Asia/Pacific Group
on Money Laundering

APG ANNUAL MEETING 2005 **[APG Yearly Typologies Report 2004-05]**

APG Typologies Working Group

APG YEARLY TYPOLOGIES REPORT 2004-05

JUNE 2005

Endorsed by the APG Plenary 14 July 2005

CONTENTS

INTRODUCTION

BACKGROUND

Since 2002, the Asia/Pacific Group on Money Laundering (APG) has produced reports on money laundering and terrorist financing trends and techniques in the Asia-Pacific region.

In September 2003, APG members endorsed a new *typologies framework*, which called for the production of annual typologies reports on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT).

The APG Typologies Working Group undertook to prepare this Annual Typologies Report 2004-05 with the assistance of the APG Secretariat.

APG's mandate for undertaking typologies work

The APG's typologies work describes and/or analyses the nature of money laundering and the financing of terrorism, as well as methods and trends. Since its establishment in 1997, the APG has used this typologies work to develop a better understanding of the money laundering environment in the Asia-Pacific region.

The demand to better understand the nature of money laundering and terrorist financing remains strong. The APG consistently receives requests for contextually relevant case studies and analysis in relation to these issues, from members and observers, multilateral donor organisations, AML/CFT standard setting bodies and implementing agencies.

The APG is the regional focal point for AML/CFT matters. It is the best-placed body in this region to collect, analyse, and share information and case studies. The typologies information contained herein has many uses for the APG. For example, to support policy setting, implementation of international standards (particularly in the law enforcement sector), assessment work and the APG's input into the AML/CFT standard setting processes.

An important factor driving the continuing high demand for timely typologies information is the effect of the global pressure to implement the Financial Action Task Force (FATF) *40 Recommendations* and *Nine Special Recommendations*. An understanding of AML/CFT threats and vulnerabilities assists jurisdictions with the effective implementation of the revised global standards. Knowledge of the environment is a vital component in designing and implementing a risk-based AML/CFT system.

The Typologies Working Group

The APG Typologies Working Group leads the typologies work and has been established to conduct a series of in-depth studies on particular typology topics, support a network of APG typology experts and provide practical advice on the APG typologies collection and analysis framework. APG

Typologies Working Group Meetings are open to all APG members and observers. The Typologies Working Group currently consists of:

- New Zealand (Co-chair)
- Indonesia (Co-chair)
- Australia
- Canada
- Chinese Taipei
- Cook Islands
- Fiji
- Germany
- Hong Kong, China
- India
- Japan
- Korea
- Malaysia
- Pakistan
- Palau
- Philippines
- Thailand
- United States
- Egmont Group
- FATF
- IMF

APG Typologies Workshop 2004

Building on previous successful APG Typologies Workshops, Brunei hosted the most recent Workshop in Bandar Seri Begawan over 5 and 6 October 2004. It was attended by 155 participants, representing 30 member jurisdictions and nine international and regional organisations.

The 2004 Typologies Workshop was jointly chaired by Mr Haji Muhammad Syaippudin Haji Abdullah, Director of Financial Institutions, Ministry of Finance, Brunei Darussalam and Mr Rick McDonell, Head of the APG Secretariat.

Presentations were given on a range of topics and breakout groups discussed specific issues in greater depth. Major topics included:

Terrorist financing methods

Certain aspects of terrorist financing methods were the subject of examination. For example, terrorist financing trends in Southeast Asia, wire transfers, abuse of charitable institutions and recent case studies showing methods and trends.

Cash couriers

Methods and trends in relation to cash couriers were discussed, including dialogue around *red flag* indicators for detecting cash couriers, as well as cash economy and trade-based money laundering issues.

Illegal logging

Methods and trends involved in laundering the proceeds of illegal logging/forestry activities in the Asia-Pacific region were examined. Further information on illegal logging money laundering issues is available via the APG website.

Corruption issues

Further consideration was given to corruption-related money laundering issues in the Asia-Pacific region. Opportunities for co-operation between

Financial Intelligence Units (FIUs) and specialist anti-corruption bodies in investigating the proceeds of corruption were the main focus.

