Asia/Pacific Group
on Money Laundering

APG YEARLY TYPOLOGIES REPORT 2009

Adopted by Members at 12th Annual Meeting
Brisbane, Australia, 10 July 2009

Applications for permission to reproduce all or part of this publication should be made to:

APG Secretariat
Locked Bag A3000
Sydney South
New South Wales 1232,
AUSTRALIA

Tel: +61 2 9286-4383
E Mail: mail@apgml.org
Web: www.apgml.org

CONTENTS

INTRODUCTION

Background

The Asia/Pacific Group on Money Laundering (APG) produces regional typologies reports on money laundering (ML) and terrorist financing (TF) techniques in the Asia/Pacific region.

Typologies of money laundering and terrorist financing allow governments to understand the nature of existing and emerging ML and TF trends and design effective strategies to address those threats. Typologies studies also help APG members to implement effective strategies to investigate and prosecute money laundering and terrorist financing, as well as design and implement effective preventative measures.

The APG Typologies Working Group conducts a series in-depth studies on particular typology topics and supports a network of typology experts.

Recent Regional and Global Typologies Events

Sri Lanka hosted the 11th APG Typologies Workshop in Colombo from 27 – 29 October 2008. It was attended by over 120 participants, representing 27 APG members and 6 international and regional organisations.

The 2008 workshop focused on:

- Vulnerabilities in the casinos and gaming sector;
- Proceeds of Crime Investigations & Prosecutions;
- Vulnerabilities in the securities sector; and
- Terrorist Financing.

In November 2008, the APG participated in the joint Typologies Meeting between the Financial Action Task Force (FATF) and MONEYVAL in Monte Carlo, Monaco. The FATF/MONEYVAL meeting focused on:

- Money laundering and terrorist financing risks in the securities industry;
- Money laundering through sporting clubs;
- Money laundering through money service businesses; and
- The global threat assessment.

Detailed outcomes from the FATF's Typologies work are available for download at www.fatf-gafi.org.

Overview of Typologies Workshop 2008 – Sri Lanka

The Central Bank of Sri Lanka hosted the 11th APG Typologies Workshop in Colombo from 27 – 29 October 2009. Mr P Samarasiri, Assistant Governor, Central Bank of Sri Lanka and Dato' Zamani Abdul Ghani, Deputy Governor, Bank Negara Malaysia served as Co-chairs for the first day of the workshop. Mr H A Karunaratne, Director, Financial Intelligence Unit, Central Bank of Sri Lanka and Mr David Shannon, Principal Executive Officer, APG Secretariat served as Co-chairs for the second and third days of the workshop.

Typologies Working Group Meeting

The Typologies Working Group met on Sunday 26 October 2008, with the meeting being chaired by Ms Foo Lee Mei – Malaysia Securities Commission. Participating Delegations included Sri Lanka, Japan, Australia, Lao PDR, Bangladesh, Malaysia, Cambodia, United Kingdom, Chinese Taipei, Asian Development Bank, Fiji, and UNGMPL

Casinos Project
David Shannon gave an update on the progress of the joint APG/FATF casinos paper and acknowledged the very hard work of Ms Rachel Horton of New Zealand in leading the drafting of the report. A number of delegations added suggestions to the draft paper, which were reflected in a subsequent draft of the paper.

Possible Future Topics
The Working Group discussed a number of possible future topics and considered issues of resources to undertake additional typologies work.

A wide range of areas were put up as initial suggestions including illegal logging and ML; illegal fishing and ML; phone remittance and ML/TF; human trafficking and people smuggling and ML; identity fraud and ML; Non-profit organisations and TF; and regional developments in TF.

Given the wide range of topics discussed and the recently received jurisdictions reports, the Working Group agreed that the Co-Chairs would work the Secretariat to develop draft project proposals for priority topics for the coming year.

Joint work with the FATF
The Working Group discussed the need for APG members to contribute to current FATF global typologies projects including the Global Threats Assessment (GTA) Project and the Securities Sector Project.

The Secretariat undertook to keep all APG members informed of developments of the FATF typologies projects.

Workshop

Welcoming Ceremony
Mr Ajith Nivard Cabraal, Governor, Central Bank of Sri Lanka, gave the opening address to welcome all delegates and to set out the conduct of the Workshop. The Hon. Mr W P G Dep, Attorney-General of Sri Lanka gave an address and highlighted the importance of clear arrangements to ensure effective powers are available in the fight against money laundering (ML) and terrorist financing (TF). The Attorney General outlined a number of the key legal measures which are being implemented in Sri Lanka. Hon. Mr. Sarath N. Silva, Chief Justice, provided the key note address. The Chief Justice highlighted a number of risks flowing from the increasingly globalised nature of the world economy and associated ML and TF threats.

Overview of APG and global typologies work
The workshop co-chairs outlined the importance of APG regional typologies workshops and this year's agenda. A key development in 2008 was the inclusion of representatives from the private sector during the whole 3rd day of the workshop. This is intended to assist government and private sector representatives to share experience and ideas to support efforts to prevent, investigate and prosecute money laundering and terrorist financing.

Report by the Typologies Working Group
Ms FOO Lee Mei (Malaysia Securities Commission), APG Typologies Working Group Co-Chair provided an update on the outcomes of the APG Typologies Working Group meeting held on Sunday (above).

Update on global Typologies work
The FATF Secretariat provided an update on the FATF's typologies work. The following FATF typologies reports were published by the FATF in the 12 months to October 2008 (see website www.fatf-gafi.org):

- Terrorist Financing (Feb. 2008)
- Money Laundering and Terrorist Financing Risk Assessment Strategies (June 2008)
- Proliferation Financing (June 2008)
- Money Laundering and Terrorist Financing vulnerabilities of commercial websites and Internet payment systems (June 2008)

The following typologies studies are ongoing within the FATF and are open to APG members to contribute:

- Money Laundering and Terrorist Financing risks in the securities sector
- Money Laundering through sporting clubs
- Money Laundering and Terrorist Financing through Money Service Businesses (joint project with MONEYVAL)

The FATF is also pursuing a global Strategic Surveillance project. The objectives of the project are:

- to detect and share types of criminal or terrorist activities that pose an emerging threat to the financial system
- to develop a strategic and long-term view of these threats through a regular Surveillance Discussion and the production of a global ML/TF threat assessment (GTA).

The Egmont Group highlighted a range of aligned work on typologies. Datuk Zamani noted with pride the leadership role that the APG and participants in APG meetings now have in the Egmont Group and highlighted the levels of cooperation between the groups.

The IMF highlighted work they are doing to use typologies to inform risk models for ML and TF. The IMF is developing tools to assist countries to estimate elements of risk, including the volume of proceeds of crime in the economy. The IMF has a project in Africa on precious metals and stones and related typologies. The IMF's Topical Trust Fund is moving ahead.

UNODC – GPML highlighted work going on across the region to support implementation of AML/CFT systems, including developing typologies.

Casinos & Gaming
The Casino report identified vulnerabilities from casino 'junkets' as a key finding, and this was developed during the workshop through a number of presentations by APG members on recent cases.

Proceeds of crime investigations & prosecutions
The session focused on recent cases and issues for conducting ML and TF investigations in parallel with investigation of predicate offences.

Vulnerabilities in the securities sector
Further to the FATF's global project on vulnerabilities in the securities sector, the APG Workshop focused on APG members' experience of ML/TF risks in the sector. The session resulted in shared regional experience and APG contributions to the FATF project. The

leader of the FATF Project on Securities, Mr Ian Matthews from UK Financial Services Authority outlined the project.

A half day breakout session was held to discuss the issue of securities sector vulnerabilities in detail. A range of issues were discussed, including the cross-jurisdictional influence of corruption; use of gatekeepers (lawyers) to construct ML schemes; weaknesses in CDD/KYC information collected at the broker level (over-reliance on banks). Some systems allow odd lots to be sold at a premium.

The group was also given a brief outline of the objective of FATF questionnaire on securities sector, and the information that is required.

