in transaction pattern. Before the change, customer ID was checked intermittently and customers were mainly of Finnish nationality (approx. forty) with a few Spanish, Nigerians etc.

After the pattern changed, almost every transaction contained a passport number. There were two hundred and twenty customers from the United Kingdom, one hundred customers from the USA, and seventy customers from Canada to name a few. It was considered very unlikely that such a large number of citizens from the countries declared on the form, visited the Western Union agent during a couple of months.

Copies of the Send/Receive forms which were received from Western Union Nordic headquarters were the first pieces of evidence that pointed towards the agents.

The forms have two parts. The left side is to be filled in personally by the customer and the right side is filled in by the agent. On inspection, two styles of handwriting could be seen on the legitimate transaction forms whereas the transaction forms which were suspected to be fraudulent appeared to have both sides written in the same handwriting.

Furthermore, there were similar handwriting characteristics identified on dozens of different forms with different client names suspected to be written by the same person on both sides.

International requests

Several international requests were made during the intelligence phase of the case.

The first step was to ask FIU UK whether the forty UK passport numbers and names found on the transaction lists were genuine. They responded quickly and confirmed that about fifty percent of the names had been issued passports but not with the numbers provided. The remaining fifty percent were names to which no passports have been issued by UK. Therefore the entirety of the UK passport information provided in the transaction lists by the Western Union agents was false.

Victims

The first pieces of information relating to victims came through Interpol. In some countries the victims had reported to the police that they made a car deal on the internet, sent the money to a person in Finland and never received the car. The persons mentioned to be recipients of the funds were all found on the transaction lists and confirmed to be fake.

Subsequently FIU Finland sent requests with transaction details to eighteen countries to identify the senders of the "fake-receiver transactions" and the possible crime reports. For this, Interpol and Europol channels were used as well as direct contact with IC3, the Internet Criminal Complaints Centre in the USA.

The requests covered three hundred and sixty four transactions with three hundred and seven different victims and a total amount of EUR 1,100,000 averaging a total of EUR 3,500 per victim.

Some replies were received fairly quickly but the last ones arrived almost two years later, which was after the trial but just before the case was handled in the appeal court.

Surveillance

The Western Union agents were still under suspicion but the overall picture was still unclear therefore different surveillances measures were conducted.

Traditional

The first step was to use the traditional form of surveillance. Police sitting in the car outside the suspect's office, taking photos and writing notes, visiting the office as a "customer" and so on. The main result was that there were only a few customers visiting the offices during the day, but according to the transaction lists obtained by Western Union Nordic HQ a large number of transactions took place. The date/time of the transactions were compared to the police logs and it was clear that transactions took place even though there were no customers present.

Technical

The FIU obtained a court order for technical surveillance. Some surveillance devices were installed and they provided very good results.

Conclusion of the intelligence phase

The intelligence gathered so far gave a clear enough picture of what was going on. The money was coming from fraud victims around the world. The Western Union agents were then receiving the transfers with fake names and sending them on to Romania and other countries.

The fraudsters who were committing the predicate offences were still unknown, as was the method of communication used to give instructions to the Western Union agents regarding the money transfers to be picked up. However, it was believed that these questions would be answered following the ensuing arrests and house searches.

Arrests and house searches

On 27 March 2007, three offices and two apartments were raided at 8.00 am. The suspects were arrested, premises searched and 80KG of documents, various IT and telecommunication devices were seized.

Investigations

The investigation phase was divided into two sections; technical and tactical. The technical investigation concentrated on the computers and mobile phones while the tactical investigation centered on interviewing the suspects.

Computer forensics

Computer forensics provided a few emails containing instructions for money transfers (MTCN numbers etc.) and the remains of fake passports which were factored to be attached to the agent's archives as "a copy of the identified customer's passport".

Mobile Phones

The mobile phones seized during the operation provided the most striking evidence. It was established that approximately six hundred calls had been made to nineteen other countries. By analyzing the telephone traffic, the FIU were able to identify the criminal network and further interrogation of the five hundred text messages sent provided further evidence such as names, MTCN numbers etc. Some text messages contained details of the instructions given to the Western Union agents by the criminal organisation along with further information regarding how the funds should be forwarded. The instructions related to incoming and outgoing transactions that totaled EUR 1,000,000.

Based on the names and numbers in the phone memories, call and SMS logs from the phone memories and billing information from the mobile operators, it was established that the instructions for the transactions came from two common entities; "James" in Spain and "Charles" in Greece.

Telephone call analysis and link chart techniques indicated that "James Spain" was using not only Spanish and Nigerian numbers but also had a Finnish prepaid phone. Telephone record analysis further showed that on 4th October 2006 between 12:45 and 14:15 the phone was located at the international terminal at Helsinki airport. This was preceded by several calls to the Netherlands.

At 4:30 on the same day, a KLM flight departed from Helsinki to Amsterdam. Police obtained the passenger list for the flight and checked it against the Western Union transaction list. One Nigerian name was found to be the recipient of a few of the transactions. One of them was sent by the arrested Western Union agent personally with his own name and these transactions were received in Fuenlabrada, Spain. This gave reason to believe that the person in question was "James" who was giving the orders for money transfers.

Police made a new, but more specific request to KLM and they provided information about the respective ticket reservation. That information contained not only the full name of the person but also a phone number, address and credit card information. One of the higher level members of the criminal organisation was identified!

The background information gathered from the technical investigations was used during the suspect interviews. In the beginning the suspects denied everything, especially ownership of the prepaid phones which contained the incriminating evidence. The suspects claimed they had "found" the phones in their offices just a day or two before the arrest and that they had probably been left there by a client.

The story regarding the phones was proved to be wrong by the phone billing records. It was shown that in the preceding months the pre-paid phones had always been in the same location as their registered phones; in the office, at home and when travelling.

Interviews

Other claims made by the suspects were proven to be false by forensic evidence again and again. Finally, the suspects confessed and provided additional information - not only about themselves but also about the criminal organisation behind the scheme.

The organisation had been "in business" for more than ten years and they had similar Western Union agents in Spain, Greece, Ireland, Netherlands, Sweden, Germany etc. The agents received ten percent commission from every incoming transaction. The criminals behind the fraud scheme were from Romania and the money transfers & logistics were arranged by Nigerian nationals.

Based on the information gathered in the investigation phase several Rogatory Letters were exchanged with other countries in order to identify and arrest other members of the organisation and to collect evidence for the case in Finland.

The amount of information gathered during the intelligence and investigation phases was too large to be handled manually therefore all data was stored in an i2 iBase database. Transactions, phone calls, text etc. were stored in a structured format and paper documents were scanned and manually linked to the relevant entities in the database. Altogether the database contained approximately 13,000 entities and 25,000 links.

International cooperation

International co-operation played an important role in the case during both the intelligence and investigation phases.

The initial information about the fake passports was a vital element in discovering that the Western Union agents were involved themselves and not just used by other criminals. Information about the predicate offences proved crucial as without the predicate offence it would not have been possible to prosecute for money laundering in Finland.

Requests regarding three hundred and sixty four transactions were sent out and altogether one hundred and ninety eight of those were reported back as being criminal offences. That was a substantial amount and prosecution was easy to build on such a solid base.

The channels used for international information exchange were direct contact between FIUs (via Egmont Secure Web, FIU.Net), Europol, Interpol, Rogatory Letters and specific individuals.

Trial and convictions

The main question in the trial was whether all of the transactions conducted by the agents could be considered money laundering cases, or only those where the predicate offence was identified and instructions for the transactions were found to come from the suspects.

In order to prove the case, all the Send/Receive Forms were sent for forensic examination of handwriting. The forensic specialists divided the forms into three categories based on the handwriting on the customer's part of the form:

- Unlikely that anybody else but the suspect has filled in the form
- Likely that the suspect filled in the form
- Cannot be excluded that suspect filled in the form

There were no forms in the category "unlikely that suspect filled in the form"

During the trial it was shown that:

- The modus operandi for all the transactions were the same
- The suspects could not know in advance which transactions police were able to find the predicate offences

There were instructions from the criminal organisation for many transactions for which predicate offences were not identified.

The court decided that although the predicate offence was not always identified, there remained no reasonable suspicion as to whether the transactions were also criminal or not. The suspects were convicted of money laundering for every transaction and sentenced for three years and one month in prison.

Both suspects appealed against their convictions. The Court of Appeal did not change the conviction, although the three year sentence was lowered to two years six months in prison. Both suspects again appealed against their conviction to the Supreme Court but the Supreme Court rejected the applications on 23rd March 2011. The appeal court's decision remained final.

Indicators relevant to this case

- Reports of advanced fee fraud
- Nigerian origin of the agent
- Significant change in the transaction pattern of the agent
- Large increase in the number of transactions
- Large increase in the average sum of transactions
- Depositing of funds followed by quick transfer to other accounts
- The most common source countries changed
- The most common destination countries changed
- Use of false identification
- Unexplained change in agents' due diligence process

13. The misappropriation of municipal funds (Rosfinmonitoring, Russian federation)

Introduction

The financial investigation case presented herein is noteworthy due to the complexity and serial repetition of the predicate offence and related money laundering. Funds were stolen from eight different district administrations of a subject of the Russian Federation, the predicate offence alone includes more than eight successive stages, the amount of the stolen funds exceeds USD 100,000,000.

Initially, law enforcement agencies were not aware of the funds theft scheme. It was Rosfinmonitoring's participation that contributed to reconstructing the funds theft scheme and detecting new predicate offence incidents and subsequent money laundering. In the course of financial investigation, Rosfinmonitoring initiated information exchange with FIUs of several jurisdictions (USA, Cyprus, France, Luxembourg, and Switzerland) which resulted in revealing the scheme of laundering a part of criminally gained income outside the Russian Federation.

As a result of financial analysis conducted by Rosfinmonitoring in support of the criminal investigation, the number of complainants acknowledged and the amount of the stolen funds revealed has increased ten times.

Evolution of Case

Initial detection

Initially law enforcement authorities made an enquiry addressed to one of Rosfinmonitoring's territorial subdivisions stating that they had received a declaration from a former head of a municipal formation of "A" region (see Picture 1). The former head declared that the document confirming supposed indebtedness of the municipal formation of "A" region to a public utility organisation contained false signatures on his behalf and on behalf of the head of the public utility organisation.

Initial case development was conducted by a territorial subdivision of Rosfinmonitoring, though due to the interregional and international nature of the criminal activities, the case was forwarded to headquarters for further financial investigation.

Investigation revealed that members of an organised criminal group comprised of officials of the government agency of "A" region, credit institution employees and officials of municipal authorities of "A" region, had assigned fictitious liabilities (debts) to district administrations of "A" region. These liabilities were in favour of local public utility organisations in an aggregated amount exceeding USD 100,000,000.

Furthermore, via a number of subsidiary companies, public utility organisations assigned debt claims in favour of especially created fictitious legal entities with subsequent assignment of the debt claims in favour of the credit institution.

Municipal formation administrations of "A" region obtained credit institution's loans secured by state guarantees of "A" region Government and used them to repay fictitious liabilities (debts).

Funds obtained from the transactions, which exceeded USD 100,000,000, were transferred to the account of the controlled legal entity. In turn, "A" region Government, under the guarantees provided by the credit institution, repaid the loans and interest with budgetary funds.

Role of the FIU and Analysis

Rosfinmonitoring initiated a financial investigation utilizing all available sources of information.

Some financial data became available to Rosfinmonitoring due to the effective work of internal control departments of a number of banks who reported the suspicious financial transactions. Furthermore, additional requests to certain Russian credit institutions were forwarded and active cooperation with the state Deposit Insurance Agency was carried out. As a result, relevant cash flow records from account statements of the involved persons and copies of agreements covering the investigated transactions have been obtained.

We used the innovative comparative analysis techniques as follows:

- The character of payments at the middle level of the criminal scheme revealed features which pointed to the existence of other similar chains, but with other participants. As a result, nine new criminal incidents were detected
- Available software was used to load incoming (new) data that was not found in the FIU databases into an integrated data array for analysis, comparison and systematisation of all data as logical chains of events

Firstly, we carried out a data search and, through cooperation with the territory of the Russian Federation, we were able to reveal the scheme of the predicate crime. Once the criminal scheme was revealed and the location of the stolen money was detected, further work was conducted to reconstruct the money laundering scheme, to detect the final placement of the money and to determine the individuals involved.

Analysis of information received from the specified sources made it possible to reconstruct the complete scheme of the funds theft, to detect new criminal incidents and persons involved in the criminal activities.

Domestic/International Cooperation

At all stages of financial investigation, active cooperation with Russian law enforcement authorities, with both investigative and operative officers, took place. (see Picture 3). Law enforcement officers were provided with information concerning criminal activities of the persons involved, copies of documents obtained, references and financial tie schemes. We consider that the rapid dissemination of all criminal incidents should be directly credited to our FIU.

After the detection of facts relating to the partial transfer of the money abroad, as well as intensive financial and economic activities between the main suspect and a relative of theirs abroad, active cooperation with foreign FIUs was initiated. In particular, cooperation with FIUs of British Virgin Islands, Italy, Ireland, Cyprus, Latvia, Luxembourg, USA, France, Switzerland and Lithuania was conducted. Cooperation with these FIUs made it possible to reveal a probable money laundering scheme of more than USD 10,000,000 as well as the detection of assets of the involved persons abroad (see Picture 2). Also, thanks to the cooperation with foreign FIUs, valuable information was received concerning persons involved.

Disclosure to Law Enforcement for Investigation

At present, a criminal investigation is in progress based on the Criminal Code articles related to the theft of an extremely large amount of money and money laundering. The results of the financial investigation were forwarded to the Investigative Committee under the Public Prosecutor's Office of the Russian Federation (presently - Investigative Committee of the Russian Federation) for the criminal investigation.