Alternative remittance systems
Uses of alternative remittance systems for money laundering and terrorist financing were considered from the perspective of implementing FATF *Special Recommendation VI*.

External typologies opportunities

The FATF continues to involve all APG members in its global typologies work in order to include the AML/CFT experience of the Asia-Pacific region. There is continuing co-operation and co-ordination between the FATF and APG in planning and conducting typologies work.

In December 2004, the APG participated in and contributed to the joint FATF/Moneyval (the European FATF style regional body) 2004 Typologies Meeting in Russia. APG participation included the six APG/FATF members, along with South Korea, Chinese Taipei and the APG Secretariat.

The 2004 FATF Typologies Meeting progressed a number of money laundering and terrorist financing typologies, including abuse of the insurance sector, human trafficking related money laundering issues, alternative remittance systems, drug trafficking and terrorist financing. The FATF Yearly Typologies Report 2004-2005 which summarises work on these topics and includes APG input is available for download at www.fatf-gafi.org .

Further APG typologies work 2004 - 05

The APG Typologies Working Group is scheduled to meet during the 2005 APG Annual Meeting to consider current tasks, future typologies projects, topics for the 2005 Typologies Workshop and ongoing co-operation with the FATF, the Egmont Group and other AML/CFT bodies.

The APG will hold the 2005 APG Typologies Workshop in late October in Fiji. Further details of 2005 Typologies Workshop will be posted on the APG website when available.

SECTION I

SUMMARY OF REGIONAL METHODS AND TRENDS

In 2003, the APG Secretariat introduced a pro-forma outline for APG jurisdictions to provide typologies information to the APG Typologies Working Group. While the new pro-forma outline was well received by jurisdictions, the resulting reports varied in quantity and quality.

In preparation for the 2004 Typologies Workshop in Brunei Darrussalam, the APG Typologies Working Group and the APG Secretariat again requested each jurisdiction for typology information using the pro-forma outline.

As a result of the issues previously experienced, member and observer jurisdictions were asked to make a concerted effort to ensure that they furnished a report and followed the format provided when submitting their reports. Despite this request, the number of reports submitted declined slightly, however, the number of jurisdictions that followed the prescribed format marginally increased. These results are illustrated in the table below:

Table 1: Number of typology reports submitted and number of reports that followed format

	Number of Reports				**Followed Format**			
	Members		**Observers**		**Members**		**Observers**	
2003	19/26	73%	5/13	38%	8/19	42%	1/5	20%
2004	20/28	71%	2/11	18%	9/20	45%	0/2	0%

The quality of the reports varied considerably. Some APG jurisdictions provided very comprehensive reports, while others still did not follow the pro forma or definitions provided. Some used their own terminology or did not clearly distinguish between *predicate offences* and *methods*. It should be noted, however, that in many jurisdictions the necessary AML/CFT regimes are not yet in place and/or they lack the necessary training and expertise in AML/CFT matters. As a result, they are not in a position to report as requested.

From analysing the categories of legislation/regulation, institutional framework/capacities and implementation/enforcement, around a quarter of the member jurisdictions could be considered as lacking capacity to enable them to submit the required information. Amongst observer jurisdictions, this figure climbs up to almost two-thirds.

Common methods

Even though the overall quantity and quality of the submitted reports could have been improved to provide an enhanced analysis, the following examples of the most common methods have been drawn from the material provided.

Terrorist financing (the abuse of wire transfers) and the use of cash couriers in money laundering/terrorist financing are not covered here. These issues are discussed separately in Section III and Section IV, respectively.

Association with Corruption (proceeds of corruption & bribery of officials)

Since 11 out of the 22 reporting jurisdictions addressed this, it is of special importance to the region.

Most cases reported dealt with corruption of or by government officials as one of the various predicate crimes. In the following example, however, a bank official was also being corrupted to facilitate money laundering.