Terrorist Financing - case studies & regional themes
The workshop noted that the Asia/Pacific region continues to suffer very serious terrorist financing threats and many jurisdictions have made considerable progress to tackle terrorist financing, but much work remains to be done. There had been discussion during the 2008 APG Annual Meeting of the need to better understand similarities and differences between terrorist financing models for different types of terrorist groups (e.g LTTE or Taliban which have standing military forces vs insurgent groups).

A half day Breakout session was held on building a culture of financial investigations to "follow the money" with an emphasis on case studies which highlighted parallel investigations of money laundering and predicate offences.

Presentations helped to build awareness of the tools to be utilised for successful ML & TF investigations.

A half day Breakout session was held on Proceeds of crime / terrorist funds – regional issues and opportunities for asset recovery. It was noted that APG members often struggle to use AML/CFT tools to effectively pursue and recover terrorist funds or proceeds of crime. The number of ML and TF prosecutions and the amount of proceeds of crime forfeited are comparatively low. A number of regional projects (StAR etc) were presented and discussed, highlighting the work being done to support enhanced international cooperation for asset recovery and related MLA.

Presentations were provided and discussions covered a wide range of topics, including opportunities to cooperate in relation to non-conviction based tools; developments with case management for both investigations and prosecutions as well as in depth analysis of MLA / proceeds matters in recent cases involving international cooperation.

Corruption, AML/CFT and recovery of proceeds
APG members continue to highlight corruption as a regional priority for AML/CFT. Anti-corruption/AML issues are included as a standing agenda item for each APG Typologies Workshop.

Improving quality of, access to and use of financial information for ML/TF investigations and prosecutions, including cooperation between public and private sectors
The workshop discussed issues for cooperation between the private and public sector to support improved access to CDD/STR information and improved understanding of ML/TF risks to support effective preventative measures. Presenters discussed practical issues for financial institutions and competent authorities, including identifying risks and applying 'red flags'. etc.

The workshop concluded with a discussion regarding publication of the Casino project report, APG typologies projects for the coming year and cooperative work on agreed topics including input to FATF global projects**.**

KEY PROJECTS AND THEMES

CASINOS PROJECT

Overview on Casinos Study Report[1]

The vulnerability of casinos was recognised in the revision of the FATF 40 Recommendations, with obligations on casinos being significantly enhanced. However, there remained a lack of recent regional or global typologies on casinos and gaming, which this report seeks to address.

This APG/FATF report considers casinos with a physical presence and discusses related money laundering (ML) and terrorist financing (TF) methods, vulnerabilities, indicators to aid detection and deterrence, international information exchange. The report considers vulnerabilities from gaps in domestic implementation of anti-money laundering / combating the financing of terrorism (AML/CFT) measures. Data in the report was derived from members of the FATF, APG, other FSRBs and open sources.

Online gaming and illegal gambling are beyond the scope of this study.

Overall, there is significant global casino activity that is cash intensive, competitive in its growth and vulnerable to criminal exploitation. This paper identifies significant gaps in awareness of ML typologies, gaps in regulatory and law enforcement responses, gaps in online gaming typologies, issues with controls over junkets / VIP programs, and significant issues with controls over 'high seas' gaming. The report identifies significant gaps in global coverage of AML/CFT controls over the sector, which represents a significant vulnerability. The report is a resource for policy formation.

The report identifies significant ML vulnerabilities and related case studies and typologies, but does not identify any instances of TF through the sector.

Chapter 1, *The Casino Sector,* presents a global overview of casinos organised by regions (some 100 countries). The overview sets out the numbers, locations and, in some cases, ownership of each sector and coverage of AML/CFT controls. The chapter discusses some statistics and estimates of revenues (over USD70 billion globally) and profits (where known). The chapter discusses emerging casino markets, including a number of developing countries with governance and capacity challenges.

Chapter 1 briefly discusses casino sector risk assessments as a basis for allocating regulatory and law enforcement resources. The report highlights the need to identify ML risks for both those jurisdictions with or without a casino sector.

Chapter 2, *Money laundering Methodologies and Indicators*, considers vulnerabilities such as casino chips, casino cheques, casino accounts and facilities, structuring through the casino, currency exchange, employee complicity, etc. The paper describes typologies, case studies, and includes a summary of practical indicators for the industry, regulators and law enforcement.

Casinos undertake high volume/speed financial activities that are similar to financial institutions, but in an entertainment context. Casinos are generally large cash-based businesses. Foreign exchange facilities and reduced transparency of 'high rollers' in VIP rooms present substantial challenges. The use of foreign holding accounts where funds in one jurisdiction are available for use in a casino in another jurisdiction without the need for a

[1] The APG and FATF have undertaken a joint study of vulnerabilities in the gaming and casinos sector. The project was led by New Zealand, with Ms Rachael Horton of New Zealand Department of Internal Affairs leading the work, including the drafting of the report. The work arose due to FATF and APG mutual evaluations and earlier typologies work, which noted a range of ML/FT risk factors related to gaming and casinos.

cross border remittance presents further issues.

Chapter 3, *Sector Vulnerabilities and emerging Issues*, explores a number of additional vulnerabilities and emerging issues. Casino-based tourism, or "junkets" are identified as a vulnerability as they involve the cross border movement of people and funds and often target high net-worth / VIP clients. Transparency of the movement of funds is an issue with junkets, due to gaps in controls, and weak implementation and supervision .

The emerging issue of high-seas cruise ship casinos and associated junkets is a challenge for regulators and law enforcement. The question of who has jurisdiction is prominent, including where the vessel is registered, where it operates from and where it visits. The paper notes that few jurisdictions regulate this sector.

With respect to VIP rooms and 'high roller' customers, vulnerabilities are noted with identifying source of funds and movement of funds. In many casino markets high-roller clients make up a large majority of casino turnover, yet only a very small percentage of casino patrons.

Other vulnerabilities discussed include corrupt or inadequately trained staff, new markets opening and terrorist financing.

Chapter 4, *Policy Implications*, reiterates various key findings of the report and discusses a number of policy implications, including:

- Online gaming requires further typologies study and sharing of cases and regulatory models is needed;
- A significant number of jurisdictions do not subject their casino sector to AML/CFT controls;
- When casinos are subject to AML/CFT controls, many jurisdictions lack effective implementation of preventative measures (CDD, STRs, internal controls);
- There is a lack of regulatory tools that carry effective, proportionate and dissuasive sanctions;
- AML/CFT controls over casino foreign branches, offices or subsidiaries are not well regulated and there is a need for international guidance and best practice;
- Casino foreign holding accounts are not clearly covered for AML/CFT, which allows movement of funds without sending a cross-border wire transfer;
- Controls over VIP rooms vary and some jurisdictions lack clear powers regarding collecting and sharing information of VIP program participants;
- High-seas gaming is a large market over which there is little regulatory control;
- Many jurisdictions' casino regulators lack AML/CFT capacity and experience;
- International cooperation between casino regulators on AML issues is lacking and it is not always clear who are the competent authorities for information sharing.

The full text of this report can be found at:

www.apgml.org/documents/default.aspx?DocumentCategoryID=6

Case Study – Macao, China

A man approached casino X and requested deposits of USD600k cash into it for remittance to its branch in country B. He claimed that the purpose was for his own gaming and entertainment later in this branch. Casino X rejected his request because it was an unusual practice and he was not their registered customer, but allowed him to deposit the cash at its cash vault until they got confirmation of identity from their branch. Soon after the deposit the police arrested the man and found that the cash deposited in X was actually the proceeds of his robbery.

Open Source example

Two Bank of China managers convicted of $688m fraud
1 September 2008 TODAY (Singapore)
Two former Bank of China managers and their wives have been convicted of conspiracy charges in an elaborate, 13 year scheme to embezzle US$485 million ($688 million) from a state-owned bank and launder the money in other countries. The bankers created a number of shell corporations in Hong Kong and funnelled money through Canada and the United States. Among a host of other methods, the bankers tried to launder more than US$3 million by making deposits at several Las Vegas casinos. The Casinos were not accused of wrong – doing.