Conclusion

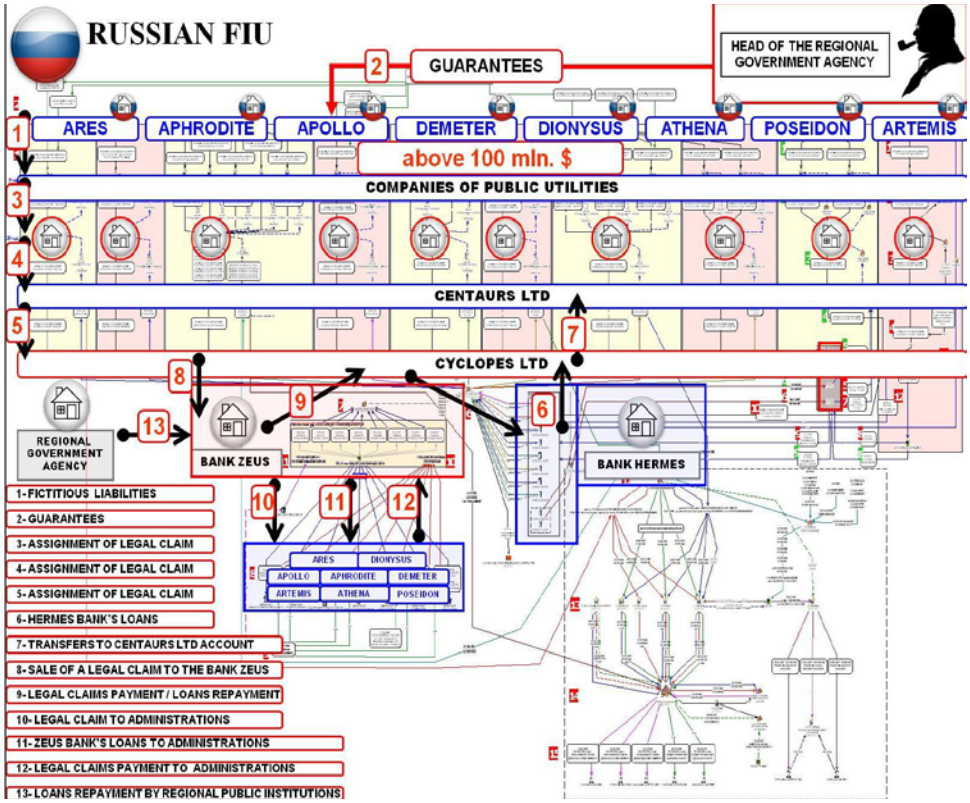
Thanks to the work of Rosfinmonitoring, it became possible to quickly reconstruct the chain of settlements and transactions related to the predicate crime. Only successful cooperation with national law enforcement authorities, credit institutions and other entities enabled us to reconstruct the complete scheme of the money theft, given that single databases do not include all data necessary to reproduce all criminal incidents concerning a certain case.

Further work enabled the FIU to determine the direction of the laundered money and its final destination. As part of financial investigation, a probable money laundering scheme of more than USD 10,000,000 abroad and more than USD 10,000,000 in the territory of Russia was reconstructed.

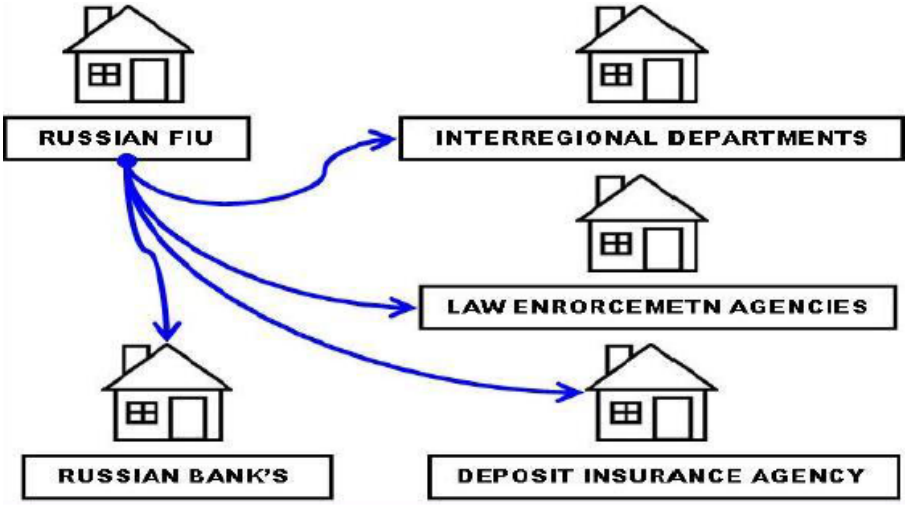
In summary

Based on the case material collated, a typology of regional and municipal budgetary funds misappropriation was developed. This was further used when conducting a number of lower-scale financial investigations. The specified typology is based on the creation of artificial debts of budgetary enterprises to public utility organisations, initiated by the latter and the transfer of this debt to companies controlled by the criminal organisers. After that, the debt was sold for real money to lending agencies, which received compensation for the specified debts from the state budget on quasi-legal grounds.

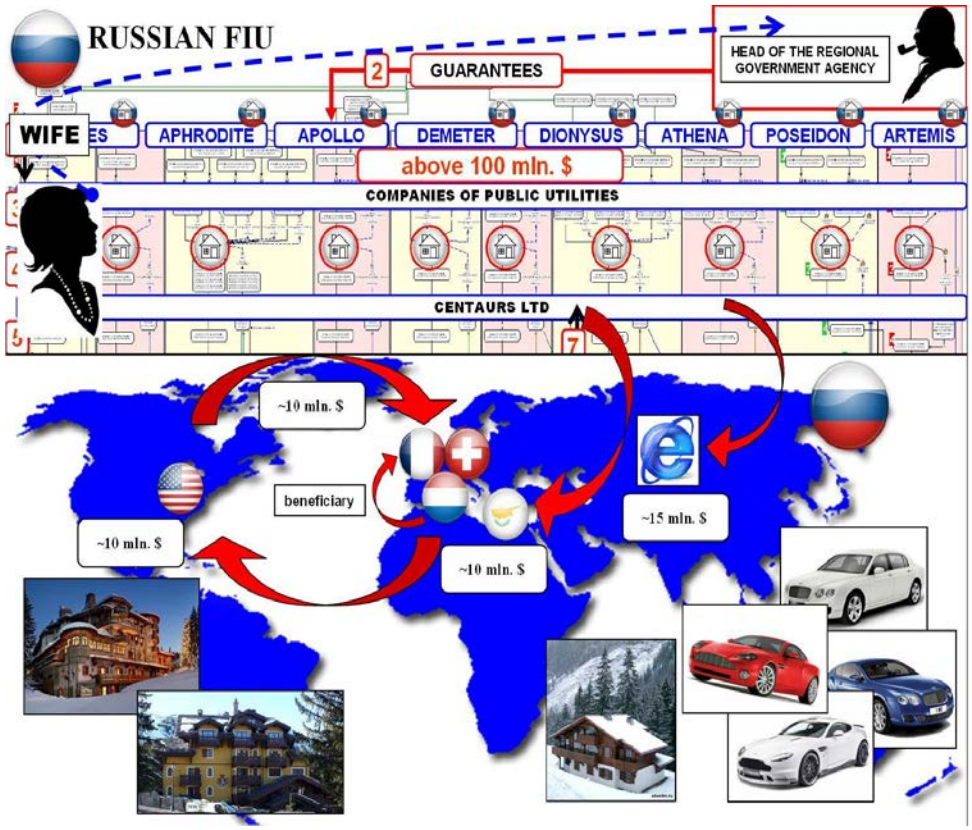
Picture 1



Picture 2



Picture 3



Indicators relevant to this case

- Use of false signature on documents confirming supposed indebtedness of high amounts
- Assignment of fictitious liabilities to government administrations in favor of public organisations for amounts exceeding millions of US Dollars
- Use of fictitious legal entities, especially created for the assignment of debt claims
- Use of a number of subsidiary companies for the assignment of debt claims, with subsequent assignment of the debt claims in favor of credit institutions
- No proper KYE performed, especially on the employees of the public utility companies, thus creating the possibility for fraud (conflict of interest of employees, fictitious legal entities, false signatures, false debts etc.)
- Complex structure of the subsidiary companies and movement of funds, making it difficult to detect

Money Laundering related to Human Trafficking, kidnapping, and Illicit Pornography

It is no surprise that criminal organisations are used to violating people's rights in order to obtain large sums of money, even if this means taking away a person's freedom. This serious violation of one of the most fundamental of rights in order to obtain illegal profits can be performed through the trafficking of people who are vulnerable because of their circumstances, into other countries and regions for sexual exploitation. Taking this into account and in an effort by the international community to prevent and counter the commission of these crimes, the Protocol to Prevent, Suppress and Punish Trafficking in Persons, supplementing the United Nations Convention against Transnational Organised Crime (the Palermo Convention), in its Article 3 defines "trafficking in persons" as the transportation or receipt of people, usually under threats, use of force or by abduction, fraud, deception or abuse of a vulnerability to achieve consent of a person having control of another one for the purpose of exploitation, which includes sexual exploitation, forced labor or slavery.[10] Likewise, the United Nations (UN) defines "sexual exploitation" as the abuse of another, either actual or attempted, for sexual purposes including profiting, either monetarily, socially or politically from such practice.[11] These offences are committed because they can be highly lucrative, with annual profits of approximately USD 28 billion, according to a report published by the Financial Action Task Force in July 2011.[12]

10. United Nations Office on Drugs and Crime (2004) United Nations Convention Against Transnational Organised Crime and the Protocols thereto http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf
11. United Nations Secretary-General's Bulletin ST/SGB/2003/13 of 9th October 2013 "Special measures for protection from sexual exploitation and sexual abuse" http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N03/550/40/PDF/N0355040.pdf?OpenElement
12. Financial Action Task Force (July 2011) Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants http://www.fatf-gafi.org/media/fatf/documents/reports/Trafficking%20in%20Human%20Beings%20and%20Smuggling%20of%20Migrants.pdf , p.16

Another way in which criminals can profit from denying freedom to a person is by holding them hostage through kidnapping for ransom. This activity has been identified in recent years as one of the main sources employed by terrorists to finance their activities. The risk it entails is considered low and the profit obtained through engaging in such activities is often high, regardless of the efforts made by the international community to cut off terrorist groups and individuals from other sources of funding.[13] According to estimates provided by the British Ambassador to the UN, Mark Lyall Grant, several islamist extremist groups, some of them affiliated to Al-Qaeda, collected at least USD 105,000,000 between 2010 and 2013 from kidnapping hostages and releasing them after payment of a ransom.[14]

In this sense, as both criminal activities described above are oriented towards obtaining monetary benefits and can be considered to be profitable, the perpetrators of these offences employ similar techniques to those that are used for other serious crimes to provide the illicit money with a legal and explainable origin.[15] Considering their common mandates and objectives of preventing and countering money laundering and financing of terrorism, financial intelligence units (FIUs) around the world can contribute to combating these events by detecting and analysing the money trails left behind by these criminal activities.

The following four cases provide us with successful examples of how FIUs have worked alongside local law enforcement agencies and foreign counterparts, to tackle criminal and terrorist groups that infringe upon the freedom of their victims for their own benefit. Three of these cases show how FIUs have conducted investigations on the illicit flows of money linked to activities of sexual exploitation of persons, two of which involve human trafficking and the third one dealing with the illicit production of pornographic materials.[16] Another case provides us with an enlightened example on how financial intelligence analysis can assist in the investigation of an ongoing offence, a kidnapping for ransom performed by a terrorist group, which provided the authorities with the elements required to locate, act against the criminals and rescue the victims alive.

---

13. Financial Action Task Force, July 2011, Organised Maritime Piracy and Related Kidnapping for Ransom, http://www.fatf-gafi.org/media/fatf/documents/reports/organised%20maritime%20piracy%20and%20related%20kidnapping%20for%20ransom.pdf, p.24
14. AFP, "Al-Qaeda groups reap $100 million in ransoms," Google News, January 27, 2014. http://www.google.com/hostednews/afp/article/ALeqM5iqLVYQJ1QEqDbvdTGI9k0hjrr4cg?docId=9324bed5-abf0-43de-a59e-4d42f538b9a8&hl=en
15. Financial Action Task Force (July 2011) Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants http://www.fatf-gafi.org/media/fatf/documents/reports/Trafficking%20in%20Human%20Beings%20and%20Smuggling%20of%20Migrants.pdf, p.7
16. It should be noticed that according to Article 223 of the Belarusian Criminal Code, the production, distribution or advertisement of materials of pornographic nature is a crime punishable with up to a three-year prison term or a fine. An English translation of the Code can be consulted through the UNODC Tools and Resources for Anti Corruption Knowledge (TRACK), at http://track.unodc.org/LegalLibrary/LegalResources/Belarus/Laws/Belarus%20Old%20Criminal%20Code%201994.pdf

These four examples represent only a very small sample of all the cases, most of which remain unknown, where the information and analysis performed by the FIU have made an invaluable contribution to the authorities' efforts to protect the rights of citizens and ensure the rule of law.

Indicators

- Setting up of companies with the alleged purpose of offering tourism or employment services in a foreign country
- International money transfers using money service providers traditionally used for remittance purposes (such as Western Union, Contakt, MoneyGram etc.) from countries with a high risk of receiving illegal traffic of persons
- The number of remittance senders is considerably larger than the number of recipients
- Remittances sent are split amongst different related accounts
- Funds received through remittances or transfers are withdrawn in cash from ATMs in short periods of time or consecutive transactions
- Money transfers inconsistent with the economic activities of the senders themselves
- Individuals receiving transfers of funds or remittances from senders with no apparent connection between them
- Reception of funds by companies registered as providers of telecommunications or internet services that receive funds supported by invoices with undisclosed or poorly described "services" concepts
- Acquisition and use of legitimate off shore companies, in order to open bank accounts for said companies in countries different to those where the companies are registered
- Use of online credit card systems, such as CC Bill, to transfer money to open accounts for the off shore companies or credit card accounts

14. Laundering the proceeds of illegal pornographic material (DFM, Belarus)

In mid-2008, the law enforcement authority verified information on the production and distribution of pornographic photo graph and video materials in Belarus.

As a result of taking proper actions, concrete persons who were involved in this activity were identified and detained; Discs, videocassettes containing pornographic pictures and films were also seized.

A criminal case was initiated against six members of the criminal group (citizens of the Republic of Belarus and other countries) based on production and distribution of pornographic materials or pornographic items.

It was established in the process of the criminal case investigation, that over a three year period a number of citizens of the Republic of Belarus and other countries, were combining to form an organised criminal group connected with the production of pornographic materials and the further realization to internet site users.

The law enforcement agency established that criminals acquired illegal proceeds amounting to no less than USD 350,000 from this criminal activity.

These funds were then laundered both inside and outside the Republic of Belarus.