Hong Kong China
A Land Inspector of the Lands Department accepted advantages amounting to approximate HKD$500,000.00 (US$64,000.00) from a village house developer as a reward for creating and/or providing Lands Department records or documents required for redevelopment of certain village houses. The two of them also conspired together to defraud a finance company by dishonestly submitting to the finance company false Lands Department documents in relation to some village houses in support of applications for mortgage finance. An employee of the finance company was paid HKD$10 million (US$1.28 million) in bribes for assistance in granting the loans.

Structuring

This method, which involves large numbers of small deposits to avoid threshold reporting, is quite common in the region.

Australia
In December 2003 two people were arrested and charged with structuring transactions contrary to the FTR Act. Investigations revealed that in December 2003, both defendants structured 19 separate cash withdrawals, each under AU$10,000.00 (US$7,500.00) from their bank account. Within eight days both defendants structured a further 125 cash deposits each under AU$10,000.00 (US$7,500.00), into a joint account at a different bank. AUSTRAC disseminated the intelligence to a law enforcement agency for further investigation. The intelligence showed clear structuring that led to both people being charged with offences under the FTR Act. Approximately AU$1.17 million (US$880,000.00) was restrained pursuant to the Proceeds of Crime Act 2002. In April 2004, both defendants pleaded guilty to the structuring offences, were ordered to forfeit approximately $1.17 million (US$880,000.00) and were released on an AU$5,000.00 (US$3,750.00) good behaviour bond for three years.

Chinese Taipei
KNIGHT was a famous international sports goods purchasing agent for a company operating in the Asia region. The head office was located in Taiwan. KNIGHT illegally asked for kickbacks (cash) from the factories in the Asia region that provided materials to the company and then carried the cash back to Taiwan. To conceal the illegal benefit, which amounted to over US$400,000.00, he firstly stored the cash in a bank's safe deposit box and then intentionally removed the cash in small amounts and deposited it into his personal bank

account to avoid cash transaction reporting thresholds. He also transferred part of the funds to his close friends and relatives who lived in China and Egypt, as well as to his personal United States bank account. Some of the cash was concealed in parcels and delivered to the United States by express delivery channels. KNIGHT requested that the bank did not deliver the banking check sheets to his company and intentionally avoided triggering transaction reporting thresholds by structuring the cash deposits. His activities eventually came to the attention of the bank and in March 2004, a suspicious transaction report was submitted to the FIU in Taiwan. The report was then forwarded to a law enforcement agency for further investigation. The activities of KNIGHT violated the breach of trust, which is not included in the scope of predicated crimes of money laundering in Taiwan, although, this case is still under investigation in the company's home country.

Many jurisdictions, have no cash reporting regulations and as such, there are no thresholds to avoid. Furthermore, one jurisdiction reported that even though structuring is not necessarily a criminal offence, it is considered reason enough to submit a suspicious transaction report to the FIU. Another jurisdiction, also without cash transaction reporting thresholds, noted that it had experienced occurrences of structuring to avoid identity verification requirements.

Use of credit cards, cheques, promissory notes etc.

The questionnaire asked jurisdictions to report cases where these instruments were used by money launderers and/or financiers of terrorism to access funds held in a financial institution in another jurisdiction. The majority of reported cases made no reference to the cross-border criteria and had only a domestic background.

The use of credit cards in money laundering was reported as being the source of illicit funds, rather than a vehicle to launder those funds. In contrast, the use of pre-paid, personal identification number protected cards was seen as an emerging method to launder funds.

New Zealand

TRAVELEX in New Zealand issue a pre-paid, personal identification number protected card called a *Cash Passport*. With this product, the purchaser can load any amount onto the card between NZ$250.00 (US$190.00) and NZ$25,000.00 (US$19,000.00). These funds can be accessed through any Automatic Teller Machine (ATM) around the world that displays the *Visa* sign (according to TRAVELEX advertising, approximately 800,000 machines may be used worldwide). When the card is issued, a duplicate card is also issued. The *Cash Passport* can be reloaded with any amount, up to the maximum amount, as many times as the holder wishes, within the three year period that it is valid for. During a recent drug operation, a methamphetamine manufacturer's safety deposit box was searched. The box contained jewellery, some bullion, NZ$300,000.00 (US$230,750.00) in cash and a TRAVELEX *Cash Passport*. The card was in credit to the value of NZ$10,000.00 (US$7,700.00). The investigators had never dealt with this type of product before and did not know that the drug manufacturer still had access to the NZ$10,000.00 (US$7,700.00) from the duplicate card. As a result, the drug manufacturer withdrew all the stored credit on the *Cash Passport* without the investigators knowing until it was too late.