SECURITIES PROJECT
Update of FATF project

The typology was approved at the FATF WGTYP meeting and plenary in June 2008. The project team has conducted a literature review, and found little information in the public domain: hence the need for the current study.

The FATF/Moneyval typologies meeting was held in Monaco in November 2008. A workshop was held on the securities typology, which was very well attended. The APG secretariat provided information to the workshop on APG members' experience that was well received. The results of the workshop went some way to informing the project team's thinking on the vulnerabilities in the sector and the challenges faced by the industry and competent authorities.

The typology questionnaire was sent out on 10 November 2008. The project team has now received 40 responses, including from APG members. These responses have given a broad overview of how jurisdictions supervise the securities industry, and have highlighted a range of red flags/indicators of ML in the sector.

The project team has now drafted the main headings for the areas that the report should address; and has a good idea of the public sector's views on this subject, but much less about the private sector's experience. The aim is to produce a report that is relevant to the private sector. The project team will, over the next few months, be consulting with the private sector.

The typology report is due to be adopted at the FATF plenary in October 2009. The relevant documents, including the questionnaire responses are available on the typology secure website.

Outcomes from APG Typologies Workshop in Sri Lanka in Oct 2008 on securities sector vulnerabilities

- Many cases of predicate offences in the capital market reported
  - Few follow up ML investigations
  - Reflects weak capacity to investigate ML
- A few cases showing simple purchase of securities
  - Using nominees or 3rd parties
  - A number of cases of corruption proceeds invested in capital markets
- Securities regulators are using STRs to ID predicate securities offences
- All case presentations and jurisdiction reports available to FATF members and project group
- APG countries need to better understand the risks and vulnerabilities
  - Demand for typologies and information to raise awareness
- Strong interest from APG jurisdictions – probably missing a lot of cases

  - Welcome the Moneyval paper and the upcoming FATF report
- Some jurisdictions allow securities regulators to investigate ML offences related to proceeds of predicate offences involving securities e.g. Malaysia
- Opportunities for ML typologies to receive more focus amongst securities sector regulators
  - APG meeting included large numbers of securities regulators
  - They noted possible opportunities for IOSCO and or others to do more to keep this on the regional agenda in the Asia/Pacific region
  - APG Typologies WG Co-chair is from Malaysia SC
- APG mutual evaluation reports have some useful information on the sector, but not a lot on ML/TF risks specifically in the sector.

Example of addressing ML risks in countries without a stock exchange - Macao, China

- No securities market in Macao, China
- Overseas securities through banks and securities companies operating in Macao.
- Securities usually kept on behalf of the investors by the overseas partners of the Macao banks and securities companies. Payments are routed through banks.

**Authorities ID purchase and sales of stocks to conceal real source and ownership of funds as key ML risk in the sector.

- A number of STRs and two cases relating to securities:

CASE STUDIES (Supporting the APG's input to the FATF project on vulnerabilities in the securities sector)

Korea

An STR identified that 'A' had frequent large fund transactions with unspecified persons and securities accounts at several companies. It was suspected that A was manipulating market price using bank accounts of assumed identities with embezzled money through a computer IP.

Analysis revealed that a director of U Co., Ltd embezzled corporate funds and deposited them as payment for shares and was manipulating market price using securities account in the name of unspecified persons with the embezzled funds. The FIU forwarded the STR to law enforcement agencies.

Executives of entities involved conspired to manipulate stock price more than 10 times through false stock trading orders using illegal proceeds worth 35 billion won.

Malaysia

An investment scam known as Swisscash offered an investment scheme through several websites. It allegedly invests and holds itself as investing in among others, offshore development projects, hedging, equity, high yield investments, commodities and foreign exchange. The scam offers returns up to 300% within 15 months of investment.

An investor is required to place a minimum cash investment that is then converted into 'e-points'; US$1 is equivalent to 1 'e-point'. This 'e-point' can be exchanged for cash through the investor's trading account or sold to other investors. Similar to a pyramid scheme, existing investors (known as up-liners) who bring in new investors (known as down-liners) will receive lucrative commissions and incentives.

Methods employed in this case include:

- Cash couriers/currency smuggling (concealment, security, amounts etc)
- Use of shell companies/corporations
- Investment in capital markets
- Use of offshore companies/ banks (roles of trust and company service providers)
- Use of foreign bank accounts
- Currency exchanges/cash conversion
- Use of the internet and new payment technologies (encryption, payment systems etc)

Malaysia

Investors from two foreign countries were duped into investing their money in products traded on a fictitious stock exchange via cold calling activity. The cold callers claimed that they were representatives of a brokerage firm.

The investors were advised to refer to three fictitious websites (the broker, a fictitious exchange, a fictitious capital market regulator) to give appearance that the proposed investment scheme is genuine. The investors remitted money into a bank account in Malaysia which was then transferred to another bank account in Malaysia using cash and house cheques. Methods employed in this case include:

- Investment in capital markets
- Use of shell companies/corporations
- Use of the internet and new payment technologies (encryption, payment systems etc)

Malaysia

Company ABC held seminars where the suspects made representations to potential investors that their monies would be used to invest in futures instrument such as Crude Palm Oil. Investors made direct deposits to the company bank accounts or via several futures brokers. The monies banked-in by the investors were later withdrawn and used for payment of some promised returns, purchase of assets, personal expenses and financing other businesses owned by the suspects.

Malaysia

Mr. W opened five trading accounts and two margin accounts at five stock broking companies in various names.The scheme was carried out on four separate occasions, involving two cycles where the proceeds from the first cycle were used to facilitate the scheme carried out during the second cycle. During the first cycle, Mr. W placed odd lot buy orders using trading accounts and simultaneously placed odd lot sell orders through another stockbroker to match the trades, but at exorbitant prices. Mr. W controlled both the selling and the buying parties.

Mr. W had then took out the proceeds at the selling brokers and defaulted on the buying brokers' side. This allowed him to raise huge amount of sales proceeds that were used to increase his margin and facilitate his scheme during the second cycle. During the second cycle, the same modus was used but involved different stock broking companies.

Philippines

Two suspects maintained 12 bank accounts where significant sums (exceeding USD1million) were deposited monthly. Funds were used to buy government securities (USD5million) among other assets even though neither suspect was required to declare their sources of income. The funds were proceeds of drug sales.

CORRUPTION AND AML
Report From Typologies Workshop in Sri Lanka

APG members continue to highlight corruption as a regional priority for AML/CFT. Anti-corruption/AML issues are included as a standing agenda item for each APG Typologies Workshop. Ms Rita O'Sullivan, ADB / OECD Anti-Corruption Initiative provided an overview of the initiative's recent work. Mr I Nyoman Sastrawan & Mr I Gede Arnawa, of Indonesia's FIU (PPATK) gave a presentation of recent cases, including one case which clearly demonstrates the use of financial intelligence to pursue cases of bribery of foreign officials and the role of receipt of information from foreign counterparts spontaneously and on request. Results from the case included over USD16million being frozen and a very significant fine.
Ms Cari Votava provided a presentation on the World Bank's Stolen Assets Recovery (StAR) project. The workshop had some discussion on the StAR Guidebook on non-conviction based forfeiture.

Case Studies
Indonesia – Rice scandal case

In 2007, an Indonesian state-owned company had a contract for buying rice worth US$10 million with a foreign company. The rice procurement was conducted through an intermediary. The foreign company advanced US$1.6 million that is alleged was a bribe to a high ranking public officer associated with the state-owned company in return for being awarded the contract to supply rice to Indonesia.

Some of this money was re-deposited to an account belonging to a private Company which was owned by a relative of the public official. From this company's account, funds were forwarded to accounts owned by the family members of the public official and was used for buying assets and other investments.

Bank accounts, land, luxury houses and cars belonging to the public official and his family, amounting to more than US$16 million in value were frozen and seized. The official was sentenced to 10 years in prison with IDR500 million fine and US$16 million in penalties. Cooperation with other agencies and foreign FIUs was critical in securing the evidence.