In the process of money laundering, members of the organised group acquired and used legitimate off shore companies registered in a number of countries. Later, bank accounts were opened for these companies with banks that were located in countries other than the countries of their registration.

Members of the criminal group carried out financial transactions in two ways for laundering acquired criminal proceeds. Internet users acquired access to the pornography site using a «CCBill» processing center for a charge.

The processing center transferred money to the account of the payment system «Fethard» or to open card accounts and bank accounts of off-shore companies in banks.

In Minsk, members of the group were managing off-shore company accounts through the internet using multiple password systems and the secure test key technology. This was done using ATMs in Belarus and other countries. Participants also used e-money (Webmoney) and withdrew cash in specialised ATMs.

While investigating the case, the law enforcement authority submitted legal assistance requests to a number of countries for the purpose of identification and seizure of monetary funds located on accounts in banks of these countries. Information regarding the movement

of money through the accounts as well as person and account owner details for those who had received proper cards, was provided by these foreign countries.

As a result, the necessary evidence was gathered. This confirmed the laundering of funds that were a result of the criminal activity in Belarus, through settlement accounts of off-shore companies by members of the criminal group.

Moving money through the internet outside the customs frontier of the Republic of Belarus, meant they were able to conceal their activities from state authorities, banks of Belarus and other countries Disguising to the true nature, origin, location, placement and movement of funds.

A lot of photography, video, computer equipment, mobile phones and other property used in the process of the criminal activity, as well as monetary funds, were discovered during searches carried out at dwellings of the accused persons.

It was also established that organisers and members of the organised group were owners of expensive vehicles.

Considering this property was acquired out of the criminal proceeds it was considered material evidence and seized by the law enforcement authority.

Organisers and members of the organised group were accused of committing crimes envisaged by part 3 of article 343 of the Criminal Code ('production and distribution of pornographic materials or pornographic items'), by part 3 of article 173 of the Criminal Code ('underage involvement with anti-social behavior and committing crime'), and by part 3 of article 235 of the Criminal Code ('legalization 'laundering' of property acquired through crime committed by an Organised group'). The criminal case was taken to the court.

The court decided that the accused persons had withdrawn cash money using payment systems and the bank card account and then spent it at their discretion, including for the production and distribution of pornographic items.

Organisers and members of the organised group were sentenced to between three and seven years imprisonment for committing the crime of production for the purpose of distribution of pornographic materials and for underage involvement with anti-social behavior.

According to article 96 of the Procedural Criminal Code, the court decided on material evidence. In particular, special confiscation was used which resulted in confiscation to the state budget of the exempt and seized property as well as destruction of prohibited items.

Indicators relevant to this case

- Use of offshore companies
- Use of e-money/web money
- Bank accounts held in multiple jurisdictions
- Multijurisdictional company structures
- ATM cash withdrawals foreign to the company
- Withdrawal of e-money in cash
- Ownership of expensive vehicles

15. Human Trafficking - Modern Day Slavery (Rosfinmonitoring, Russian Federation)

Case description

The presented case is international in its nature and related to such a socially dangerous offence as human trafficking. The fight against this crime, regarded as a form of modern-day slavery that violates human rights and discriminates against women, requires the combined efforts of the international community, national authorities and civil society of each individual country concerned. According to the International Organisation for Migration, trafficking in humans has become global and one of the most profitable criminal business activities, comparable with drugs and arms trafficking. To combat this type of criminal activity, Russia, while using the Palermo Protocol on Trafficking in Human Beings as a minimum standard, has adopted broader legislative measures than those required by the above-mentioned international instrument.

Introduction

In the period from 2007 to 2009, one married couple from the city "K" of the Russian Far Eastern Federal District (FEFD) set up a company called "W Ltd" with the goal of cooperating with foreign employers in the areas of culture and arts. In reality, however, they were engaged in the trafficking of Russian citizens abroad, mainly to Mediterranean countries, for sexual exploitation.

In May 2010, the law enforcement authorities in FEFD initiated a criminal case under paragraphs "a" and "d" of Part 2 of Art. 127.1 (human trafficking) of the Criminal Code of Russian Federation (CCRF) with reference to the establishment of a human trafficking

channel disguised as an employment arrangement for people seeking jobs in Europe and Asia. In October 2010 another criminal case under paragraph "c" of Part 3 of the same article was initiated and on Jan 31, 2012 it was referred to the court.

Case development

Initial detection

The primary indicators of the crime were introduced in September 2008 by the territorial directorate of the Ministry of Interior RF in the FEFD (MI FEFD) with an enquiry on Mrs. N. Another piece of factual information came with a request made by the Border Department of the Federal Security Service of Russia in Territory "K" and Autonomous Region "J" in respect of law enforcement officer Mr. N (Mrs. N's husband), who had been suspected of corruption.

Role of the FIU analysis

An initial check against Rosfinmonitoring's federal database revealed that in June 2008, Mrs. N made exchange transactions with U.S. dollars and deposited funds to the account of her company 'W Ltd' as payment for services related to overseas employment.

The proposed hypothesis was that wife and husband N had been receiving funds from abroad, possibly via Western Union remittance system, and investing part of the money into the business they owned.

The collation of information on the possible involvement of husband and wife N in human trafficking received from the MI FEFD and the data found in Rosfinmonitoring's federal database resulted in the launch of an in-depth financial investigation aimed at verifying the proposed hypothesis.

By using its powers to request information from public authorities and credit institutions, as provided by the regulations of the Government and the Central Bank of the Russian Federation, the relevant regional office of Rosfinmonitoring in FEFD has requested and subsequently received data on the bank accounts, financial transactions and money-based relationships of the subjects under investigation.

Among the achievements of the presented case development was the close interaction between the initiators of the above requests aimed at preventing any illegal attempts by Mr. N to influence the course of the investigation. As a result of their efforts, in 2009 Mr. N's position as a law enforcement officer was terminated and he was fired.

Analysis of the data obtained from credit institutions revealed that in the period from 2007 to 2009 the above mentioned individuals had been receiving funds transfers from residents of Israel, Greece, Italy and other countries via Western Union, Contact, MoneyGram and Leader remittance systems.

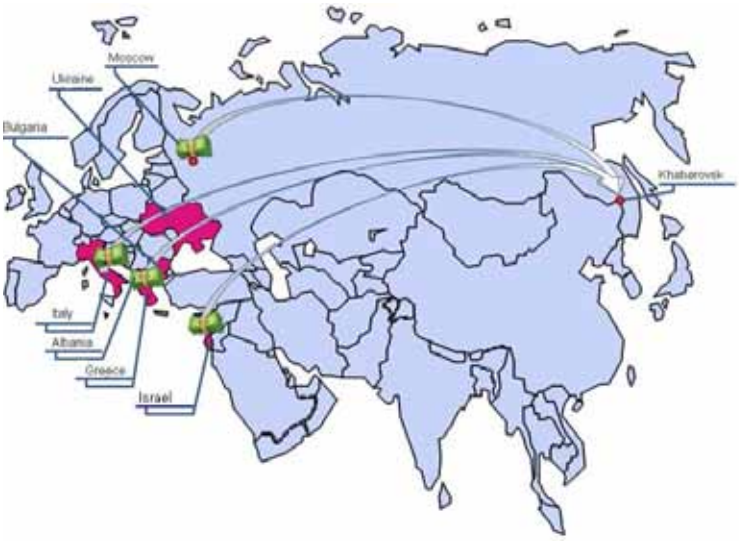
Information about the money-based relationships of husband and wife N and their associates with individuals residing in Israel, Greece, Cyprus and China, as well as data on the depositing of funds to the accounts of "W Ltd" was disclosed to the MI FEFD under Art. 8 of Federal Law 115-FZ* and has significantly contributed to the case development. The officers of the MI FEFD have used the initial disclosures in the proceedings related to the initiation of a criminal case under Art. 127.1 of the CC RF and for additional qualification of offence under Art. 174.1 (self-laundering) of the CCRF.

Domestic/International cooperation

The entire financial investigation was conducted in close collaboration with the officers of the MI FEFD, Border Control Department of the Federal Security Service of Russia in the Territory "K" and Autonomous Region "J", Investigation Department of the Investigative Committee of the Russian Federation in FEFD, and Investigation Department of the Investigative Committee of the Russian Federation in the Territory "K". There was an ongoing exchange of information on the newly identified subjects of the financial investigation.

Thus, in February 2010 the MI FEFD forwarded information on the new subjects of the case, including Miss X, Miss Y, and Mr. Z - the associates of the husband and wife N.

In order to obtain information on the partners of husband and wife N, Miss X and other individuals in Israel, Greece, Republic of Korea, Bulgaria, Lithuania, Moldova, Romania, Italy and Ukraine, in 2009-2010 requests were sent by Rosfinmonitoring to the FIUs of these countries.



The FIUs of Bulgaria, Ukraine and Romania supplied information related to the issuance of passports to certain individuals.

In November 2009, a reply was received from the FIU of Greece confirming a link between a local criminal gang, engaged in human trafficking and exploitation of women in night clubs, and the Russian company "W Ltd" owned by Mrs. N. It was also reported that in July 2009 the police department in city "A" of Greece had neutralized the said gang. In January 2011, the FIU of Greece responded positively to a request for information on the revenues of the subjects under investigation.

*Basic AML/CFT Law in RF.

In July 2011, Rosfinmonitoring shared with the FIU of Italy the details of several Western Union remittances sent to the subjects' accounts in Russia by individuals from Italy. The agency was also granted permission to disclose this information to the Italian law enforcement authorities. The information received from foreign FIUs has made it possible to reveal the scope of criminal activities.

Dissemination to law enforcement authorities

The information disseminated by Rosfinmonitoring to the law enforcement agency of FEFD has founded the evidence for proving that between November 2007 and 2010 Miss X and Miss Y, under the pretext of helping to secure jobs as dancers, trafficked to Greece a number of girls for providing sexual services in local nightclubs. In Moscow the girls were patronized by Mr. Z, who first accommodated them in a hotel, then escorted them to the airport and afterwards received remuneration with some of the money derived from this criminal activity. The "host party" was paying for the "services" by transferring funds in foreign currency from Greece to Russia via money remittance systems such as Western Union, Contact, MoneyGram and Leader, as well as via a number of the city "K" banks. The receivers of the transfers were either husband and wife N, or Miss X and Miss Y, or their relatives and friends.

Case closure

The information provided by Rosfinmonitoring has helped the Investigation Department of the Investigative Committee of Russia in the Territory "K" to initiate in October 2010 the criminal case under par. "c" of Part 3 of Art. 127.1 (human trafficking) of the CCRF. It has contributed also to the detention and prosecution of the organised criminal group members.

The detained members of the organised criminal group were linked to a transnational criminal community specialising in human trafficking. It was led by Rami Saban, a well-know Israeli criminal boss, who was convicted for human trafficking by the Tel-Aviv District Court in January 2012.

A total of fifty one women, five of whom were still underage when sold into sex slavery, have been recognized as victims of trafficking. In collaboration with the Greek police, the law enforcement agency in the FEFD managed to release a resident of the Territory "K" from sex slavery.

Furthermore, the information gathered by field investigators was used to launch an extensive police operation in Greece, resulting in the discovery of a large criminal group engaged in the exploitation of Russian citizens. As a result of this operation, the activities of ten strip clubs were exposed, more than one hundred and eighty people were penalised, and 19 members of the group were arrested.

The evidence gathering process involved five hundred interviews with witnesses, over one hundred searches and seizures, more than fifty different expert examinations. The criminal investigation lasted more than two years and numbered one hundred and fourty one volumes.

The criminal case against the Russian participants of the criminal group has been referred to court in 2012 and they were facing long prison terms for the multiple offences committed. For example, par. "c" of Part. 3 of Art. 127.1 of the CCRF (trafficking human being outside Russia committed within an Organised criminal group) provides for a punishment of up to 15 years imprisonment. The investigation against other individuals involved in the criminal case under paragraphs "a" and "d" of Part 2 of Art. 127.1(human trafficking), as well as under Art. 174.1, was still ongoing.

Conclusion


ПРОИСШЕСТВИЯ | ДАЛЬНИЙ ВОСТОК 12 ЯНВАРЯ 2011, 11:02

В Хабаровске поймана банда, поставлявшая дальневосточниц для секс-услуг за границу

ПРОИСШЕСТВИЯ

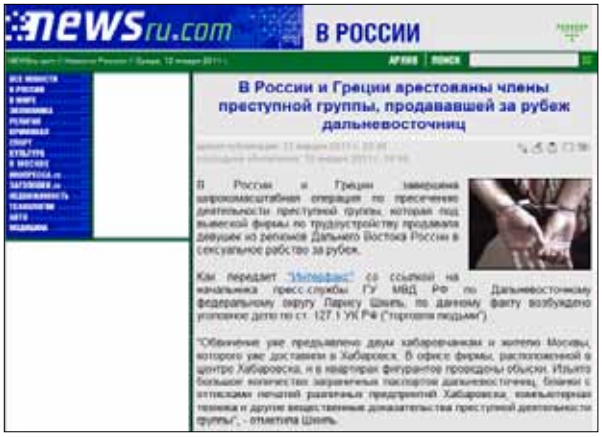
- В Благовещенске горел мебельный склад
- Караван судов в Охотском море прошел самый сложный участок
- На Сахалине прогнозируют сход лавин

Работорговцы открыто проводили набор девушек в офисе в центре города

В Хабаровске пресечена деятельность фирмы, которая как минимум три года занималась работорговлей. Международная преступная группа, состоящая из граждан России и Греции, поставляла девушек для интим-услуг за границу. Операцию провели сотрудники Главного управления МВД России по Дальневосточному федеральному округу совместно с коллегами из Департамента уголовного розыска МВД России.

Трем лицам предъявлено обвинение. Один из подозреваемых в причастности к совершению неправомерных деяний на днях был задержан в Москве и доставлен в Хабаровск.

The dissemination of financial intelligence by Rosfinmonitoring to the law enforcement agencies in FEFD under Art. 8 of Federal Law 115-FZ has clearly demonstrated to the investigators and prosecutors the scale of the activities and sophisticated techniques applied by the criminal group participants, contributed to the initiation of a number of criminal cases of which have been referred to court.


newsru.com В РОССИИ

В России и Греции арестованы члены преступной группы, продававшей за рубеж дальневосточниц

Additionally, the materials of this case formed the basis for developing the typology that reveals the use of international remittances for generating and moving criminal proceeds gained from the sale of women from Russia to other countries for sexual exploitation.