The APG Typologies Working Group has held discussions with TRAVELEX regarding the potential for misuse of this product. TRAVELEX have implemented several measures and are in the process of implementing others

to lower the risk of this product being used for money laundering and/or terrorist financing.

Where cheques and promissory notes were reported as being used, they were predominately used as instruments in the commission of predicate fraud offences. One jurisdiction did report that a number of drug investigations, conducted over the last 12 months, had indicated that cheque accounts had been used to launder funds. This method primarily involved cash deposits being placed into accounts and cheques being drawn to be used to purchase goods and services.

Purchase of portable valuable commodities or valuable assets

Jurisdictions were asked to report cases where *portable valuable commodities*, such as gems and precious metals etc., had been used to conceal or move monetary value without detection and, consequently, avoid financial system anti-money laundering measures. The physical movement of precious gems, for example, to transfer valuable commodities to another jurisdiction, has the advantage of avoiding financial sector reporting requirements and also obscures the source of the original funds.

Similarly, in the case of *valuable assets*, where criminal proceeds are invested in high-value, negotiable goods, such as real estate, race horses and motor vehicles etc., reporting requirements are reduced and the original source of funds disguised. Approximately a quarter of the reports addressed this issue and the region continues to see these methods being used.

Chinese Taipei

LIU was a senior legal clerk in a legal firm and in charge of dealing with buying/selling transactions of stocks entrusted by clients. In 2003, a foreign company entrusted the firm to sell its investing stocks in Taiwan, which were valued at over NT$3 billion (US$96 million). The firm assigned LIU to handle the selling transactions of stocks on behalf of the foreign company. LIU had the authority, therefore, to open accounts, sell stocks and remit the income in the name of the foreign company. LIU continually sold-out the stocks and embezzled the income. He used the following six methods to launder the embezzled funds: (1) withdrawing cash several times, which amounted to NT$482.9 million (US$15.5 million); (2) exchanging foreign currency, which amounted to NT$2.8 billion (US$90.3 million), then remitting to a shell company account opened by LIU in a neighbouring jurisdiction; (3) purchasing bank cheques, which amounted to NT$368 million (US$ 11.8 million), then cashing them at two separate banks, both with personal accounts held under his name; (4) transferring NT$366.74 million (US$11.8 million) to his personal account, then withdrawing the cash to purchase diamonds, jewels and vouchers from department stores; (5) purchasing traveller's cheques, which amounted to NT$20 million (US$645,000.00) and (6) transferring a total of NT$20.5 million (US$661,000.00) to a diamond company's account for purchasing diamonds and jewels.

New Zealand

An investigation into a drug courier in New Zealand, who was importing methamphetamine from Malaysia, ended in a search warrant executed at his address. The search located six kilograms of methamphetamine, NZ$100,000.00 (US$70,000.00) in cash and a cache of jewellery, including seven Rolex watches. It is believed that this courier had made approximately NZ$400,000.00 (US$307,600.00) from his drug-related activities and that a significant proportion of this money was used to purchase jewellery.

Australia
In an organised tax evasion scam, two brothel owners withheld cash takings, understated their income to the Australian Taxation Office and siphoned funds to overseas bank accounts over a three-year period. The offenders obtained false identification documents and structured the transfers using false identities and names of associates. One of the offenders then changed his method of laundering the cash payments, possibly as a result of his growing awareness of the role and function of AUSTRAC. Methods included the physical carriage of cash out of Australia, the purchase of bullion, acquisition of prestigious motor vehicles and loans to associates.

Wire transfers
Refer to Section III of this report.