FEATURE CASE – INTERNATIONAL COOPERATION
Operation Outrigger: Fiji ~ Hong Kong ~ Australia ~ New Zealand ~ Malaysia

Summary

In June 2004, a substantial ICE clandestine laboratory in Fiji was raided resulting in the arrest of four foreign nationals and two Fijian citizens as well as seizure of 2.8 kg of ICE and chemicals that could produce 800 kg of ICE, worth approximately of USD500 million.

At that time, it was the largest clandestine laboratory ever detected in the Southern Hemisphere and one of the largest in the world – having the potential to produce 500 kg of crystal ICE per week. The six arrested persons were charged, convicted and sentenced to imprisonment in Fiji.

At the same time, the alleged mastermind and his wife were arrested in Malaysia but were later released due to insufficient evidence. They were deported to Narau and Hong Kong, being their respective places of residence.

In August 2004, the wife of the mastermind was arrested by the Hong Kong Police for money laundering upon her deportation from Malaysia. Searches of her residence and safe deposit

boxes resulted in the seizure of HK$22 million in cash and numerous luxurious watches and jewellery items, valued around HK$10 million, which were suspected of being the proceeds of crime.

In April 2008, the wife was convicted of money laundering and sentenced to five years of imprisonment. The conviction depended entirely on circumstantial evidence that included her concealment of a large amount of cash at home and in the safe deposit boxes, and her failure to account for the sources of her assets. Confiscation proceedings for HK$32 million in assets have commenced.

International cooperation

Operation Outrigger was a hallmark of international cooperation, involving 14 months of intensive investigation by agencies from five jurisdictions – Australia, Fiji, Hong Kong, Malaysia and New Zealand.

As virtually all operational activity was occurring in Fiji, New Zealand was engaged to assist with technical assistance in-country. The Suva TCU (transnational crime unit) played a critical role. Regular phone conferences using liaison officers in Malaysia, Fiji and Hong Kong – and their host agencies ensured a consistent flow of information.

A Joint Agency Agreement (JAA) was formulated in Sydney in 2004 between all the jurisdictions involved – focussing on the roles and responsibilities each had during the investigation and at the time of resolution. The JAA was designed to facilitate a smooth exchange of intelligence and ensure timely coordination of operation activity. (Importantly, at a joint agency meeting several months after resolution, future targeting opportunities were discussed – which underscored the openness that had been achieved during Operation Outrigger.)

JURISDICTIONAL TYPOLOGIES

All APG members agreed to provide detailed typologies information on a range of typologies topics. The collection template supported each jurisdiction's preparation of a detailed typologies report on current methods and trends of ML and TF. In 2008 the collection pro-forma included a focus on vulnerabilities in the securities sector.

APG members and observers were asked to prepare a report providing case studies, statistics and key findings for each of the listed categories.

CASE STUDIES

1. Supporting the APG's Input to the FATF Project on Vulnerabilities in the Securities Sector

ML/TF Techniques identified involving securities

Techniques reported:

- Manipulation of market price by buying and selling in large volumes and using false stock trading orders. Fraudulently obtained funds used in transactions to launder money. (Korea)
- Scam inviting investors to pool funds in fictitious securities through a maze of accounts. Also used cold calling as invitations. (Malaysia)
- Using trading accounts and margin accounts at different stock broking companies to place simultaneous buy and sell orders that matched – but at exorbitant prices. Proceeds removed at selling broker's side but default on buying broker's side. The proceeds increased the margins and facilitated a second cycle that used the same modus operandi but involved different stock broking companies. (Malaysia)

Open source example

British stockbroker jailed for laundering
27 November 2008 South China Morning Post
A British stockbroker was jailed yesterday for laundering about HK$680 million allegedly generated from a "boiler-room" fraud operation based in Britain.

Judge Joseph Yau Chi-lap in the District Court sentenced Jerome Hertzberg, 38, to three years and four months in jail after he pleaded guilty on November 24 to five charges of handling illegal proceeds.

The Hong Kong Commercial Crime Bureau said it was believed that thousands of investors, mainly elderly people in the UK, had fallen victim to the boiler-room investment scheme, in which they were lured into making payments for illegal trades in shares.

Police said about 30,000 people every year were ripped off in such schemes, losing around £300 million (HK$3.5 billion) in Britain alone.

2. Money Laundering & Terrorism Financing Methods

2.1 Alternative remittance services and underground banking

Techniques reported:

- Use of Providers of Designated Remittance Services (PoDRS) to transfer proceeds of crime abroad. Source of funds was imported drugs. Even though vast

sums were detected and the businesses closed down, remittances quickly recovered through other means to levels higher than before intervention. (Australia)

- Small groups of peoples on short term visas laundering bulk amounts of cash offshore via PoDRS. Rather than structuring funds under reportable limits, bulk quantities were preferred in the hope of remitting as much as possible offshore before detection. False identities were used as risk mitigation by the offenders. (Australia)
- Groups of individuals attending an agency of a registered PoDRS at the same time, providing minimal identification and sending funds to various beneficiaries offshore. (Australia)
- PoDRS failing to report transactions and/or providing falsified information to the FIU. (Australia)
- Poorly trained proprietors of a sub-agency being exploited by a group utilising their services near closing time and providing false names. Reporting compliance obligations were poorly understood. The super-agents encouraged a relaxed attitude towards sub-agents reporting compliance due to commissions earned on the business. Use of super-agents clearing accounts clouded the identity of transactions processed by sub-agents. (Australia)
- In response to enhanced AML/CTF regime, practice by PoDRS of seeking new ways to avoid reporting – such as encouraging structuring and use of multiple fictitious names in the 'Ordering Customer details'. (Australia)
- Existence of registered PoDRS infact providing other types of sophisticated Financial Services (eg foreign exchange contracts). (Australia)
- Use of company names to open multiple accounts in various domestic banks to facilitate underground remittance business. Flyers advertised the business and customers could use the company accounts to avoid government agencies tracing the real remittance originators. (Chinese Taipei)
- Structured outwards transactions through a Western Union Branch revealed by an STR. (Cook Islands)
- Third parties invited via internet to cash counterfeit travellers cheques (which were undetected by the banks and foreign exchange dealers), deduct a commission, and remit balance through Western Union. (Fiji)
- Use of multiple accounts in a child's name to receive deposits of cash and cheques, and conduct inter-bank transfers to try and conceal ownership of the monies. (Macau, China)
- Alleged terrorist sending remittances from off-shore to Pakistan. (Pakistan)
- Terrorist receiving money remitted from offshore – and via physical cash couriers, netting off arrangements, under/over invoicing and smuggling of currency/commodities. (Sri Lanka)

Open source example

Pakistani national pleads guilty to conspiracy to operate an unlicensed money remitting business

5 February 2009 Justice Department Press Releases

Imdad Ullah Ranjha, age 34, a Pakistani national residing in Glen Burnie, Maryland, pleaded guilty today to conspiring to operate an unlicensed money remitting business, announced United States Attorney for the District of Maryland Rod J. Rosenstein.

According to his guilty plea, Imdad Ranjha worked at Hamza, Inc., a money remitter business in the District of Columbia operated by co-defendant Saifullah Ranjha (S. Ranjha). A cooperating witness, acting at the direction of law enforcement, gave S. Ranjha and his associates a total of $2,208,000 in government funds in order to transfer the monies abroad

through an informal money transfer system called a "hawala," using a network of persons and/or businesses to transfer money across domestic and international borders without reliance upon conventional banking systems and regulations. The cooperating witness represented that the monies were the proceeds of, and related to, his purported illegal activities, including drug trafficking.

S. Ranjha arranged with Imdad Ranjha and other associates for the equivalent amount of monies, minus commissions, to be delivered to the cooperating witness, his third party designee, or a designated bank account in Canada, England, Spain, Pakistan, Japan and Australia.

Saifullah Anjum Ranjha, age 45, a Pakistani national residing in Washington, D.C. and Maryland, pleaded guilty to conspiring to launder money and to concealing terrorist financing and was sentenced to 110 months in prison.