A group of related entities regularly receives remittances from countries Russian women are often being trafficked for sexual exploitation. Remittance amounts tend to be small, between USD 2000 and USD 6000 each. Some individuals connected with a Russian-based company offering tourist or employment services abroad are sure to be found among the beneficiaries of the scheme. The number of remittance senders is significantly larger than the number of recipients. Senders can be divided into two categories: men with foreign names and surnames, and women with Russian names and surnames.

Indicators

- Money received from overseas transfers via money remittance systems such as MoneyGram, western union etc
- Money is received from countries where Russian women are known for being trafficked for sexual exploitation
- One of the suspects has previous convictions for corruption
- There are parties in the operation who are under investigation by a foreign entity
- The number of remittance senders is significantly larger than the number of recipients

Organised Crime

Today there are many definitions of organised crime. However, until the 1980's organised crime referred to just one group in particular: The Mafia. Although this infamous group of American Sicilian criminals, made famous by the media for illegal activities such as the sale of liquor, gambling, prostitution, stolen goods as well as other criminal services, were prolific. It is important to note that organised crime has always existed, it just didn't attract the attention of the media and the public at large in the same way. With advances in communication, technology and ever increasing globalisation, organised crime has become a global problem which transcends different cultures and geographical borders. The need for investigating authorities to mirror the organised crime group structure, working together with multiple organisations within and across multiple jurisdictions just like the organised crime group themselves, has become essential.

Organised crime affects every country, with global revenues of over a trillion dollars each year. These vast sums of money can compromise legitimate economies and are often used to fuel corruption with the purpose of influencing political decision making.

The illicit drug trade is the most profitable trade, though organised crime groups are also involved in a broad spectrum of criminal activities including fraud, financial crimes, illicit firearm trade, and smuggling of anything from people to restricted goods. Generally, organised crime groups are diverse and flexible with ever increasing sophistication as they seek to exploit legitimate activities for criminal purposes and find new markets for established illicit activities.

They will often use professional facilitators who have specialised knowledge and expertise to exploit loopholes and find opportunities to assist criminals to launder their funds and give them the appearance of legitimacy.

The activities that may indicate money laundering or the financing of terrorism by organised crime groups can include any indicators related to any of the criminal activities that may be associated with the criminal group.

The first case in this chapter was the winner of the 2013 BECA and shows how the financial intelligence unit was able to find linkages between criminal groups when even the criminals themselves where unaware of the identity of their associates.

In fact, in each of the following cases, the effectiveness of following the money trail to detect that activities of organised crime networks is demonstrated.

Indicators

- Use of foreign banks
- Use of foreign currency
- Use of nominees, fronts, or other devices to hide the ownership of assets, businesses or bank accounts
- Known criminal associations
- Deposits followed by immediate transfers to countries of concern
- Deposits of large amounts of cash
- Payment of air tickets by third party
- Large cash withdrawals
- Interconnection with seemingly independent businesses
- Use of "ghost employees" by businesses
- Presence of "silent partners"
- Ownership of hidden assets

16. El Loco Barrera - Colombian Narcotrafficker (UIAF, Colombia)

Background

The Financial Information and Analysis Unit (UIAF) of Colombia, based on its Systemic, Wide and Bidirectional Model (SAB, for its Spanish-language acronym), and with the cooperation of national intelligence agencies, foreign intelligence agencies and a European FIU, managed to consolidate a case. This was based on the development of five cases that date from the year 2011, where the link was the inclusion of natural and judicial persons, purportedly front men and lieutenants of Daniel Barrera Barrera, alias "El Loco Barrera".

Daniel Barrera Barrera, alias "El Loco Barrera", is a Colombian narcotrafficker captured on 18 September 2012 in Venezuela, in an operation that was coordinated by the National Police from Washington DC, with the aid of the Venezuelan and British governments. Alias "El Loco Barrera" is considered one of the greatest narcotrafficking "capos", who had his main centre of operations in the Oriental Plains of Colombia (Llanos Orientales) and was one of the most-wanted "capos" of

all times. He was one of the most important chiefs of the BACRIM (Emergent Criminal Bands at the service of narcotrafficking) and did business with the Colombian Auto-Defense Forces – AUC and with some of the fronts of the Revolutionary Armed Forces of Colombia – FARC.

Due to the complexity of the cases and as a result of the sources of information, the UIAF managed to collect, in one single case, information related to the criminal organisation. The actors were people who acquired and managed goods through the constitution of front companies, derived from narcotrafficking, which were hidden under the name of third parties and whose real owner was "El Loco Barrera".

These people exercised their criminal activities in different parts of the country, without knowing each other. Nevertheless, their main link was with front men and the lieutenants that worked for the great capo "El Loco Barrera".

As a result of the five cases, the UIAF detected, through its financial analysis, six hundred and twenty nine immoveable goods for possible asset forfeiture, up to a total value of USD 146,294,000,000 Colombian pesos, which is approximately equal to USD 82 million.

Introduction

The UIAF, since November 2010, began a structural change in its manner of operation, with the aim of directing the fight against the crimes of money laundering and financing of terrorism (ML/TF) in an integrated manner. For this reason, it incorporated a model of operation that is known as SAB (Systemic, Ample and Bidirectional). This system is based on the standard international anti-money laundering and financing of terrorism system, but adds new sources of information and involves other actors, articulating them all. The aim of the model is to strengthen the capacity of the Colombia State in obtaining concrete and effective results in the prevention and detection of criminal activities related to the crimes of ML/FT, as well as supporting the investigations that lead to future judicial processes and prosecutions.

For the above reason, the present case is the result of the practical application of this new approach, based on sources of information from reporting sectors, open source information and an important inter-institutional cooperation through the exchange of information and data verification with national and foreign intelligence agencies.

Based on objective reports and other reports (Suspicious Transaction Reports – STR), and working tables carried out with national and foreign intelligence agencies, a financial analysis process was carried out which lead to the identification of one hundred and ninety seven natural persons, who belong to criminal organisations and illegal armed groups, who participate in Organised crime in different parts of the country and who, through thirty three front companies, acquired immoveable goods that were a product of resources derived from narcotrafficking and apparently had no relationship among one another, but who had in common that they were lieutenants and front men of one of the most wanted capos, alias "El Loco Barrera".

At the center of these individuals, a network dedicated to the transportation of cocaine abroad through logistics and aviation companies was identified. The money derived from this illicit activity was laundered through companies dedicated to livestock farming and through the same logistics and aviation companies.

Evolution of the case

Initial Detection

Sources of information:

1. Suspicious transaction reports (STRs)

Between 2008 and 2010, the UIAF produced different financial intelligence reports that were delivered to the Attorney General's Office. These reports were developed as a result of information contained in suspicious transaction reports that were received by the UIAF from a number of different reporting sectors. The STRs provided information on transactions and red flags related to people who, in open source information, had been identified with links to narcotrafficking.

Subsequently, the UIAF received STRs on people who were reported to have carried out financial transactions that deviated from their expected economic profile. Nevertheless, there was no knowledge within the unit at that time as to whether these people were linked to narcotrafficking or criminal organisations, or whether they were known to judicial authorities. However, there was a suspicion that they could be front men or lieutenants for alias, "Loco Barrera".

2. Intelligence information from a national agency

Through an initial working group table carried out with a national intelligence agency, the UIAF obtained data about the identification numbers of eight people who apparently have registered links to illegal armed groups or criminal bands. There is no additional information or knowledge linking these individuals to particular criminal groups.

3. Information from a foreign intelligence agency

Through 'working group tables' carried out with a european intelligence agency, the UIAF obtained data about three people who registered direct links to "Loco Barrera". This foreign FIU requested UIAF's cooperation in finding financial information related to these individuals and to assist in the development of a case.

4. Open source information

Through open source information including press reports, the UIAF was able to establish links between people who registered a relationship with criminal bands associated with "El Loco Barrera" and who are linked to narcotrafficking.

The UIAF's role and analysis

Methods to collect information related to the case:

Based on the information first obtained through the aforementioned sources, the UIAF undertook some research to determine the financial profile of the reported people and their relationships with each other as well as possible link to "El Loco Barrera" by performing a search of their own database plus other databases that they had access to.

In the same manner, the UIAF requests supporting documentation from the reporting entities with regards to customer due diligence.

Analysis techniques and processes

The analysis techniques used by the UIAF included:

- Revision of the data: to corroborate or disclaim the initially received information
- Observation: through research into different databases, obtain information that would not be detected otherwise in isolation
- Document revision and analysis: establish the financial profile of those reported in STRs and attempt to determine whether there were financial links among the people identified in the case, based on supporting evidence
- Focus of analysis: center the analysis on financial intelligence, compared to the profile of those about whom reports were received
- Trace the financial information through research and cross-checking information contained in databases

Furthermore, and importantly, the UIAF used working group tables with different intelligence agencies (national and foreign) as a technique in the development of the case. UIAF also exchanged information with a European financial intelligence unit to obtain additional information based on the findings made by the UIAF up to that point.

Analysis process:

Entries:

Data received through suspicious transaction reporting and working group tables with intelligence agencies, as well as open source information.

Activities:

- Research into data-bases available at the UIAF and those to which it has access
- Request supporting documentation from the entities that are obliged to report to the UIAF, as well as from other entities.
- Financial study of the case based on the financial research and additional information sent by the reporting entities upon request, in light of the financial movements, economic profile and other information contained in the UIAF databases.
- Graphical representation of the financial analysis.
- Determination of links through the financial transactions that were performed, as well as through the supporting documentation sent by the reporting entities.
- Working group tables with the intelligence agencies, in order to expand information based on the findings found throughout the development of the case.

Outputs:

The UIAF presented the case to the Attorney General's Office and subsequently accompanied and supported that authority's Unit on Money Laundering and Asset Forfeiture in understanding the case. Furthermore, the unit worked jointly with other national and foreign intelligence agencies and cooperated with a European FIU, which collaborated through the verification of information.

Development of the case and the UIAF contribution in that development

The case was consolidated into five cases developed from the year 2011, Due to the complexity of the cases and as a result of the data received through the STRs as well as other intelligence, the UIAF managed to collect in one single case the financial information extracted from the available databases, as well as the identified immoveable goods, pertaining to a group of people who apparently belong to criminal organisations. The people seemingly do not know each other, but are nevertheless linked by being possible front men or lieutenants of alias, "El Loco Barrera", and by performing their illicit activities in different parts of the country.

Through the cross checking of databases, the UIAF was able to establish the rationality of the information obtained. It was then able to establish the financial profiles of the reported people, with the aim of directing the analysis so that information with regards to properties that could be subject to asset forfeiture could be identified.

The main sources of information were:

Suspicious Transaction Report – STR: reception at the UIAF of information on people who perform financial transactions that deviated from the economic profile.

National and foreign intelligence agencies: obtainment of identification numbers belonging to eleven people who were possibly linked to the organisation which "El Loco Barrera" heads.

Open source information: press reports on people associated with "El Loco Barrera".

Based on the data submitted by the national intelligence agency to the UIAF jointly with a foreign intelligence unit, as well as the information the UIAF received from STRs, the unit proceeded to verify the likelihood of the information, corroborating at a minimum the identification numbers. Subsequently, the unit accessed its own databases in order to firstly establish the existing financial information and the possible links among the initial group of people of whom they had received information. The aforementioned data was then complemented through research into the databases that the UIAF had access to, which allowed the unit to specifically identify links, vehicles, ownership of moveable and immovable goods, cash transactions, notary acts etc. The results of this then allowed UIAF to prioritise the need for further requests that the UIAF would have to make to other institutions based on the cooperation agreements it has with them, or based on the legal instruments at its disposal. In this way, other companies and natural persons who had links with the initial subjects were identified by UIAF.

With regards to the latter group of people, the UIAF was able to establish the details of their participation in the societies identified as legal representative, members of the board of directors, associates and fiscal supervisors. The financial profile of all subjects was also established.

The information and analysis that was being generated in the development of the case, was represented in graphical form, through the tool Analyst's Notebook.

After the information requests were prioritised, the requested information from the reporting entities was collected; the new information was then analysed and added to the case. This fed the "grafo" (graphical representation), which reflected links on the following types of transactions: immoveable goods, cash and participation in companies, among others. The graph not only contained information on the initial group of people, but also on natural and judicial persons. As as a result of the analysis performed, these people were identified as natural people belonging to criminal organisations and illegal armed groups that carried out criminal activities in different parts of the country. Through 33 front companies, these people acquired immoveable goods and products of resources derived from narcotrafficking.

At the center of these people, a network dedicated to transporting cocaine abroad through logistics and aviation companies was identified. The money received through the illicit activity was laundered through livestock farming companies and through the same logistics and aviation companies.

After formulating the hypothesis, analysing a significant portion of the information and having a well-funded, solid case, a work plan was agreed upon. This work plan was agreed to by all agencies involved in the case including UIAF, the Attorney General's Office and the members of the local and foreign intelligence agencies (the agencies that provided the initial information). The aim of this collaborative approach was to ensure that all members of the inter-institutional group participating in the case met each other, the documents that supported the hypothesis and the network of links, were presented. This allowed for effective information exchange among the different actors, who together verified the natural and judicial personas involved in the case.

As soon as the information exchanged was analysed and the case was developed at a 95% completion level, a new meeting was convened among all the inter-institutional actors and the UIAF presented the case orally. The precedent of a previous encounter among the same actors (entities), facilitated comprehension of the case. The case was presented and explained with all the collected and analysed information, which included the links between the people and companies, the properties, vehicles and financial information that demonstrated an unjustified asset increase among the people analysed. The aim of finding the greatest number of properties was to include these in the asset forfeiture processes that was to carried out against the organisation headed by Daniel Barrera Barrera, alias "El Loco Barrera".

The UIAF's ability to request information from different sources came from the fact that, by law, the Unit has the capacity to override legal, exchange and tributary secrecy, a faculty that allows it to optimize its analyses and case development processes and times.

Contribution to the investigation

The UIAF contributed to the development of the case in the following aspects:

1. In the sphere of joint cooperation among state and international agencies, a working group table was first carried out, during which initial pieces of information were shared. The UIAF was then able to begin finding and linking companies and people, who registered an asset increase and high levels of property acquisition that needed to be justified. Some of these people were linked by registered transactions that were in cash or through societies or goods, with people who had already been identified as front men or lieutenants of alias "El Loco Barrera".