Underground banking services/alternative remittance systems
More than half of jurisdictions reported on this category, which again indicates that underground banking services/alternative remittance systems (UBS/ARS) are very common to this region. Many jurisdictions did stress that UBS/ARS, whether legal or illegal in the jurisdiction, are mostly used for totally legitimate purposes. In contrast, several reports also contained cases that demonstrated the illegal use of UBS/ARS. No significantly new methods, however, emerged from jurisdictions' reports.

Trade-based money laundering (false invoicing)
In this category, jurisdictions were asked to comment and give examples of trade-based money laundering, such as that seen in the *Black Market Peso Exchange.* For example, brokers in the criminal's home jurisdiction typically deposit clean money into the local account of a person generating criminal proceeds in another jurisdiction.

The brokers have associates based in the foreign jurisdiction who use *tainted* money to purchase goods to be imported back to the criminal's jurisdiction to be sold or exchanged for *clean* money. The goods are either shipped back under the guise of *legitimate* trade or smuggled to avoid any importation duties or taxes.

While some duty or tax avoidance may occur, the ultimate purpose of this trade-based money laundering is to legitimise *tainted* money rather than avoid importation taxation. Almost half of the jurisdictions reported cases of incorrect invoicing, although, they were mainly incidents of understating invoices to avoid importation taxes, duties, etc. These cases did not reflect a money laundering technique, but rather regular criminal offences.

Cases where this method was used to transfer illicit funds within or between jurisdictions were not reported at all, which may reflect a lack of awareness amongst many AML/CFT agencies and some FIUs in particular.

Gambling activities (use of casinos, horse racing, internet gambling)
Following on from the APG Typologies Report 2003-04, this year the use of casinos to launder money was again seen as the most prominent vehicle in this category. The most common methods reported were:

- Buying casino chips and cashing them in without gambling.
- Structuring the purchase of chips where cash reporting thresholds were mandatory.
- Putting money into slot machines and claiming the accumulated credits as a jackpot win.
- Playing games with low returns but high chances of winning, such as *Baccarat*.

Sports betting and the purchasing of winning jackpots were also seen as other vehicles to launder funds. The following cases illustrate these methods:

Indonesia
A bank chief cashier took money from the bank vault and manipulated the bank's record. He used the money to bet on soccer games. The gambling proceeds were then deposited into his bank account and were later transferred to a housing agent as payment for his new house in a prominent area. It was found that the bank lost approximately Rp.20 billion (US$2.2 million).

Australia
AUSTRAC referred a matter relating to a group of overseas nationals buying winning jackpots at various clubs in Sydney. The suspects deposited approximately AU$1.7 million (US$1.3 million) in winning cheques within a year, immediately withdrawing money in cash afterwards. The source of the funds used to buy winning jackpots was suspected to be from illegal means. This matter was referred to partner agencies for further investigation.

Abuse of Non-Profit Organisations (NPOs)

In the cases reported by jurisdictions under this category, some linkages to terrorist financing were seen. In one case an NPO assisted a terrorist linked organisation to arrange a speaking tour to raise funds. Another jurisdiction reported that an NPO was misused by a terrorist organisation, as it had used the NPO as a front contact.

Furthermore, in a more complex case, a network of NPOs located in different jurisdictions used a number of foreign charities, commercial entities and private individuals to raise and move terrorist funds. Different instruments, such as bank drafts, money service businesses and cash couriers were also used to disguise the origin and ultimate use of the money.

Use of shell companies/corporations

In 2003-04, the use of shell companies and/or corporations to launder illicit funds was uncommon within the Asia-Pacific region. For the 2004-05 year, jurisdictions have reported this method as more common. The instruments of shell companies and corporations were seen as providing a façade of legitimacy to further distance the illicit funds from the predicate offending and, consequently, aiding in the cleansing process.