United States Attorney Rod J. Rosenstein thanked U.S. Immigration and Customs Enforcement, the Federal Bureau of Investigation and the Internal Revenue Service - Criminal Investigation for their investigative work. In addition, Mr. Rosenstein thanked our international partners, the Spanish National Police; Australian Federal Police; London Metropolitan Police; and Royal Canadian Mounted Police for their help.

33 held in raids on underground bank
18 September 2008 South China Morning Post
Police arrested 33 people in a crackdown on what they believe is an underground bank that allegedly laundered HK$288 million. One money laundering case involved HK$44 million channelled through the bank account of a company set up by two Hong Kong residents.

2.2 Cash Couriers and currency smuggling (concealment, security, amounts etc)

- Proceeds of sale of imitation goods attempted to be carried through airport with no declaration. (Australia)
- Identity/access cards issued by an Airports Authority to a person involved in remittance business in a different country which authorised the person to receive and deliver foreign currency by providing access to restricted areas in the airport where cash couriers that were employees of an Airline. (Australia)
- Airline pilot being used to smuggle large amounts of cash out on behalf of a money laundering syndicate. The pilot's position facilitated easier passage past border controls. (Australia)
- Use of PoDRS to remit proceeds of crime to Nigeria via China. PoDRS knowingly allowing group members to use false names in exchange for secret commissions on top of normal fees. (Australia)

2.3 Trade-related money laundering and terrorist financing

- Tax fraud (false claims) incorporating stolen and false identities used to open and operate bank accounts, obtain credit cards and register companies – even opening serviced and virtual offices. A constant movement of funds between accounts gave the appearance of legitimacy. International accounting firms (gatekeepers) were employed to further distance the offender from the fraud. Ultimately layered funds were withdrawn in a multitude of forms – including structured transactions. The offender was a financial advisor, involved in drug crime. (Australia)
- Use of forged trading certificates importing commodities. Finance was obtained and the providers defrauded. Customs certificates, bills of lading, commercial invoices and shipping bills were all employed in the fraud. Proceeds were ultimately moved through underground banking systems and by couriers. (Chinese Taipei)

- Over and under invoicing of goods and using backdated letters of credit. Fraud spread over three countries. (Cook Islands)
- Importation of concentrated juice products from the US. Collusion of senior employees resulted in use of an agent in Australia who provided inflated invoices. Excess funds generated were remitted into related accounts using wire transfers.
- Proposed lease finance for heavy equipment. Initially instalments were paid, but then the outstanding payment was made in a lump sum. Suggestion was that a bank loan was used in an attempt to hide true source of illicit funds. (Indonesia)
- Unauthorised importation of medical supplies with proceeds deposited into multiple trading companies. Fictitious debts to those companies from off-shore companies were supposedly settled with the off-shore companies drawing cheques in favour of the suspect. (Japan)
- Suspects with effective control over a legitimate company defrauded it by transferring significant funds to an offshore corporation on the basis of false invoices. (Korea)
- Corrupt government officials in a Customs departments approved false exports in order to gain sales tax refunds, Customs rebates and other benefits. (Pakistan)

Open source examples

Cash laundered 'through ports'
17 February 2009 Gulf Daily News

A number of Gulf ports are being used for trade-based money laundering, experts said yesterday. Under or over-invoicing of goods can take place at intermediary ports in the Gulf while re-exporting goods to the final destination, said International Chamber of Commerce's (ICC) Bahrain Trade Finance Forum chairman Pradeep Taneja.

"Several invoices issued and routed through various financial institutions lead to multiple payments for the same goods," he said.

"Also, it is essential to know if the money is diverted for tax evasion, terrorist funding or the like."

Fake internet drugs risk lives and fund terrorism, warns journal editor
13 February 2009 Drug Week

People who buy fake internet drugs could be risking their lives and supporting terrorism, according to an editorial in the February issue of IJCP, the International Journal of Clinical Practice.

Editor-in-Chief Dr Graham Jackson, a UK-based Consultant Cardiologist, has called for greater public awareness of the dangers and consequences of the counterfeit drugs market, which is expected to be worth £55 billion by 2010.

"In one scheme, Americans buying fake Viagra on the internet were actually helping to fund Middle East terrorism, unknowingly jeopardising the lives of men and women serving in their own armed forces."

2.4 Real estate – laundering or terrorist financing through the sector

- Use of title to real estate to bribe an official for assistance in an unrelated commercial dispute. (Chinese Taipei)
- Proceeds from scam online gambling invested into the construction of a resort. (Fiji)

- STR from a real estate agency reporting that foreigners purchased property without the usual evaluation. The agent discovered images of the property were being posted on the internet to attract overseas buyers. Appears to be part of a layering of proceeds. (Fiji)
- Long serving bank official invested corruption related funds in real-estate and attempted to hide beneficial ownership by using names of dependents and other associates. (Pakistan)

2.5 Abuse of non-profit organisations / charities

- Fundraising on behalf of an identified terrorist organisation with large number of IFTIs to businesses in a third country (believed to be front organisations to launder funds for the terrorist organisation). Wire transfers to international bank accounts and bank transfers to accounts held within Australia. Internet banking utilised frequently. (Australia)
- Directors conspired to defraud a foundation that was to be used only for social welfare purposes – and any investments were to be cleared with a central supervisory authority. The Directors ignored the controls and caused the funds to be paid directly to them. (Chinese Taipei)
- Religious society remitted funds to a suspect terrorist organisation based in Australia. (Fiji)
- STRs identified PEPs defrauding not for profit non-government organisations to fund election campaigns. (Philippines)

2.6 Money laundering associated with illegal logging / illicit resource extraction

- Corrupt army member received funds from a company associated with illegal logging. Travellers cheques bought in different names were used to disguise the proceeds. (Indonesia)

2.7 Structuring / smurfing

- Bank drafts in false names and payable to false payees, purchased over an extended period, and under reporting thresholds, then either posted or couriered offshore to be deposited and destined to be used to facilitate large importation of precursor chemicals. (Australia)
- Structuring of over 1500 cash deposits and wire transfers using a network of associates using false names and addresses moving from one bank branch to the next. All deposits under the reporting threshold. Up to AUD100,000 per day to total in excess of AUD14m. (Australia)
- Purchase of multiple insurance products to hide corruptly obtained funds. Funds were structured into bank accounts then transferred to insurance companies to avoid the insurance companies reporting the transactions. (Indonesia)

2.8 Wire transfers

- Proceeds of narcotics trafficking were gambled using third parties to purchase gaming chips and conduct multiple chip cash outs. Large cash payments sent through remittance dealer who was complicit and non-compliant with reporting procedures. (Australia)
- Individuals were recruited at night clubs to send wire transfers on behalf of POIs to fund cocaine importation. Funds were sent to company accounts in the US. (Australia)
- Scam investment lured investors to wire money to an account. No returns / dividends ever made. (Fiji)
- Third party (abroad) used to pay premium on an insurance policy. Premiums were overpaid (by a factor of 13 times) and overpayment was directed to a company account in the host country of the insurance policy. (Indonesia)

- Proceeds of 'Nigerian' Fraud wired via Japanese bank account and then forwarded to other countries. (Japan)

2.9 Investment in capital markets

- Proceeds invested through share trading accounts held off-shore with profits returned to criminals in Australia via international funds transfers. (Australia)
- Trades through a Contracts For Difference (CFD) account were restrained. The subject had used false identification to open a trading account via the internet. Deposits to the related bank account were structured to avoid reporting limits. (Australia)
- Free medical scheme seeking donations in promise of dividends and medical services. Scheme closed abruptly after attracting FJ$1million. (Fiji)
- Multiple accounts in false names used to apply for a Public Offering of shares. Once allocated, off market instructions transferred funds to one account. (India)
- Proceeds of company fraud invested in capital markets. (Indonesia)
- Illegal fund raising caused multiple small investments to a single account. (Korea)
- BVI companies traded large funds for stocks in two companies with a parent-subsidiary relationship. Major shareholder of the BVI company was an employee of the subsidiary. It appeared the BVI company was conducting huge trade frequency in an attempt to encourage investors in the stocks. (Macao, China)
- Directors of a Pakistan registered company, acting in concert, acquired a majority shareholding of the company with inside knowledge of a takeover bid prior to any public announcement. Shares were sold to a dormant UK based related company, later selling those same shares to the takeover company at a profit of some 2000%. The illegal gain was then laundered through some 26 bank accounts. All proceeds were ultimately identified and frozen by the Securities Exchange Commission. (Pakistan)