2. The UIAF instructed and trained members of the judicial people, members of the inter-institutional working group (UIAF, Attorney General's Office and the National Police's Technical Investigation Corps – CTI, for its Spanish acronym) of the progress

of the development of the case. This ensured that the line of investigation produced effective and precise evidence necessary to seize assets including various immoveable goods belonging to the criminal organisation.

3. The UIAF performed all the tracing of the financial flows of the criminal organisation and the network of front companies at its service, in order to determine the amount of laundered money as well as precisely determining the front men at the service of the criminal organisation. This then allowed the identification of the investments that had been carried out by the criminal organisation.

Finally, the significant contribution by the UIAF to the present case is the result of the new approach (under the Systemic, Ample and Bidirectional working model), which has directed the UIAF towards the process of case development and disclosure, through the conformation of working groups with national and international intelligence and judicial organisations, as well as collaborating with foreign FIUs, in this case one specific European FIU. The unit's new approach is a formula that in this case demonstrates that it is efficient and effective in contributing to the fight against criminal organisations and cooperating in the support (from an intelligence perspective) in the judicial processes that ensue from the cases.

National and international cooperation

A working group made up of the UIAF, Attorney General's Office and the National Police's Technical Investigation Corps (CTI) was created. This group received the support of national and foreign intelligence agencies, as well as a European FIU. The team defined with clarity each of its roles: one group (UIAF and CTI) dedicated itself to the study of the financial operations and economic assessments of each of the people involved in the case, with the support of a European FIU; and another group focused on investigation and collection of evidence on the case (CTI and national and foreign intelligence agencies). The interconnection and joint collaboration made possible that the process of analysis was precise, effective and strong. This allowed the initiation of various processes of asset forfeiture of the goods and resources of the organisation headed by alias "El Loco Barrera", a process currently underway, under the direction of the Attorney General's Office, with the support of the UIAF.

Case disclosure

The UIAF, in fulfilling its legal obligations, communicated possible cases of money laundering and/or terrorism financing, through the verbal disclosure of financial intelligence to competent authorities, containing the information received and consulted in the databases available to the UIAF.

Equally, in fulfillment of its mission, the unit communicated to the competent authorities and to the entities legally able to exercise asset forfeiture, any information that was pertinent within the framework of the integral fight against money laundering, financing of terrorism

and those illegal activities that give origin to state intervention in the form of the seizure and recuperation of assets (in Spanish, and under Colombian law, also known as "extinción del derecho de dominio" – loss of the right of domain).

For this reason, in the development of the case, there was verbal delivery of information pertaining to the quantity of assets, links, financial products and notary acts, as well as other relevant financial information. This allowed the competent authority to use this as guidance for performing the acts of verifying information and obtaining evidence. Furthermore, there was an informal delivery of data with regards to locations, which also contributed to the competent authority's investigation process.

Case conclusion

Through the financial analysis performed, it was possible to identify goods that were in the name of the identified individuals. This served as a starting point to initiate the process of asset forfeiture which was carried out by the competent authorities. In the same manner, other financial transactions were identified, which included cash transactions which were taken into account in determining the value of the case.

Number of natural persons	Number of judicial persons	Quantity of Immoveable Goods	Value of Immoveable Goods in Colombian pesos	Quantity of Moveable Goods in Colombian pesos
197	33	629	146.294.922.522	177

Value of Moveable Goods in Pesos	Amount of Financial Information	Value of Financial Information in Colombian Pesos	Total Value of the Case
10.002.101.782	6.904	254.349.918.711	410.646.943.015

Conclusion

1. The new formula that was derived from the new approach of the UIAF's work process, has generated tangible results which have allowed significant asset forfeiture in one year with other cases currently underway. It also made possible the dismantling of various autonomous networks that lent their services to launder money derived from narcotrafficking to the organisation headed by alias "El Loco Barrera". These networks carried out investments in the real estate, financial and logistics sector and were also utilised in all the operation of transporting illegal drugs from Colombia, abroad. This case demonstrates that the joint inter-institutional, national and international work, is efficient and effective.

2. Carrying out the case analysis in parallel independent phases, facilitated the identification of a network as complex and large as the one pertaining to the organisation headed by alias, "El Loco Barrera". Furthermore, it allowed for greater clarity with regards to the modus operandi of each arm (or part of) the network that was detected. This allowed judicial authorities to carry out the judicial processes with greater speed.
3. Through the working group tables that were carried out during the detection stage, as well as during the disclosure of intelligence state to the Attorney General's Office, it was possible to share feedback among the agencies present, which in turn generated a greater comprehension of the case, data verification and corroboration. It also provided more elements for the prosecutors in charge to guide them through the necessary judicial investigation.

All of the above could serve as reference to other FIUs in terms of implementing best practice in the development of financial intelligence and generating effective results. UIAF of Colombia in cooperation with other national and international institutions was able to identify numerous moveable and immoveable goods that were in the name of those that belonged to the criminal organisation headed by Daniel Barrera Barrera alias "El Loco Barrera". This information had not been previously detected by judicial authorities.

Indicators

- Use of front companies
- Financial transactions not in line with expectations
- Open source links to narcotrafficking
- Acquisition of goods, products and resources connected to narcotrafficking
- Connections with transportation and aviation companies
- Interconnection of seemingly independent businesses
- Unexplained wealth

17. AUSTRAC information sparked investigation into illegal money remitter (AUSTRAC, Australia)

Introduction

Following the money trail has proved an effective way of detecting the activities of organised crime networks. The following case highlights the successes that can be achieved when a Australian Transaction Reports and Analysis Center (AUSTRAC) and law enforcement agencies share financial transaction information about suspected criminal groups.

In the case detailed below, AUSTRAC's monitoring systems identified a substantial increase in cash activity undertaken by a remitter. Further analysis identified significant inconsistencies between the information the remitter had reported to AUSTRAC, and the information reported by those institutions where the remitter was a customer.

This information was referred to the Financial Intelligence Assessment Team (FIAT)[17], which is hosted by the Australian Crime Commission. After the AUSTRAC referral, the FIAT undertook intelligence profiling activity and disseminated the intelligence to the Australian Federal Police (AFP), who conducted the investigation.

As a result of the investigation, two suspects were charged with money laundering offences under the Criminal Code Act 1995. One of the suspects was the remittance dealer, while the other suspect, allegedly acting on behalf of third parties, deposited large amounts of cash into accounts owned by the remittance dealer.

Evolution of the case

AUSTRAC information as seen from 'business' and 'customer' perspectives

The above investigation was triggered by a recognised 'red flag' for authorities. This occurs when AUSTRAC data reveals significant inconsistencies between the transactions reported by the remittance dealer from a 'business perspective' and the transactions reported to AUSTRAC by other institutions from 'the customer perspective', where the remittance dealer is a customer.

In a typical remittance business, authorities would reasonably expect that, over time, a high proportion of the cash paid by customers to the remittance dealer to pay for international funds transfers will eventually be deposited in a bank account held by the

17. The FIAT is a whole-of-government approach to financial information sharing, co-ordination, collaborative targeting and the development of response strategies. Member agencies are the Australian Customs and Border Protection Service, Australian Federal Police, Australian Securities and Investments Commission, AUSTRAC, Australian Taxation Office, Centrelink, the Department of Immigration and Citizenship (DIAC) and the Australian Crime Commission (ACC).

remitter. This 'balancing' of money received by the remitter versus money ultimately deposited with financial institutions should be recorded in AUSTRAC transaction reports, as per the below example:

Step 1. A remittance dealer receives AUD100,000 cash from various customers as payments for international funds transfer instructions.

The remitter, as a 'business', should submit to AUSTRAC:

- where cash payments of AUD 10,000 or more are made by their customers, threshold transaction reports (TTRs) ; and corresponding international funds transfer instruction (IFTI) reports detailing the transactions.

Step 2. Over time, the remitter would normally be expected to deposit some, if not all, of the AUD100,000 cash with a financial institution. A financial institution would inturn report the cash deposit/s to AUSTRAC as threshold transaction reports, where the remitter is recorded as the 'customer'.

If the remittance dealer operates in the manner described above, it is relatively straightforward for AUSTRAC to follow the flow and volume of money, as the amounts reported from both 'business' and 'customer' perspectives are relative.

However, certain business practices by the remittance dealer may lead to discrepancies between the transaction amounts reported by the remitter and the deposit amounts reported by financial institutions.

For example, the remitter may decide not to deposit the entire AUD 100,000 cash into a bank account to pay for the outgoing international transfers, instead using some of the cash to pay for incoming funds transfers sent to Australian-based customers. This is consistent with the 'hawala'[18] method of transferring funds.

The remitter may also utilise hawala for international transfers by arranging for an overseas associate to pay an overseas beneficiary directly. Remitters using hawala channels and not requiring the mainstream banking facilities to physically transfer funds offshore may be less inclined to report transactions to AUSTRAC.

Authorities recognise that the use of hawala by remitters may lead to some discrepancies between a remitter's turnover as reported from the 'business' and 'customer' perspectives. However, the effect of hawala alone seldom explains larger discrepancies. Where significant discrepancies do occur, AUSTRAC is more likely to suspect a remittance business to be handling and moving proceeds of crime, and escalate such matters to law enforcement.

18. Hawala is a type of banking system which operates around the world, primarily in the Middle East and South Asia regions. Hawala systems operate outside traditional banking and financial channels, and typically involve little or no regulation and minimal documentation. In Australia, it is an offence for a person to provide a registrable designated remittance service if the person's name and registrable details are not entered on the Register in accordance with the Anti-Money Laundering and Counter-Terrorism Financing Act 2006.

Case study - AUSTRAC information sparked law enforcement investigation into illegal money remitter

This major AFP investigation, which included valuable contributions from the ACC and AUSTRAC, foiled a major money laundering operation. Transaction reporting information received by AUSTRAC revealed a number of significant and suspicious changes in the financial transaction patterns of the remittance dealer. These changes included inconsistencies in the remitter's transactions reported to AUSTRAC from business and customer perspectives.

- The remittance dealer's activities changed from facilitating small outgoing international funds transfer instructions (IFTIs), to accepting large cash deposits and facilitating large IFTIs. Notably, a spike in financial transaction activity was clearly inconsistent with the remitter's previous profile and history.
- Shortly after this increase in the size of IFTIs, business accounts of the remittance business ceased to receive deposits. However, AUSTRAC analysts were able to identify additional accounts of the remittance business, which had been opened under a different and new company name. Under this new company name, the remitter's modus operandi appeared to change. While the remitter continued to report that the majority of its remittances were being sent to Iran, information received from institutions dealing with the remitter as a customer reported that a significant proportion of the business's outgoing IFTIs were now being sent to the United Arab Emirates (UAE).
- AUSTRAC information revealed discrepancies between the destination countries for the outgoing IFTIs. The remitter reported that IFTIs were being sent to Iran. However, this information conflicted with the destination of IFTIs reported from a customer perspective.
- The remitter's transaction activities continued to escalate while operating under the new company name. Over a three-month period, the remitter recorded cash deposits totalling AUD 34,000,000 and outgoing IFTIs totalling AUD 33,000,000. At the peak of activity, the remitter was receiving cash deposits of AUD1 million each day, and on one occasion received almost AUD 4,000.000 in two days. The third party making these cash deposits made no attempt to conceal the large cash deposits, which were conducted at the same bank branch.
- The value of the remittance dealer's business activity was significantly less than that reported to AUSTRAC by the financial institutions dealing with the remitter as a customer.

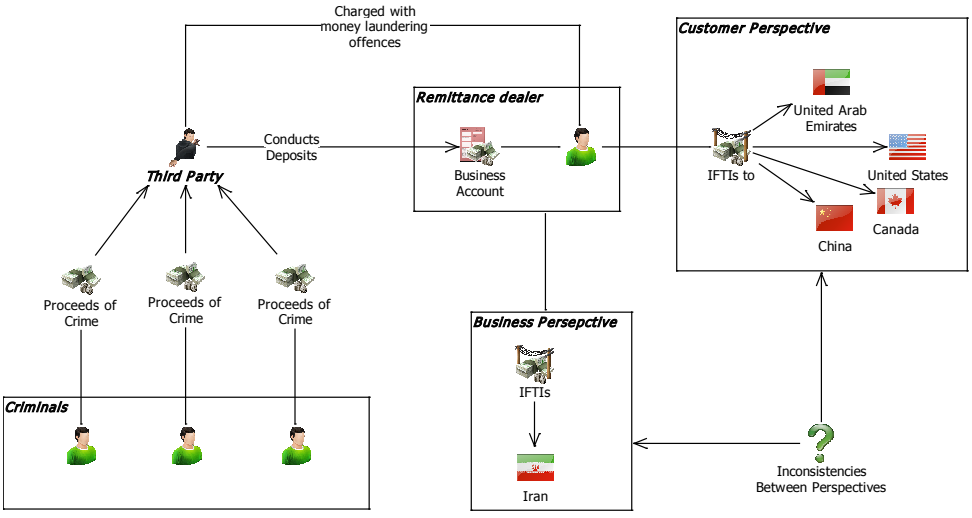
This discrepancy in reporting strongly suggested to authorities that the funds involved were not linked to legitimate business activities, and increased their suspicions that the remittance dealer was dealing with proceeds of crime. Information submitted by industry was also invaluable in highlighting discrepancies in the remitter's activities.

The following table highlights the discrepancies over a 10-month period in the remitter's transaction activities as reported from customer and business perspectives:

Transaction Types	The remittance business (i.e. from the 'business perspective')	Value as reported by reporting entities dealing with the remittance business (i.e. from the'customer perspective')	Difference
Cash deposits recorded in TTRs	AUD 48,000,000	AUD 92,000,000	AUD 44,000,000
Outgoing IFTIs	AUD 55,000,000	AUD 95,000,000	AUD 40,000,000

As the amount of the remitter business's cash activity was increasing, law enforcement agencies progressed to execute warrants against the syndicate and stop its operations. The AFP arrested two individuals, and restrained AUD 1,200,000. The original source of funds could not be established; however the large amount of cash involved led authorities to suspect that the funds were the proceeds of crime.