Hong Kong China
Secretarial Company X was based in Hong Kong with agents in a few European jurisdictions. Company X set up shell companies for its clients and its employees acted as nominal directors for the shell companies. The employees also opened bank accounts with Bank Y in

Hong Kong for the clients and acted as authorised signatories to handle transactions for the clients upon instructions. The clients did not need to come to Hong Kong for operation of their companies or accounts. The clients could give instructions simply by telephone, facsimile etc. Bank Y had no idea of who the actual beneficiaries of the accounts were or what their businesses were, but apparently they were more than happy to continue opening bank accounts and keep the business relationship with Company X in this manner. An investigation later revealed that the bank accounts of the shell companies were involved in money laundering, valued-added-tax fraud, commercial crimes, etc. in Europe.

Indonesia
A senior manager of a state enterprise office had created a fictitious transaction between his enterprise and a shell spare-part supplier company that had already become non-operational. He had opened a new current account in a bank by using fake supplier company's documents to accept the payment of Rp.3.2 billion (US$355,000.00) without transfer of goods. This official gradually withdrew the money in cash for his personal gain. Part of the money was used to buy travellers cheques, which were then distributed as gifts to his colleagues in the enterprise. The case is still before the court.

Use of nominees, trusts, family members or third parties, etc.

Nominees, trusts, family members or third parties are often used as a way of concealing the identity of the person(s) actually controlling illicit funds. More than half of the reports addressed this category. This method appears to be quite common in the region. The cases reported show how nominees, trusts, family members or third parties can be misused for the opening of accounts or for the concealment of assets.

Republic of Korea
Company X was a house construction and selling business. Person A was the CEO/Executive Director of Company X. Person A built ten shell companies with investment solely from Company X and used those shell companies in the process of money laundering. Company X was constructing apartments all by itself, but was disguised as if it had contracted with suppliers, which were represented by the ten shell companies. Afterwards, Company X inflated construction expenses from 8% to 15% and received the rebate of the difference. Company X, therefore, received the rebate of KRW 27 billion (approximately US$23.5 million) on 4,293 occasions during a period of five years. The money was deposited into 150 third party accounts including the accounts in the name of family members of the employees of Company X. The illegal proceeds were provided as illegal political funds. Person A had also appropriated the money for his personal purpose.

Macao China
Person D, who was unemployed, opened an account with a bank. Person D assigned the authorisation to his wife, who was a housewife, to operate his account. There were transactions of small amounts for the first year of operation. Later on, however, over HKD 14 million (US$ 1.8 million) was transferred into Person D's account from third party accounts in the same bank over two months. The funds were then withdrawn from the account by outward remittance, account transfer, cash withdrawal or purchases of promissory notes. As the account owner's economic status was obviously not commensurate with the transaction amounts, the bank filed a suspicious transaction report with the Judiciary Police.

Canada
Two employees of a software manufacturer in Country A used their positions to steal approximately CA$3 million (US$ 2.4 million) from this company. The company's financial officers both had signing authority on the company bank accounts. They fraudulently wrote cheques to fictitious businesses, in the names of friends or relatives, for services that were

never rendered. The principal suspect wired approximately CA$800,000.00 (US$645,000.00) from accounts in Country A to accounts of nominees in Country B.

The successful detection of these methods depends largely on the quality of *Know Your Customer* and *Know Their Business* procedures. If the question of identity and beneficial ownership are correctly addressed and the behaviour of the customer is monitored and checked against this profile, the misuse of nominees, trusts, family members or third parties can be detected and reduced.

Use of foreign bank accounts

The use of foreign banks in order to obscure the identity of the person(s) controlling illicit funds and/or moving funds out of the reach of domestic authorities was very common. Almost half of the jurisdictions reported on this method. It was noted that in one jurisdiction it is forbidden to have a foreign bank account.

Use of false identification

The use of false identification to obscure identity proves to be a key facilitative activity in the reported cases of money laundering and terrorist financing. The extent of this problem seems to vary significantly amongst jurisdictions.

Countries with strict identification procedures are more likely to detect cases involving false identification. In contrast, countries without strict identification procedures are more likely to be misused and due to a lack of necessary capacity, and capability, have a harder time detecting the misuse.