2.10 Use of shell companies / corporations

- Tax avoidance using legitimate profits achieved by a tax haven company being directed to an Australian company through payment of false invoices. (Australia)
- Proceeds of a fraud committed on a European bank laundered in Australia through purchase of assets. Funds were deposited to Australian bank accounts of registered entities via a Dutch corporate bank account. (Australia)
- Shell companies in Australia receiving large amounts of funds from Switzerland and Liechtenstein that originated in East and South East Asia from drug importations to Australia. Suspects also control shell companies in the BVI and Vanuatu. (Australia)
- Shell company created in same name as unrelated company that had significant funds in a bank account (information from former bank employee). Shell company opened a foreign currency bank account and defrauded the legitimate company by tricking its bank into transferring the funds. (Chinese Taipei)

2.11 Use of offshore companies/ banks (roles of trust and company service providers)

- Sale of shares in an Australian company by a BVI company with subsequent transfer of funds to a family trust in Australia. Tax fraud. (Australia)
- Flow of funds designed to avoid tax between local and off shore companies that were all part of the one group. (Macau, China)

2.12 Use of nominees, trusts, family members or third parties ('onshore')

- Misappropriation by employee of Public Trustee and use of third parties to open accounts and use forged payment vouchers to steal monies from beneficiaries accounts. (Fiji)

- Misappropriation by employees of Public Trustee colluding with guardians of minors to raise payment vouchers and steal funds. (Fiji)
- Using a third party at a spouses company to appropriate funds and deposit / withdraw same. (Fiji)
- Investments through multiple folios using third party cheques and demand drafts.(India)
- Use of third party to open bank account on behalf of a prisoner which was then used in an ongoing drug business. (Indonesia)
- Corrupt government official used third parties to invest proceeds in term deposits on his behalf, which was later paid into new term deposits in the name of his daughter. (Indonesia)
- A civil servant used a relative to open investment accounts offshore and invest proceeds of corruption. While relative was the nominal owner, the civil servant was the actual beneficiary by virtue of a power of attorney. (Macao China)

Open source example

Ex-banker sued over dirty money
22 January 2009 Philippine Daily Inquirer

The Anti-Money Laundering Council (AMLC) has accused a former branch manager of Equitable-PCI Bank (EPCIB) of facilitating the laundering of dirty money allegedly earned from drug dealing in Pasig City by the Boratong group.

Godofredo Medenilla, manager at EPCIB branch on Sixto Antonio Avenue in Pasig, was charged with money laundering in the Department of Justice early this week.

The group had deposited more than P900 million from 2001 to 2006, according to the AMLC.

2.13 Use of 'gatekeepers' professional services (lawyers, accountants, brokers etc)

- Entities in a tax haven transferred funds to an account linked to an accountant who was enlisting high net worth clients to participate in an offshore scheme that resulted in tax deductions for the clients. (Australia)
- An accountant offered money laundering and tax evasion services to clients. Money was remitted to tax havens using a corporate infrastructure. (Australia)
- An attorney associated in an investment company defrauded it by colluding with another company employee. (Chinese Taipei)
- A notary received bribes to arrange residency status by bogus marriage. (Japan)

Open source example

Chen Shui-bian's accountant admits forging documents
5 February 2009 South China Morning Post

The chief accountant of former Taiwanese president Chen Shui-bian pleaded guilty yesterday to document forgery in the special state fund embezzlement case, saying she was doing so under the instruction of her former bosses.

However, the chief accountant pleaded not guilty to embezzlement and money-laundering charges, saying she merely followed Chen's instructions and those of his wife and the two aides in relation to the special state funds and the wiring of money abroad.

Chen Chen-hui, the former president's accountant for two decades, was the first of 14 defendants in the massive corruption case to be detained, on September 25. She was released on November 20 after she had agreed to become a witness and handed over a computer drive containing records of all revenue and expenditure by the former first family between 2000 and last year.

2.14 Use of foreign bank accounts

- Numerous IFTIs to a tax haven under the reporting threshold. (Australia)
- Purchase large quantities of duty free cigarettes and alcohol for local sale and avoiding tax obligations. False export receipts were used to mask the imports. Original payments were made using bank accounts in Belize – funds for which were sent from Australia, Belize, Hong Kong and Vietnam. (Australia)
- A scam illegal foreign exchange investment company was used to solicit investors. (Pakistan)
- Probable layering phase of money laundering by Hawala type group using a network of foreign accounts for vast numbers of transactions against fraudulent exports. The group also capitalised on sales tax refunds, customs rebates and other benefits. (Pakistan)

Open Source example

Morgy busts claw back $175m
11 February 2009 New York Daily News

Greed can be good for the city, which yesterday collected $175 million in fines and forfeitures from two disgraced executives and a bank that laundered money for Iran.

Manhattan District Attorney Robert Morgenthau collected $109 million from former Tyco executives Dennis Kozlowski and Mark Swartz after their fraud and larceny convictions.

He also won $66 million from Lloyd's Bank for hiding the origin of Iranian money in New York accounts.

Morganthau said eight more banks are still being probed, and at least one might generate a larger fine than Lloyd's.

2.15 Currency exchanges / cash conversion

- Conspiracy with principals of a currency exchange business to launder the proceeds of a drug syndicate. Structure deposits were remitted overseas. (Australia)
- CEO of a finance company colluded with a suspect to exchange AUD for USD and travellers' cheques. False names were used and structured transactions combined with altering the exchange rates in an attempt to hide the true amount of the transaction. (Australia)
- A company diverted duty free exports (cigarettes) to the domestic market – and disguised using false sales to ship's crews. Tax avoided. Company directors purchased significant amounts of foreign currency. (Australia)
- Probable bribery of PEP who collected foreign currency from a money changer that had been paid in from local currency by the suspect. (Indonesia)

2.16 Use of credit cards, cheque, promissory notes etc

- Purchase of legitimate bank cheque using a fraudulent cheque. Legitimate cheque use to purchase foreign currency. Complicity by teller issuing bank cheque was suspected. (Australia)

- Theft of cheques by an employee which were converted to real estate and vehicles. (Fiji)
- Collusion with a postmaster who intercepted cheques (issued by local govt agency). Cheques altered and cashed. (Fiji)
- Forgery of company vouchers to raise cheques by an employee. (Fiji)
- Payments to former directors using bank cheques purchased with cash. (Fiji)
- Company drawing valueless cheques. (Fiji)
- Attempt to withdraw cash at ATMs using stolen credit card details. (Pakistan)

2.17 Purchase of portable valuable commodities (gems, precious metals etc)

- Purchase of silver using cash amounts under reporting limit. (Australia)
- Suspects in cocaine importation opened bank accounts in the names of infant grandchildren through which cash was channelled to buy assets (cars, property). Australia
- Conversion of proceeds of crime into Gold bars (Chinese Taipei)

Open Source example

Hunt for Gang's gold
11 July 2008 Birmingham Mail

UK Gang converted the proceeds of an elaborate identity theft scam into gold bullion. The suspects posed as potential buyers, copying homeowners' details and using the information to alter title deeds and secure massive mortgages over the properties.