Indicators relevant to this case



Reporting entities with remittance dealers as customers can play a role in detecting money laundering activity when a remitter acts illegally. Although reporting entities can only report on the remitter's activities from the 'customer' perspective, the following indicators may assist those entities to recognise illicit activity by their remittance business customers:

- Sudden increase in transactional activity inconsistent with the remitter's established profile or transaction history
- Significant increase in cash deposits received by the remitter
- Regular large cash deposits made by the same third party, who does not appear to be directly linked to the remittance business
- IFTIs being sent by a small remittance business to a wide range of different countries, especially when the destination countries are inconsistent with the business's established remitter profile and/or transaction history
- IFTIs being sent directly to individuals rather than an overseas business contact
- Businesses appearing to provide a remittance service despite not identifying itself as a remittance business in its dealings with the reporting entity and/or not being enrolled with AUSTRAC Online

18. Use of foreign bank to conceal source of funds (CTIF-CFI, Belgium)

Introduction

A foreign bank established in an Eastern European country opened two accounts in Belgium for the purpose of correspondent banking.

Analysis of the transactions on these Belgian accounts revealed that they were used as transit accounts. The credit transactions consisted of transfers from the accounts of companies opened at the foreign bank in the home country of that bank. Seventy five percent of the foreign bank's customers (approximately four hundred and sixty customers) were companies headquartered in tax havens. Only five percent of the transactions were related to customers in the home country of the foreign bank. The debit transactions on the Belgian accounts consisted of payments (by order of the customers of the foreign bank) to various counterparties across the world. A large number of these transactions were in US dollars and the amounts totaled up to over a billion Euro between 2008 and 2009.

Evolution of the case

Given the international character of the case file, CTIF/CFI – the Belgium Financial Intelligence Unit (FIU), sent requests for information to at least ten different FIUs through the Egmont Secure Web (ESW). Furthermore, requests for information were sent to Belgian customs, the state security department and the fiscal authorities. The Belgian FlU also checked its own database for all counterparties, as well as police databases and public sources.

The analysis and the information of foreign FIUs revealed that the majority of the clients of the foreign bank were considered to be shell companies, administered by trusts, lawyer's offices and/or companies specialised in establishing offshore companies.

The analysis also revealed that several of these companies and/or financial beneficiaries were known for serious and organised tax fraud, corruption, embezzlement, fraud and organised crime. More than ten percent of the identified customers were known to be directly related to a criminal activity. Taking into account the international context of the case, a percentage often percent was regarded as very significant.

The foreign bank chose to involve another bank, in this case a Belgian bank, to perform the suspicious transactions. This was probably due to the fact that the foreign bank deemed it unlikely that a bank would disclose another bank's activities. However it was the Belgian bank who took the initiative to report the transactions on the accounts of the foreign bank to CTIF/CFI. The Belgian bank settled the accounts of the foreign bank soon after it had made a disclosure to CTIF/CFI.

It should be noted that despite the substantial amount of the transactions being in USD, there were no financial correspondents to carry out these transactions. A foreign FlU confirmed that the foreign bank had been the subject of several Suspicious Transaction Reports (STRs) concerning infringements to the AML legislation and/or infringements on the Bank Secrecy Act.

The method used by the foreign bank enabled the foreign bank to conceal the origin of the funds. Money received in the accounts of the foreign banks in the home country was then transferred in part as aggregated amounts to the two Belgium accounts in the name of the foreign bank in order to carry out payments in favour of the third parties. Thus, every separate credit transaction in the foreign bank's country of origin was then grouped with other credit transactions and transferred to the bank in Belgium. This made it difficult for the bank in Belgium to determine the origin of the money. On the basis of the collected data, CTIF/CFI decided that it was probable that the foreign bank offered its customers the possibility to perform dubious financial transactions through a foreign bank (Belgian bank), without this Belgian bank being able to retrace the origin of the funds.

The CTIF/CFI forwarded the case file to the Public Prosecutor on the suspicion of money laundering probably related to organised crime. After CTIF/CFI had forwarded the case file, it received STRs from three other Belgian banks concerning the foreign bank (similar transactions took place on the Nostro accounts of the foreign bank), as well as an FIU-request concerning this foreign bank. These disclosures were made soon after the judicial authorities made public that they were investigating a huge money laundering case concerning the foreign bank.

Conclusion

The information mentioned in the following disclosures, as well as the information gathered from foreign FIUs that had been requested by CTIF/CFI (information concerning suspicious transactions on accounts of counterparties, and information concerning the beneficial owners of counterparties), has been the subject of several additional reports that have been forwarded to the Public Prosecutor.

Indicators relevant to this case

- Account not used in line with expectations
- Large amount of transactions are related to companies headquarters in tax havens
- Use of gatekeepers
- Use of nominees
- Use of shell companies
- Entities with connections to serious and Organised crime
- Pooling of transactions used to disguise the origin of funds

19. Operation Hammer (FIS, Guernsey)

Case Description

Operation Hammer relates to a complex money laundering investigation which emanated from financial intelligence via numerous Suspicious Activity Reports (SAR's) received from a financial institution. The case was the first of its kind in Guernsey to successfully apprehend and charge multiple offenders for money laundering. It provides an excellent example of the workings of the reporting regime, intelligence development and dissemination to multiple agencies, successful enforcement action and prosecution.

Introduction

Operation Hammer was instigated by the Guernsey Border Agency (GBA) as a money laundering investigation in 2011 and focused on the potential criminal activities of a number of workers originating from Latvia. In the early stages of the investigation the predicate offences could not be established however intelligence suggested that the syndicate was involved in a variety of criminal activities including drug trafficking, prostitution, fraud and extortion. This kind of criminal activity would have a detrimental impact on the island community and the reputation of the island. In addition, individuals were potentially benefiting from acts of criminal conduct. This was not to be tolerated and the investigation was prioritised.

The investigation originated from the receipt and development of substantial financial intelligence received from a local financial institution. The investigation established that the Latvian syndicate were involved with criminal activity in Guernsey, Jersey, United Kingdom and Latvia. The initial subjects of the investigation were Martins Apskalns and Krists Dabra, both Latvian nationals working in Guernsey. The Guernsey Financial Intelligence Service (FIS) received Suspicious Activity Reports (SARs) relating to both individuals and this was supplemented by law enforcement intelligence. The SARs identified that large cash amounts were being paid into bank accounts in Guernsey and electronically transferred to Latvia for the benefit of Apskalns.

The criminal activity being undertaken was initially difficult to substantiate but as the investigation developed it became evident that the fraudulent use of compromised credit cards to purchase numerous airline flights and mobile phone 'top up' for third parties was contributing to the overall generation of the proceeds of crime. The investigation identified another Latvian male, Edgars Gravitis as being involved in the laundering process by allowing large cash amounts to be credited to his bank account. Subsequently, the money was electronically transferred to Apskalns' girlfriend's Latvian bank account again for his benefit.

There was a significant development in the investigation in November 2011 when as part of the joint working approach, Jersey Police identified a Jersey based individual who was a member of the syndicate and involved in fraudulent activity occurring in Jersey. Financial evidence obtained in Jersey provided a direct evidential link to Apskalns and Dabra in Guernsey and therefore substantiated the criminality with which these men were involved. The matter was immediately acted upon with the evidence obtained via the service of a Letter of Request to the Jersey authorities.

Additionally, in February 2012 coercive orders were served upon the financial institution in Guernsey which produced substantial financial evidence which confirmed that proceeds of crime had been laundered via the use of Guernsey based bank accounts

held in the names of Apskalns, Dabra and Gravitis. In total, between 1st November 2010 and 28th February 2012, 163 individual cash credits amounting to GBP 210,460.00, all the proceeds of criminal conduct had been deposited into a number of Guernsey bank accounts. The criminal proceeds had then been electronically transferred to Latvian held bank accounts under Apskalns' control where it was withdrawn in cash by numerous members of the syndicate.

The GBA Financial Criminal Team devised a targeting operation and conducted directed surveillance on the members of the syndicate in order to establish the criminality involved to an evidential standard. In March 2012 two of the syndicate, Dabra and Gravitis, were arrested in Guernsey, interviewed under caution and subsequently charged with the offence of money laundering. Searches of residential premises following the arrests of these two men directly led to the arrest, interview and charge of a third Latvian male, Madars Jankevics.

Money laundering charges were brought against the four Latvian individuals. Apskalns, considered the syndicate leader, was sentenced on 1st March 2013 and is serving a four year custodial sentence. The three other Latvian males absconded prior to being dealt with by the Royal Court of Guernsey and currently remain at large with arrest warrants having been issued by the Court. The syndicate member in Jersey was prosecuted for fraud offences. Confiscation matters are ongoing with an ongoing asset tracing initiative being undertaken by the FIU in conjunction with the Latvian authorities.

Evolution of the Case

The case evolved when a Guernsey financial institution (clearing bank) identified numerous suspicious cash deposits being credited to Apskalns' bank account. The deposits were significant, out of keeping with the expected activity on the account and seemingly not from a legitimate source.

The FIU developed the intelligence received and by completing wide-ranging financial enquiries an intelligence package was disseminated to the Guernsey Joint Intelligence Unit where it was further developed by intelligence officers working in the field. Intelligence indicated that Apskalns was employed in Guernsey by a local construction company.

Intelligence identified that in January 2010 Apskalns' name had been noticed in connection with numerous flight bookings for Latvian Nationals inbound and outbound from Guernsey and beyond to Latvia. This pattern continued throughout the year and it became apparent that bookings had often been completed in false names and paid for with third party credit card details, often held in the names of United States residents. In some instances the flight tickets were used and at other times the passengers, usually Latvian Nationals, failed to travel.

The GBA in conjunction with Guernsey Police instigated a risk assessment exercise aimed at accumulating intelligence surrounding the booking of these flights in order that progress could be made towards executive action.

On 29th October 2010 Apskalns departed from Guernsey to St Malo, France by ferry and absconded from the island in contravention of his bail conditions which were the result of his arrests by Guernsey Police earlier in the year on suspicion of fraud offences. Apskalns also failed to complete a Community Service Order which the court had handed to him as punishment for his involvement in the importation of a Class C controlled drug in February 2010.

In summary, part of the criminality generating the proceeds was identified as the purchase and onward sale of flight tickets and mobile phone top-up with stolen credit card details obtained from websites which facilitated the sale of compromised card data. Access to such websites or forums is typically restricted, with new users having to be vouched for by people already signed up to the forums, so as to avoid detection by law enforcement agencies. It was the use of two such internet sites which was eventually to put Apskalns at the center of this particular web of deceit.

The way the frauds worked would be as follows: Apskalns would obtain the stolen card data from one of these websites. He or one of his associates would then use the stolen data to book a flight or obtain a mobile phone top-up. Sometimes the people on the flights or receiving the top-up would be known to Apskalns, sometimes not. Either way, a cash payment would change hands and Apskalns would be left with a problem – how to get the cash which he obtained for the frauds back into the bank accounts of himself and his criminal associates.

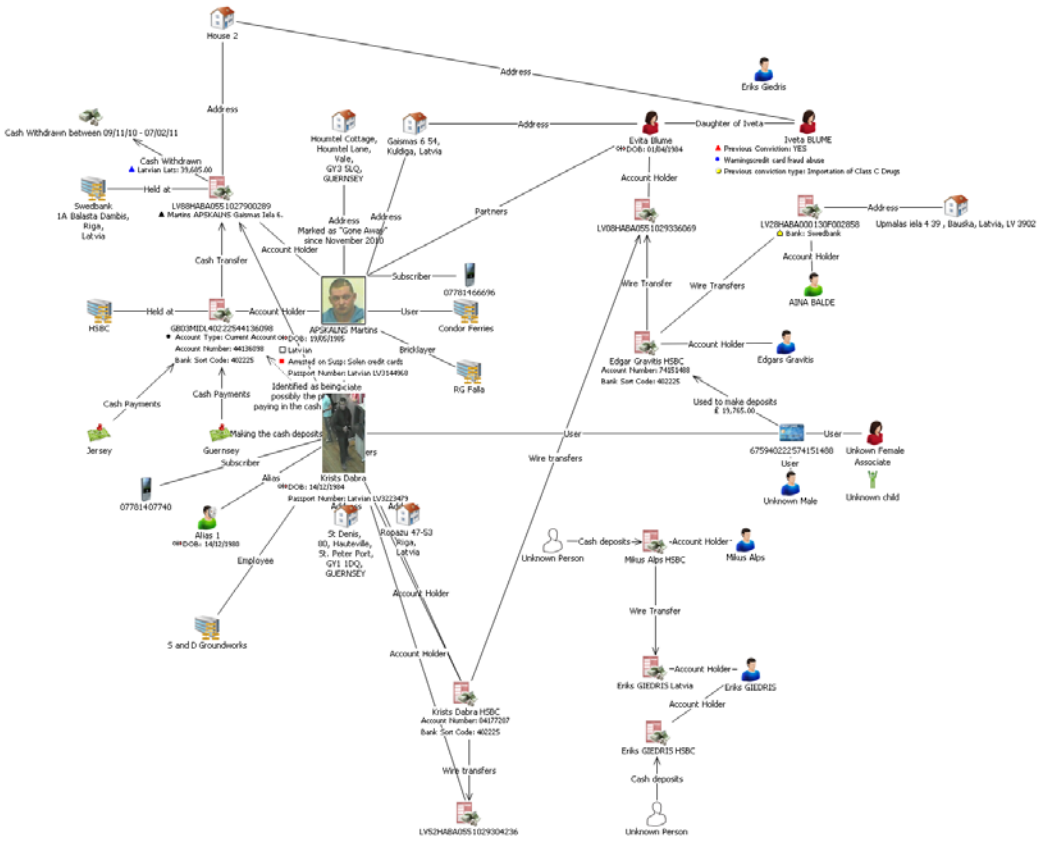
In February 2011, the FIS received a further SAR from a financial institution relating to suspicious cash payments being credited to Apskalns' account and subsequently electronically transferred out of the jurisdiction to Latvia. This significant financial intelligence indicated that the bank account was being used as a vehicle to move suspected proceeds of crime through the banking system to Latvian held bank accounts under Apskalns' control. However, the type of criminality generating these criminal proceeds remained unsubstantiated. Similar SAR reports were later submitted relating to suspicious activity on bank accounts held in the names of Dabra and Gravitis.

Suspicions tended towards drug trafficking but investigations had failed to substantiate the type of criminality generating the suspicious credits. An innovative method that the FIU used during this investigation was directed surveillance which had not been utilized in previous money laundering investigations in Guernsey. The purpose of the directed surveillance was to substantiate the predicate offences which were generating the proceeds of crime.