Use of professional services/gatekeepers

Previous typologies work has identified that professional service providers, such as lawyers, accountants, brokers etc., are excellent vehicles for laundering money. This is because they can not only act as a conduit to facilitate the *placement* stage, but they can also assist in providing the tools to set up more sophisticated money laundering schemes or asset protection structures. For example, trusts, offshore accounts and entities.

For the 2004-05 year, only a few jurisdictions reported this method being used. The reports did, however, highlight a higher level of sophistication in the money laundering schemes.

Australia
An accountant and her de facto husband were offering money laundering and tax evasion services to their clients. The services offered involved the remittance of undeclared cash furnished by the respective clients to entities in offshore tax havens. The subjects had developed a well-planned and meticulously executed money laundering and tax evasion scheme through the formulation of a corporate infrastructure to aid their illegal activities.

Australia
An Australian-based solicitor structured funds to an offshore account in Hong Kong. At times it is believed that he actually carried cash to Hong Kong. His colleague, a Hong Kong-based solicitor, arranged for the creation of offshore companies in the British Virgin Islands and bank accounts in Hong Kong to receive structured funds from Australia. These funds were then

transferred to other countries by the Hong Kong-based solicitor to hide from authorities or returned to Australia in order to appear legitimate.

Indonesia
A state company transferred money estimated at Rp.3.5 billion (US$389,000.00) to an infamous public accountant for a management consultant fee. Two days later, most of the money (Rp.2.85 billion (US$317,000.00)) was cashed and transferred to a government officer's personal savings accounts in other banks. A part of the money was then transferred to an automobile agent as payment for three luxury cars. The government officer is a high-ranking person in a state company. This matter is still being investigated.

Use of internet (encryption, payment systems, online banking, etc.)

Only a few cases were reported where modern instruments of communication, such as the internet and mobile telephone short message systems (SMS) were misused to obscure and remit criminal proceeds. In one case, money generated from internet banking theft was laundered by transferring the funds to a regular bank account and allowing third parties to withdraw the money via the internet by providing those third parties with the account number and access code.

Often the internet or SMS has been used as a facilitating instrument in sophisticated fraud cases by hiding the identity and location of the persons committing these crimes.

New Zealand
Phishing scammers send potential victims an email purporting to be from the victim's bank. The email advises that their bank is updating its online security. The email has a hyperlink to a fake bank website where the victim enters in their online banking identification and password. Once this is obtained, the *phishing* scammers then transfer money from the victim's account to a *mules* account, which is usually in the same country. The *mules* will then transfer this money overseas to places like Estonia, Latvia, Russia etc. In New Zealand's experience, the *mules* were recruited by an email convincing them that they were forwarding money from the sale of plasma televisions. For completing this service the *mules* receive 5% commission.

Internet and SMS scams, similar to online auctions, advance fee fraud, false billing for web services etc., seem to be quite common, especially in jurisdictions where SMS are free or cost less than telephone calls.

Uncommon methods

The following methods were either not commonly found or not reported as being used at all. These methods still warrant mention and consideration, however, within this section.

Currency exchanges/cash conversion

Only two jurisdictions reported that this method was being used. This was somewhat surprising considering the high-level of cash used in jurisdictions throughout the region. One jurisdiction reported a method that involved the importation of false US currency banknotes, which were then exchanged for

local money. The local money was then exchanged back into *clean* US currency banknotes, which were then taken out of the jurisdiction again.

Another jurisdiction reported cases where persons violated the existing exchange control restrictions by sending funds abroad, under third party names, and using more than one foreign exchange dealer in order to minimise the risk of detection.

Commodity exchanges (barter/reinvestment into illicit drugs)
This method was not generally found during the period covered by this report.

Investment in capital markets
The rationale behind this category was to report cases where relatively low reporting requirements had been exploited to obscure the source of the proceeds of crime by purchasing negotiable commodities. The reported cases were more or less related to fraudulent activities. One jurisdiction, however, reported the following case:

Hong Kong China
In an ongoing case of laundering the proceeds of organised crime by the use of illegal bookmaking, funds were traced to a licensed brokerage. The profits from the illegal bookmaking were transferred from the bank account of the syndicate head's wife and sister-in-law to the share margin account of the syndicate head. Little or no trading occurred on the margin account and the funds were then withdrawn as cheques payable for cash and subsequently deposited into the personal bank account of the syndicate head.