2.18 Association with corruption (laundering proceeds & corruption of AML/CFT measures)

- Corrupt government official receiving bribes from importer of rice. **Rice scandal case – separate write up coming from Djoko.**
- Judicial official with unexplained assets and suspicion of bribery in a large court case. (Indonesia)
- Govt official stole superannuation funds which were laundered through third party bank accounts and insurance companies. IDR9.2 billion (Indonesia)
- Govt official accepting bribes to promote public servants and facilitate foreign exploration for natural resources. (Bangladesh)

Open source examples

Macau bribery and money laundering charges
20 February 2009 The Australian

Two Macau based casinos, the City of Dreams and Crown Macau have been mentioned in a Macau court in connection with bribery and money laundering allegations against a former Macau government official. The same official was arrested in late 2007 and later sentenced to 27 years in prison after being convicted of taking millions of dollars in bribes. The trial would centre on 19 land deals, public works projects and private development projects.

Chen's wife admits forgery, laundering Taiwan's ex-first lady pleads guilty
11 February 2009 South China Morning Post

Former Taiwanese first lady Wu Shu-chen pleaded guilty at a hearing in Taipei yesterday to laundering US$2.2 million and forging documents

But she denied more serious embezzlement and corruption charges, in a strategy seen as an attempt to clear herself, her husband ex-president Chen Shui-bian and her son.

Wu was charged along with Chen with taking at least NT$491.8 million (HK$117 million) in bribes, embezzling NT$104 million in special state funds, and laundering US$21 million abroad. "[In] the Nankang case and the related money laundering, I plead guilty," she told a three-judge panel at Taipei District Court, referring to a government exhibition centre construction project in Nankang, Taipei, in 2003.

She admitted that through a co-defendant she helped a businessman win the contract for the project, for which she was given a commission of US$2.2 million. She said she later wired the money abroad without telling the former president.

On the embezzlement charges, Wu admitted document forgery by using receipts provided by others to account for funding claims made by her husband.

Crime track - IT helps police crack online crime gang
19 January 2009 Bangkok Post

It took police two years to trace and eventually uproot an international crime syndicate allegedly headed by Malaysian drug trafficker Abubaka bin Sulaiman on Jan 10. Many high-ranking government officials allegedly back the gang.

The crime gang is notorious for online football gambling and is involved in various other crimes such as kidnapping, extortion, drug trafficking, document forgery, money laundering and murder.

Police seized over a billion baht in assets belonging to about 1,000 people suspected to be involved.

"Information technology was the key to the crackdown. It is not easy to obtain access to information, but once we get it, the whole case can conclude rapidly," said Crime Suppression Division chief Pongpat Chayaphan.

Police worked in conjunction with the US Drug Enforcement Administration on the case.

2.19 Use of the internet and new payment technologies (encryption, payment systems etc)

- The ACC identified a drug trafficking group associated involved in online soccer betting. The group used a central contact in Australia, who then used an overseas contact to place bets on a global soccer betting website.

  The group used the funds generated or lost through soccer-betting to offset drug debts and earnings. This method was particularly useful for offsetting debts to internationally-based members of the syndicate, negating the need to transfer funds overseas through traditional banking networks or remittance systems. (Australia)
- The POIs of a computer crime task force were involved in the purchase of stolen bank account and credit card details from Russia and Eastern Europe via the internet. These were purchased through IFTIs of approximately AUD$2,000 and by way of e-Gold payments. The principal POI was arrested on 26 fraud and computer crime offences in relation to using these bank details to withdraw funds without authorisation in internet transfers to ‘mule’ accounts. AUSTRAC searches revealed that another POI in this syndicate had previously come to

notice of authorities for suspected involvement in internet bank fraud through phishing.

A laptop seized on the arrest of the principal POI revealed details of IFTIs transacted through Western Union and e-gold. Russian and other recipients identified from these transactions facilitated the identification of additional POIs from further AUSTRAC searches. The commodity (e-gold) transactions used by this POI avoided reporting to AUSTRAC.

- Overseas based student created false websites leveraging off a legitimate on-line book seller. The websites solicited legitimate customers and directed their payment for books (USD5.7 million) into the suspect's local and foreign accounts. (Malaysia)

Open source example

Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges
22 July 2008 PR Newswire

The E Gold operation provided digital currency services over the internet. Several characteristics made it attractive to users – such as not requiring users to provide any specific identity. The ability to transfer credit between e-gold accounts enabled users to avoid usual money transmission controls.

2.20 Identity fraud – use of false identification

- Large scale use of multiple false identities and bank accounts, personal loans and credit cards. Proceeds of loans used as 'proof' of savings to secure additional loans. (Australia)
- Use of false names to transfer large amounts of money offshore to facilitate drug importations. (Australia)
- Use of forged credit cards (Fiji)
- Falsified passports use to facilitate cashing of forged VAT cheques. (Fiji)

2.21 Other methods/emerging vulnerabilities

- Skimming devices on ATMs that could siphon money from client accounts. Syndicate members came from Canada and had links to other groups in NZ and other States of Australia (Australia)
- Use of cash passport accounts providing access to pre-paid cards. This enables the holder to obtain currency anywhere in the world. (Australia)
- Use of legitimate superannuation funds to support gambling. (Australia)

The ACC has identified, and has expressed serious concern about, the use of so-called super-agents operating under contract of a particular PoDRS.

- Under current arrangements, the PoDRS is reporting to AUSTRAC, remittances processed by around a dozen super-agents acting as a franchise for more than 300 sub-agents. Although the sub-agents report to the PoDRS, the main issues concern the application of principles of 'know your customer' (KYC).

3. Money Laundering & Terrorism Financing Trends

3.1 Research or studies undertaken on ML/TF methods and trends

Australia

Applying a risk-based approach to anti-money laundering investigations has resulted in additional outcomes, including improvements in data-quality control and compliance.

Trend analysis of international movements of funds from Australia to Country A indicated a significant increase in the value of outgoing IFTIs reported by money remitters. AUSTRAC data confirmed that from 2004 to 2007, money remitters reported transferring a total AUD$260 million. In the same period, banks only reported transferring a total AUD$12.3 million.

Further analysis indicated that a small business in Western Australia that had previously come to the attention of the Australian Crime Commission (ACC), had reported transferring a total of AUD$257 million, of which AUD$248 million had been transferred during 2007.

Due to the business having previously come to the attention of the ACC, the value of funds recorded as having been remitted warranted further investigation.

Enquiries conducted by AUSTRAC established that the business had reported remittances in a foreign currency and that the Centre had inadvertently applied a black-market foreign exchange rate when calculating the Australian dollar value.

The ACC also identified significant compliance issues, but concluded there was no evidence of the business being exploited for the purpose of removing significant proceeds of crime from Australia to Country A.

The case highlights the importance of data quality control and ensuring compliance with reporting requirements. Further cases investigated by the ACC have also highlighted issues concerning the quality of data with respect to self-reporting PoDRS.

3.2 Association of types of ML or TF with particular predicate activities

Open Source example

U.S. Department of Justice; Afghan Drug Kingpin Charged With Financing Taliban Terrorist Insurgency
14 November 2008 Drug Week

Haji Juma Khan, an Afghan drug trafficker charged with conspiracy to distribute narcotics with intent to support a terrorist organization is among the first defendants to be prosecuted under the 2006 federal narco-terrorism statute.

According to the indictment since at least 1999 Khan led an international opium, morphine and heroin trafficking organization (the "Khan Organization") based principally in the Helmand and Kandahar provinces of southern Afghanistan. The Khan Organization arranged to sell morphine base in quantities as large as 40 tons - enough to supply the entire U.S. heroin market for more than two years. In addition, the indictment alleges that the Khan Organization also operated labs in Afghanistan that produced refined heroin and sold the drug in quantities of as much as 100 kilograms and more.

Khan has been closely aligned with the Taliban, which was designated by the President of the United States as a "specially designated global terrorist group" in 2002.

Khan has supported the Taliban's efforts to forcibly remove the United States and its allies from Afghanistan by providing financial support in the form of drug proceeds.

3.3 Emerging trends; declining trends; continuing trends

3.3.1 Technological advances

None reported.

3.3.2 Organised crime – overseas remittances

Australia
ACC investigations identified a PoDRS using separate ledgers hidden in a secret compartment to record funds received for the purpose of making available to persons residing abroad.