A breakthrough came when the GBA FIU was contacted by Jersey Police who were investigating a Jersey resident by the name of Darren Hendron. Jersey Police initially believed that it was Dabra who was involved with credit card fraud with Hendron due to the evidential content of mobile phone text messages and payment details that they had discovered during their investigation. It later became apparent that Apskalns and Dabra had worked with Hendron on building sites in Guernsey.

The FIS disseminated evaluated intelligence reports to the Guernsey Border Agency Financial Criminal Team, Guernsey Police, Jersey Joint Financial Crime Unit, Serious Organised Crime Agency Financial Intelligence Unit and the Latvian Financial Intelligence Unit via Egmont secure web. The disseminations were followed up by conference calls and meetings.

Although now absent from Guernsey, Apskalns continued to perpetrate his fraudulent activities through the internet. Initially, Apskalns arranged for other people to pay the cash obtained from his continuing frauds into his own Guernsey based bank account. Detailed forensic analysis of the bank activity established that November 2010 and April 2011 there were sixty two separate cash deposits in Guernsey totaling some GBP 109,275 paid into Apskalns' own HSBC bank account. Over a similar time period, Jersey Police also later identified 5 cash payments through cash paying in machines in Jersey, again all to Apskalns' personal bank account. All this money made its way out again, in forty two separate transfers, into Apskalns' Latvian bank account, from where it was distributed to other participants in the fraud.



Due to the volume and nature of these unexplained cash deposits, nearly all of which were made through paying in machines in Guernsey and Jersey, the bank realised by early 2011 that there was something irregular going on. Accordingly, in April 2011 the bank closed down Apskalns' Guernsey bank account and declined to process any further transactions through that account. This now left Apskalns with a major issue; without access to a convenient bank account to make cash payments into, his lucrative and fraudulent activities could have been curtailed.

His solution was to persuade at least two of his Latvian friends and acquaintances, who he referred to as "his boys", being Dabra and Gravitis, to allow him to use their Guernsey based bank accounts for the same purpose.

Enquiries have identified that between 24th May 2011 and 10th November 2011, twenty seven separate cash deposits totaling GBP 55,670 were paid into Gravitis' Guernsey bank account, all of which came from criminal activities. A further GBP 39,305 was paid via cash paying in machines in Guernsey into the Guernsey bank account of Dabra who was a close friend of Apskalns. A further twenty two cash deposits totaling GBP 5,425 were also made in Jersey between September 2011 and February 2012 into Dabra's Guernsey bank account.

A similar amount of money was paid out of those Guernsey based accounts, again in several separate payments, into Latvian bank accounts over which Apskalns had control.

Background – Fraud Offences

During 2010 Guernsey Police received a formal complaint from Aurigny Air Services Ltd, a locally based airline company servicing the Channel Islands and the UK, concerning 'chargeback'[19] payments relating to credit and debit cards which had been used to make flight bookings with the company between September 2009 and October 2010. In particular, the company provided specific details which linked flight bookings to a close associate of Apskalns and co-accused in this case, Dabra.

In May 2010 Guernsey Police received a formal complaint from Cable & Wireless Guernsey Limited a local telecommunications company relating to transactions for prepaid mobile phone credit obtained via the use of the online "top-up" facility provided by the company. The complaint stated that during the early part of April 2010 their financial accounts team had received notifications of chargebacks from credit card providers. Internal investigations conducted at Cable & Wireless identified the particular IP addresses from where the transactions were originating. They noted that a large portion of the transactions had emanated from Latvia but that from April 2010 the suspect IP address related to a specific Guernsey residential address. The change in the location of the IP address from Latvia to

19. The charge a credit card merchant pays to a customer after the customer successfully disputes an item on his or her credit card statement, typically from unauthorised / fraudulent use of their credit card without their knowledge.

the specific residential address in Guernsey coincided with Apskalns relocating from Latvia, to his home address in Guernsey where the specific IP address was sourced. Subsequently, Apskalns was arrested at the property and during a search of the premises some very good evidence was discovered.

In interview, Apskalns could not explain why the IP address for all the fraudulent "top-up" transactions was that of his home address in Guernsey. Apskalns was also unable to explain why other fraudulent "top-up" transactions purchased during March 2010 showed an IP address in Latvia where he was located at the time. Apskalns denied any involvement and was bailed.

On Thursday 28th October 2010 Apskalns was intercepted at Guernsey Airport when he was attempting to travel on a flight ticket purchased with stolen credit card details. He was arrested by Guernsey Police prior to boarding. In interview Apskalns claimed that a friend in Latvia had made the flight booking on his behalf because he offered cheap flights via the internet. Apskalns denied all knowledge of the flight payment details and stated that he had been sent a text message with the flight booking locator reference and subsequently, that he had printed the boarding card from the internet. He was subsequently bailed. It transpired that Apskalns had actually been describing his own method of criminality.

Executive Action relating to Money Laundering Offences

In March 2012, Dabra and Gravitis were identified as both travelling inbound to Guernsey by separate means following short returns to Latvia. Each male was arrested, cautioned, interviewed under caution and charged with money laundering. During the resultant searches Jankevics was identified as being complicit in the criminality, arrested and subsequently charged with money laundering.

Word of the arrests transferred to Apskalns in Latvia and on 12th March 2012 he returned to Guernsey of his own free will to face the outstanding matters against him. In interview Apskalns informed the interviewing officers that the criminality was his responsibility and that he had come back to Guernsey to 'save his friends'. Apskalns was charged with money laundering and fourteen counts of fraud by misrepresentation. He pleaded guilty to all charges against him and on 1st March 2013 he was sentenced to four years imprisonment by the Court. Additionally, the Court recommended that his deportation be considered by the Governor of Guernsey.

Dabra and Jankevics were remanded out of custody and absconded from Guernsey prior to being dealt with by the Court. Gravitis entered a not guilty plea but subsequently absconded from Guernsey just prior to his trial in January 2013. Arrest warrants remain in place for all three men and liaison work continues with the Latvian authorities in order to bring these men to justice. Apskalns admitted in interview that he holds substantial assets in Latvia in the form of property and land and work is ongoing to confiscate these and any as yet unidentified proceeds of crime.

Conclusion

An intensive investigation led to the charging of four individuals with money laundering. Evidence produced in Court showed that in total Apskalns and his criminal associates laundered a total of GBP 210,460.00 over a sixteen month time period. Additionally, further proceeds of crime which had been generated via the Jersey based syndicate member amounting to GBP 5,425.00 was personally withdrawn in cash and presented to Apskalns by Dabra in Latvia. Apskalns, the main syndicate leader, is currently serving four years in the States of Guernsey Prison and arrest warrants remain in place for his three close accomplices. Guernsey remains determined that these men will face justice and are currently working with the Latvian authorities in order to reach this conclusion.

Equally, Guernsey is determined to proceed with the seizure of Apskalns' assets in Latvia to ensure that the adage 'crime does not pay' is upheld in this instance and sends this clear message to other criminals.

Indicators relevant to this case

- Existing intelligence suggesting involvement with several illegal activities
- Numerous unexplained cash deposits
- Use of automated paying in machines
- Receipt of large cash deposits into bank account not in line with expected account use
- Large cash deposits followed by international transfers
- Previous convictions for drug related activity
- Money transfers between syndicate members

20. The use of shell companies and 'round-robin' type schemes to evade tax. (AUSTRAC, Australia)

Case description

This case study involves a group of manufacturing companies using cheques, shell companies and a round-robin type scheme to avoid tax obligations. It illustrates how Australian Transaction and Reporting Centre (AUSTRAC) information and analysis led to

the detection of the multi-million dollar money laundering and tax evasion scheme. The investigation was triggered by an AUSTRAC referral to law enforcement after anomalies in the financial transaction reporting of a clothing manufacturing business were identified

Introduction

AUSTRAC information assisted law enforcement to identify a criminal syndicate that was facilitating large-scale tax evasion for a number of clothing manufacturers. The manufacturing businesses were linked as a group which withdrew more than AUD 16,000,000 in cash over a twelve-month period.

Evolution of the case

Investigations revealed that over a three-year period more than AUD 52,000,000 was deposited into and withdrawn from accounts operated by a criminal syndicate. The syndicate involved a group of ten clothing manufacturing companies.

AUSTRAC information proved essential in establishing a picture of the syndicate's financial activity and modus operandi. The annual financial activity of the syndicate increased dramatically over three years from AUD753,000 in the first year to AUD 17,800,000 in the last year. Suspicious matter reporting and financial profiling of the syndicate's financial behaviour by AUSTRAC analysts helped to uncover the mechanics of the money laundering scheme.

AUSTRAC's monitoring system and additional macro-analytical searches of related financial activity identified links among ten clothing manufacturing businesses in one geographic location which had been conducting large cash withdrawals over an extended period of time. Members of the syndicate were identified as frequently depositing cheques into company accounts, some of which were linked to shell companies.[20] Once the cheques had cleared, the syndicate would withdraw the cash in multiple amounts, often on the same day, and secretly return the cash to the businesses.

More specifically, AUSTRAC information identified:

- Over a twelve month period, approximately six hundred and fifty cash withdrawals were made from two or more company accounts at the same bank branch
- A suspicious matter report (SMR) relating to a company director indicated the person had made multiple same day cheque deposits to the accounts of several of the other network companies
- Over the preceding twelve month period, the companies under investigation were linked to cash withdrawals valued over AUD 16,000,000.

20. A shell company is formally established under applicable corporate laws but does not actually conduct a business. Instead, a shell company can be used to engage in fictitious transactions or hold accounts and assets to disguise the actual ownership of those accounts and assets.

AUSTRAC also received a number of SMRs from reporting entities and related high-value transaction reports which helped reveal the methodology used by the syndicate. Within the SMRs, reporting entities identified the following 'grounds for suspicion':

- several cheques written by the manufacturing company were deposited into accounts (often several times in one day) of regular and known customers to the bank who operated within the clothing manufacturing industry
- numerous cheque deposits were made, all on the same day, into multiple, related company accounts, followed by repeated requests for quick clearances of the cheques
- Funds were withdrawn in cash from accounts as soon as the proceeds of cheque deposits cleared, often on the same day, across multiple branches

AUSTRAC produced a financial intelligence assessment on the individuals under investigation and disseminated it to law enforcement for further investigation. The financial intelligence assessment provided an analysis of AUSTRAC's information, identifying patterns in financial activity and drawing links to other individuals.

AUSTRAC also worked with domestic partners during the investigation. AUSTRAC provided an onsite AUSTRAC Senior Liaison Officer (ASLO) to support investigating officers. The ASLO prepared regular analysis on the financial activities of the syndicate, and assisted with profiling and other tasks relevant to the investigation.

The investigation identified that the clothing manufacturers were complicit in the scheme, which enabled them to avoid paying a significant amount of tax. The method used by the syndicate to facilitate tax evasion is as follows:

1. A legitimate clothing retail company paid a clothing manufacturing company for the production of garments. These payments related to a legitimate business activity and the retail companies were not complicit in the scheme.
2. The promoters of the scheme made approaches to the garment makers and offered to reduce the amount of tax they were paying, less a commission to the promoters of between five and ten percent.
3. A series of shell companies were set up using the details of members of the community who had been approached by the promoters and paid a small amount of money for their personal details. These details were then used to register the companies, obtain workers compensation insurance and bank accounts in order to create a façade of legitimacy.
4. With the assistance of the promoters, invoices were created and issued to the clothing manufacturers purportedly for the provision of (fictitious) goods and services. These false invoices enabled the manufacturer to claim tax deductions for subcontracting expenses that were never incurred.

5. The manufacturers made cheques payable to the shell companies to pay the false invoices.
6. Members of the syndicate deposited the cheques into the accounts of the shell companies.
7. Once the cheques had cleared, the syndicate members withdrew the funds from the accounts via multiple cash withdrawals with debit cards obtained for each shell company account. These withdrawals were undertaken across various bank branches.
8. The syndicate returned the cash to the manufacturer, minus a commission.
9. The manufacturers used the cash to fund their lifestyles and paid cash wages to their employees, thereby avoiding income tax obligations.

It was established that bank employees conspired with the criminal syndicate to commit the money laundering and fraud activity. The investigation revealed a bank employee abusing their position within the bank to launder criminal funds and conceal money trails through misreporting financial activity. Employees of the bank were found to have taken bribes to ignore reporting requirements. In one instance, a bank employee was approached to help arrange the withdrawal of funds from multiple shell company accounts for the criminal syndicate, even though the accounts did not belong to the suspects.

Despite corrupt bank insider involvement, law enforcement worked closely with bank management to collect vital intelligence and financial information to support the criminal investigation.

The fraud activity was a key enabler for the syndicates tax fraud and money laundering activities. Authorities believe that, because employees working for the manufacturing companies were paid in cash, they were also able to claim welfare benefits while working.

Arrests resulted in the restraining of more than AUD 1,000,000 in cash. A number of properties believed to also be the proceeds of crime were also restrained. Two members of the syndicate involved with the scheme were charged with dealing in proceeds of crime worth AUD 1,000,000 or more, contrary to Section 400.3(1) Criminal Code Act 1995.

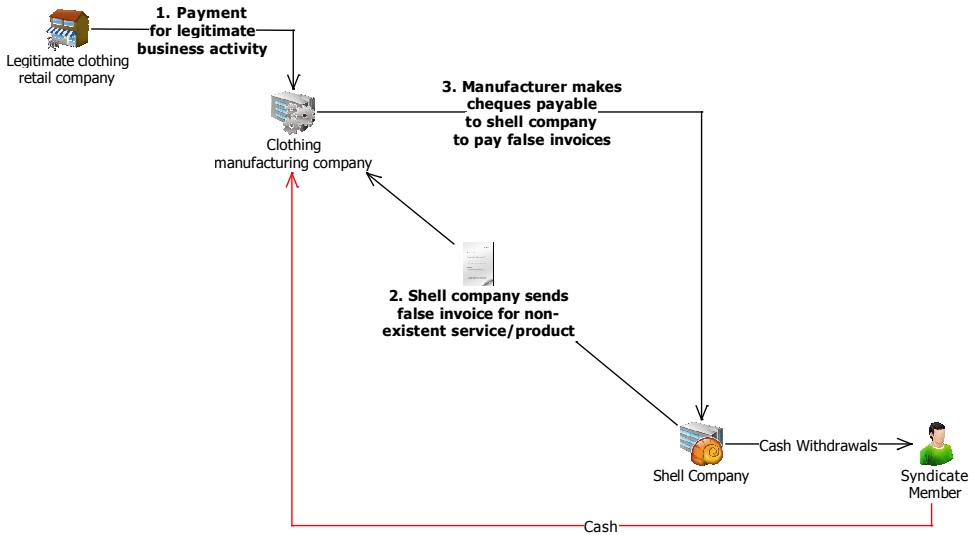
Conclusion

AUSTRAC's referral of suspicious transaction reports triggered the disruption of a major money laundering and tax fraud scheme that led to the seizure of criminal proceeds. AUSTRAC's financial intelligence reporting and analysis helped to identify members of the criminal syndicate and links among legitimate businesses. Financial intelligence also helped to establish for investigators the methodology that the syndicate was using to launder their money.

Indicator Table

Offence	Tax evasion
Customer	Business
Industry	Banking (ADIs)
Channel	Electronic Physical
Report type	SCTR SMR/SUSTR
Jurisdiction	Domestic
Designated service	Account and deposit-taking services
Indicators	Significant value and volume of cheque deposits into bank accounts Significant value and volume of cash withdrawals Same day cheque deposits, followed by cash withdrawals of an equivalent value to the cheque deposits, across multiple branches Repeated requests for quick cheque clearances

The diagram below provides a visual representation of the methodology used by the syndicate to launder funds and evade tax.



Terrorism

Terrorist organisations generally have a global reach in their activities as well as in the source of their funding. Sources of funding can include both legitimate and illegitimate sources.

Legitimate sources may include collection of membership dues and subscriptions as well as appeals within a community. This fundraising might be in the name of organisations with charitable or relief status, so that donors are usually unaware of the ultimate destination and purpose of their contribution.

Terrorist organisations may run or own legitimate businesses that have been established to generate profits and allow for the co-mingling of illegal funds. Legitimate businesses may include restaurants, trading companies, convenience stores and investment management firms.

Terrorism financing can also be generated through illegal activities, and therefore may appear similar to other criminal organisations. Kidnapping and extortion can serve a dual purpose of providing needed financial resources while furthering the main terrorist objective of intimidating the target population. In addition, terrorist groups may use smuggling, fraud, theft, robbery, and narcotics trafficking to generate funds.

Like criminal organisations, they have to find ways to launder these illicit funds to be able to use them without drawing the attention of the authorities. For this reason, transactions related to terrorist financing may look a lot like those related to money laundering. Though often the sums of money collected to fund terrorist groups are very small in amount and difficult to detect.

The following case briefly describes how a group raised money to fund terrorist activities including the establishment of a non- profit organisation which was also used as a cover for the movement of money.

Indicators

- The use of nonprofit organisations (NPOs) to generate funds
- Purchase of large amounts of foreign currency
- An account opened in the name of a legal entity, a foundation or association, which may be linked to a terrorist organisation and shows movement of funds above the expected level of income
- Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements

- Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern, such as countries designed by national authorities, FATF non-cooperative countries and territories, etc.

21. Using legitimate businesses and non profit organisations to finance terrorism (NFIU, Nigeria)

Introduction

Nigerian national, Mr. Jack, born in 1965, grew up in a wealthy family. In the 1990s he started selling guns in south-east Nigeria. He went on to become the leader of the Movement for the Emancipation of Niger Delta (MEND) and emigrated from Nigeria in 2003. The first known terrorist attack conducted by MEND was the bombing of an oil pipeline in the Niger Delta on December 20, 2005. The leader of the MEND is a well-known terrorist and a citizen of more than one African country.

Background

In 2007, Mr. Jack was arrested in Angola by Angolan law enforcement authorities on gun-running charges. At the request of the Nigerian authorities, he was extradited to Nigeria in February 2008 and charged with sixty two counts of treason, terrorism, illegal possession of firearms, and arms trafficking. Although he continued to supply arms to well-known terrorists within and outside Nigeria, in 2009 he accepted the amnesty terms during the amnesty programme of the Nigerian government and was released from prison on July 13, 2009. He subsequently left Nigeria for another African country where he established and ran an NPO and other companies, including construction, shipping and foreign exchange which were later found to be vehicles for disguising illicit funds and their beneficiaries.

Following the explosion near the Government House Annex in Warri, Delta State in March 2010, where government officials were negotiating the amnesty programme for militants in the Niger Delta with the support of the MEND, Mr. Jack and his associates attempted to disrupt the event and succeeded in bombing the venue which led to the death of one person and the injury of several others, as well as the destruction of properties.

Mr. Jack and his associates were also found to have planned and bombed the venue of the 50th Independence Anniversary celebration on October 1, 2010 where the Nigerian President, high-level officials, diplomats, and security officers were present. Several lives were lost and several cars were destroyed as a result of the bomb blasts.

Evolution of the case

The investigation into the bomb attacks led to a request to the Nigerian Financial Intelligence Unit (NFIU) for information on the activities of companies and individuals associated with the MEND. Analysis of the information from the NFIU database showed that some of the transactions were transnational in nature and involved several jurisdictions particularly in Africa.

Requests for information were sent to FIUs in other jurisdictions on entities and link accounts known to be associated with Mr. Jack. The Egmont information exchange channels provided an effective collaborative platform between the FIUs involved in this case and led to the tracking of funds related to financing of terrorism such as importation and sales of arms and ammunitions, illicit arms trafficking, terrorism/terrorist financing, environmental crime, kidnapping/hostage-taking, extortion, maritime piracy, participation in an Organised criminal group, and funding of various terrorist activities in Nigeria.

Based on analysis of the NFIU, it was discovered that the NPO set up by Mr. Jack was a cover for criminal activities. It was also discovered that funds were moved through Nigeria and other African countries in the region of over USD 1,800,000 which was electronically received by Mr. Jack when he purchased over USD 100,000 of foreign currency. It was equally found that he ran 17 bank accounts. Forty-thousand individual transactions were conducted between 2003 and 2011 with a value of over USD 4,500,000.

Mr. Jack was subsequently tried and convicted in another African country on charges of terrorism, terrorist financing, and gun-running committed in Nigeria and other African countries, and sentenced to twenty four years imprisonment. The process of recovering his illicit assets is still on-going. Some of his associates are on trial in Nigeria and one of them was sentenced to life imprisonment in February 2013.

Conclusion

This case reflects the importance of the Egmont information exchange channels in strengthening the capacity of law enforcement agencies to combat terrorism and terrorism financing.

It is also a good indication of how international cooperation and exchange of information can assist in reducing incidents of transnational organised crime.

Indicators relevant to this case

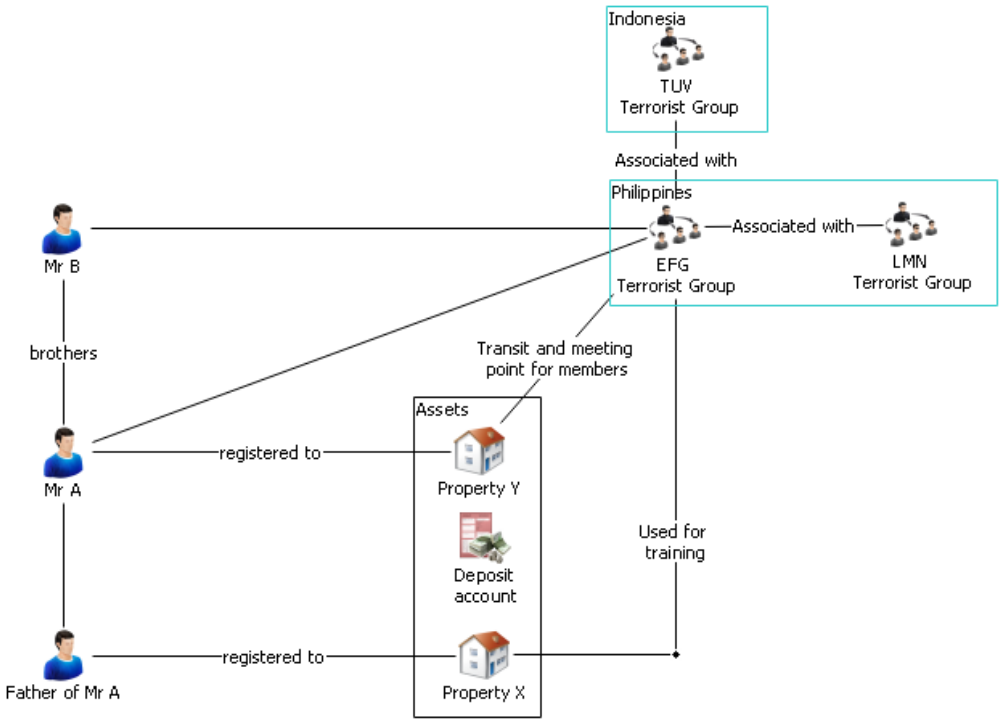
- Member of a charitable organisation
- Associated with a large number of bank accounts
- Highly transactional behaviour
- Purchase of a substantial amount of foreign currency
- Known associations with an organised crime group
- Previous convictions relating to treason, drugs, illegal possession of firearms and terrorism
- Previous involvement in successful terror campaigns
- Previous funding of terror activities

22. Disrupting the financial and material resources of terrorism through civil forfeiture (AMLC, Philippines)

Background

This case centres on the 'EFG' group, a Philippine-based Islamic extremist group that utilises violence and terrorism with the aim of turning the Philippines into an Islamic state. EFG were established in January 2002 and are associated with both the 'LMN' and 'TUV' Islamic extremist and terrorist groups which operate in the southern part of the Philippines and Indonesia, respectively. EFG receive training, funds and operational assistance from the LMN and TUV in exchange for the field operatives and a pool of potential recruits for the latter.

Among the terrorist activities that the EFG Group had conducted, along with the LMN and TUV Groups, are the bombing of a passenger marine vessel in February 2004, and the February 2005 Valentine's Day bombings in major cities in the Philippines.



This case resulted in the freezing and eventual forfeiture of two real properties - a seven hectare agricultural land (X Property), a three-storey building (Y Property), and a bank deposit.

Evolution of the case

The investigation was initiated by separate requests from a local anti-terrorism agency and a foreign government to investigate, freeze and seize the assets owned or controlled by EFG Group members including those of Mr. A, its founder and leader. The requests were based on the inclusion of the EFG Group and its members on the various foreign terrorist designation lists.

Investigation conducted

The Philippine FIU conducted an investigation with the cooperation of, and in coordination with, the intelligence units of the local law enforcement agencies.

It was established that the EFG Group utilized the Property 'X' as a training location for members. The property was found to be registered in the name of Mr A's father however it was controlled by Mr A along with his brother Mr. B, also a member of the EFG Group. In 2002, property 'X' was raided by the Philippine authorities and firearms, ammunitions, explosives, and training paraphernalia were recovered. Several of its members were arrested and criminally charged.

It was also established that the EFG Group used property 'Y' as a transit point for operations and a meeting point for members. The property was registered in the name of Mr. A and was made to appear as a "Madrasah' or Islamic School to avoid detection.

A suspicious transaction report also revealed a bank account which was maintained under the name of another EFG group member. Evidential material was obtained and revealed that the account was used to receive funds from an individual in another country, for the benefit of the EFG Group. The account could be accessed by using an ATM card with an accompanying PIN number "3845"'. The PIN number was believed to relate to firearms calibres "38" and "45" and provided a very memorable pin number which could be used by EFG group members to allow direct access to the account.

On the basis of the aforementioned requests the Philippine FIU requested that the assets be frozen. After the initial investigation the FIU commenced civil forfeiture proceedings utilising evidence from the investigation team.

Conclusion

On 14 January 2011, a Judgment-was rendered in the case, directing the civil forfeiture of the said assets. The amount of the bank deposit forfeited has been turned over by the bank to the Philippine FILJ

Indicators relevant to this case:

- Links to other terrorist organisations
- Group members appear on terrorist sanctions list
- Financial activity reported to the FIU via a suspicious activity report

What makes a good case

In 2012 the Egmont Training Working Group (TWG) established a BECA competition criteria against which the cases would be judged. Even though a number of the cases were submitted prior to this time, the criteria still provides points for discussion as to what constitutes a good case.

One of the criteria was with respect to the currency and complexity of the case. Most of the cases were reasonably recent though recent cases are often difficult to access given the length of time it takes to fully investigate a case and bring it to the courts for prosecution. Those that were still in the judicial stage were presented as sanitised cases and still provided valuable information.

Each case certainly demonstrated a complexity that highlighted the level of skills of analysts within our FIUs as well as the commitment to source additional information that would add value to the analytical process.

In each case, Financial Intelligence Unit (FIU) information was extremely valuable. It was FIU information that allowed analysts to find links between criminals who were previously known to law enforcement and others that were unknown. The important role that FIU information plays in linking criminals and their organisations cannot be underestimated. Even though criminals intentionally develop complex schemes to put distance between themselves and the criminal activity, these cases show that an experienced analyst, with the cooperation of relevant stakeholders are able to follow the money trail and establish links that are valuable to law enforcement.

The sound and thorough development of a case requires cooperation beteen both domestic and international sources. The majority of cases was transnational in nature and demonstrated the importance of international co-operation between FIUs. Domestically, information provided by other government agencies such as law enforcement and customs also proved to be invaluable, as did information provided by financial institutions and other financial services. This highlights the importance of relationship building within a jurisdiction and the value that communication and feedback play. Open source information was also utilised. Even though this information may not always prove to be reliable, in some cases it provided to offer valuable leads that could be checked and confirmed.

As part of the analytical process many FIUs established working groups or multi-agency task forces to facilitate information sharing with key stakeholders who were in a position to add value to the case. Working groups allow for two way feedback. They provide opportunities for all key stakeholders to gain a better understanding of information requirements as well as the value of the information they provide.

The manner in which the analytical findings are presented has a direct impact on the recipients' understanding of the case. A logical progression from the receipt of the trigger that initiated the case, through the development of the case to the end or final outcome of the analysis, provided a clear understanding of the analytical process. Graphical representation of the activities also greatly enhanced an understanding of the case. The use of link charts to illustrate connections between individual, companies, countries etc., and flow charts to demonstrate the flow of funds provided a more simplistic description which underpins the narrative of the case.

The collaborative efforts of Egmont member FIUs in contributing to the BECAs demonstrates a commitment to educate each other and work together in the fight against money laundering, terrorism financing and the financing of proliferation of weapons of mass destruction.