Investigations revealed that over a four day period, the proprietors received more than AUD2 million in cash. The funds were subsequently dispersed between several sub-agents for transfer abroad.

No cash dealer reports were lodged with AUSTRAC. The proprietors were subsequently charged with being knowingly involved in a conspiracy to launder proceeds from crime.

4. Effects of AML/CFT Counter-Measures

4.1 The impact of legislative or regulatory developments on detecting and/or preventing particular methods (e.g. tracing proceeds of crime, asset forfeiture etc)

Cook Islands

The Cook Islands FIU, Police and Crown Law Office in 2007 withheld the execution of a Court Order to restrain and freeze a customer account maintained by one of its Offshore Banks and to produce documents after having identified the account to have been in debit of US$1.6 million from US$700,000 credit balance. The request from Country “A” was subsequent to a report received by the FIU from the Financial Supervisory Commission of the Cook Islands of an account being held in the name of a person who was reported on World-Check being wanted by the Authorities in country “A”. The outsourcing of the Margin Trading and Trade Finance activities of the bank in the Cook Islands to a company in country “B” proved it difficult to ascertain if there has been an actual trading undertaken by the customer to incur a debit of US$1.6 million. The matter is still being investigated.

Charges laid in August 2008 against an Offshore Bank, its Chief Executive Officer and Compliance Officer for offences under the Financial Transactions Reporting Act 2004 (FTRA) for failing to identify and verify customers were withdrawn recently without prejudice after encountering problems with the definition of a “Reporting Institution” under section 2, section 4 (1) of the FTRA in relation to customer identification and verification and section 4 (7) in relation to Intermediaries or third parties introducing business to the bank. The matter is being further investigated. The legislative deficiencies in the FTRA are also being reviewed to form part of the amendments to the current FTRA.

Philippines

On 3 August 2006, the UN 1267 Sanctions Committee approved the addition of Abd Al-Hamid Sulaiman Al-Mujil and the Philippines branch of the International Islamic Relief Organization (IIRO) to its list of individuals/entities associated with Usama bin Laden, the Taliban and/or Al-Qaida who are subject to UN Security Council-mandated sanctions, including asset freezing, travel ban and arms embargo.

The Philippine branch of the Saudi-based International Islamic Relief Organization (IIRO-Phil) facilitates fundraising for Al-Qaida and affiliated terrorist groups.

Abd Al-Hamid Al-Mujil, the Executive Director of IIRO, used his position to bankroll the Al-Qaida network in Southeast Asia. Al-Mujil provided donor funds directly to Al-Qaida and is identified as a major fundraiser for the Abu Sayyaf Group (ASG) (included in the 1267 Sanctions list on 6 October 2001) and Jemaah Islamiyah (JI).

IIRO-PHIL has served as a liaison for the ASG with other Islamic extremist groups. A former ASG member in the Philippines familiar with IIRO operations in the country reported that a limited amount of foreign IIRO funding goes to legitimate projects and the rest is directed to terrorist operations.

Actions taken by the Anti-Money Laundering Council over several years has resulted in banks complying with requirements to report suspected funds, those funds being frozen and ultimately, courts issuing orders for the funds to be forfeited to the government.

Philippines

In late 2005, government forces captured 8 suspected members of a terrorist group known as the Rajah Sulaiman Movement (RSM) led by Abu “A”. It is believed the terrorist group had been involved in a number of bombings in the Philippines.

A bank based in the southern Philippines submitted two STRs concerning Mr. MA, one of the detainees, and Ms. ND, one of the wives of Abu “A”.

Inquires by law enforcement officers including interviews conducted by AMLCS staff identified some account holders who used their accounts to receive and withdraw funds for the organization.

On June 4, 2008, UNSC 1267 Committee approved the inclusion of the terrorist group and 8 of its members in the list of individuals/entities associated with Usama Bin Laden, the Taliban and the Al Qaida.

On July 9, 2008, the court issued a Freeze Order over properties and bank accounts which has been extended in anticipation of a civil forfeiture order being applied for.

4.2 Cases developed directly from suspicious or unusual transaction reports

Australia

An investigation into an individual involved in the laundering of money was initiated by information held by AUSTRAC. STRs were reported to AUSTRAC detailing multiple purchases of international bank drafts using cash structured below the reporting threshold.

The suspect would purchase multiple drafts from the same location on the same day before then moving on to other bank branches to repeat the process. Over 100 bank drafts were purchased totalling in excess of AUD$1million. The drafts were made out to family members.

The suspect pleaded guilty to 33 counts of FTR offences and was convicted and sentenced to imprisonment for an aggregate of six months.

Australia

Several STRs reported to AUSTRAC were referred to a state law enforcement agency assisting in subsequent investigations and seizure of over 11 kilograms of cannabis. The STRs provided details of numerous cash deposits and withdrawals. This, along with other information contained on the STRs did not appear consistent with the customer profile. The investigating agency made enquiries with other agencies that assisted in gathering evidence that the people had no apparent lawful means of sourcing this amount of cash.

It was further noted on a number of the STRs that the cash smelt strongly of marijuana. This led investigators to suspect that the persons may have been involved in large-scale cannabis dealing within Australia and possibly overseas.

A search warrant was obtained and executed on the suspects' premises at which time the cannabis, a large amount of cash and two vehicles were seized. Two persons were arrested and charged with various drug offences.

Australia

A revenue agency initiated an operation after receiving an STR referred to them by AUSTRAC. Suspicions were raised as the subject of the STR, a small businessman, was found to be in receipt of a large amount of government funds. AUSTRAC information was used to identify transactions conducted by the businessman, highlighting the fact that he was sending funds offshore to Africa. A further four STRs were received by AUSTRAC, showing that the person was structuring his withdrawals in an attempt to avoid detection by AUSTRAC. These reports also indicated the person's intention to leave the country permanently for an overseas destination.

Under Section 16(4) of the FTR Act, the revenue agency served a notice on the cash dealer involved to gather more information regarding the person. As a result of further enquiries, it was found that the person had defrauded the Commonwealth of over AUD$100,000. The revenue agency sought the assistance of an Australian law enforcement agency to arrest the person two days before he was due to leave Australia.

The person was charged with two counts of obtaining a financial benefit by deception under section 134.2(1) of the Criminal Code 1995. Subsequently, he was found guilty and was sentenced to one year's imprisonment on the first offence and two-and-a-half years imprisonment on the second offence, with a minimum term of 10 months to be served.

Without the cash dealer's report, their suspicions and consequently AUSTRAC's referral of the SUSTR, which highlighted the occurrence of an offence, the person would have remained undetected and would have left Australia.

Australia

An STR lodged by a bank to AUSTRAC triggered an investigation into the supply of heroin. The STR detailed the daily occurrence of cash withdrawals of AUD$4,500 by a POI. This activity occurred over a three week period totalling AUD$60,000. Through these reports law

enforcement were able to connect a known drug dealer to the POI. The investigation led to identification of the source of heroin and an operation that resulted in the arrest of the POI and associates

5. International Cooperation & Information Sharing

Philippines

IP is said to be a leader of a money laundering organization based in the Philippines who has laundered money in the past for some notorious criminal organizations. In 2006, two (2) confidential informants/undercover agents represented themselves to IP as narcotics traffickers looking to launder significant amounts of narcotics proceeds. An agreement was reached wherein IP would launder on their behalf US $200K for a fee. The money (which was actually an undercover operation fund) was eventually laundered through IP's bank accounts in the Philippines.

In the course of investigation, IP also bragged and admitted to the undercover operatives of the requesting State of having laundered money for a Philippine terrorist group. The requesting State then sought the assistance of, and submitted to, the AMLC evidence showing that the accounts of IP were actually used as channels for laundering terrorist funds to support its request for the AMLC to provide them bank records of IP to prove its money laundering case it initiated against IP.

The request was given due course by the AMLC on this basis and an Inquiry without Court Order was authorized. Upon conclusion of the inquiry, the documents gathered and analysed as a result thereof were forwarded/shared to the requesting State.

Confronted with the documents, IP was arrested and pleaded guilty to several counts of money laundering.