This case highlights the complete lack of knowledge of money laundering techniques by the brokerage firm concerned.

Co-mingling (business investments)
This method was not generally reported during the period covered by this report.

Use of offshore banks/corporations
Only one case was submitted in relation to this method. Please refer to the use of professional services/gatekeepers, previously mentioned within this section.

This method was not generally reported during the period covered by this report.

Criminal knowledge of and response to law enforcement/regulations
No specific cases where organised crime has reacted in a specific way to existing AML/CFT measures have been reported. Some jurisdictions have outlined more generally that it would be natural for criminals to study AML/CFT issues and to look for loopholes. Examples of this were noted as being:

- Structuring of transactions to avoid reporting.
- Use of third parties or *clean people* for opening accounts.

- Use of UBS/ARS in order to avoid detection by x-ray machines at airports when carrying cash.

Other methods and emerging methods
Some jurisdictional reports noted other methods that were not specifically listed on the pro-forma collection outline. One of these methods was the use of safety deposit boxes, as the contents are not recorded and, as a result, there is potential for misuse by criminals to deposit illicit funds or valuable assets purchased with the proceeds of crime. Other methods mentioned related to fraud offences rather than money laundering methods.

Trends
Jurisdictions were asked to report on general or continuing trends or patterns seen in money laundering and terrorist financing methods. In order to assist with this reporting, jurisdictions were asked to provide information on research or studies completed, associations between methods used and predicate offending, emerging, continuing and declining trends occurring in their respective jurisdictions.

Unfortunately, some reports erroneously described trends in the underlying predicate offences and not in the methods used, or described emerging, continuing and declining trends that had not been included in the methods section of the report.

Research or studies undertaken on money laundering methods/trends
Over the last year, very few jurisdictions appear to have carried out any specific research or studies on money laundering methods and trends. For that reason, the jurisdictional assessments on trends that emerged, continued or declined were not generally based on specific research undertaken, but were more or less a general impression of trends.

This indicates that resources to carry out such research and studies are limited in many jurisdictions, even in those jurisdictions with more developed AML/CFT systems. There is an opportunity for technical assistance and training to be provided to developing jurisdictions to assist them to conduct comprehensive assessments of money laundering and terrorist financing risks and vulnerabilities including typologies.

Association of types of money laundering/terrorist financing with particular predicate activities
As there have been limited research studies undertaken on methods and trends, it is no surprise that the issue of a correlation between certain types of money laundering/terrorist financing methods and particular predicate offences has not been addressed in-depth. This was also the case last year. From the few reports received on this issue in both 2003-04 and 2004-05, the following comments have been made:

- Funds from cases of fraud and breach of trust by employees have often been laundered through family members and third parties.

- Structuring was observed in connection with illicit drugs, fraud and the sex and slavery trade.
- Foreign accounts have been used in cases of tax evasion and fraud.
- Identity fraud has mainly been used in the misuse of card and payment systems.

It should be noted that these comments were not commonly shared by all jurisdictions across the region and are general observations. Even though analysis of possible correlations between money laundering/terrorist financing methods and particular predicate activities has not been addressed widely by jurisdictions, association types may still exist.

This highlights that this issue has not yet been thoroughly examined. The APG Typologies Working Group considers that this matter should remain on the agenda and become a stream of its work when resources permit.

Emerging trends

When looking for emerging, continuing or decreasing trends, it is prudent to keep in mind that jurisdictions' within the region are at different stages of AML/CFT regime development.

Some countries that have had AML/CFT regimes in place for a long time, therefore, may consider certain methods as continuing because they have dealt with them for sometime now. In contrast, jurisdictions still in the process of setting up AML/CFT regimes may consider the same methods as emerging, even though it may have already been present, albeit undetected, until certain cornerstones of the regime were established.

For these reasons, the emerging trends reported reflect some common threads seen by two or more jurisdictions and not a reflection of the overall situation in the Asia-Pacific region. The emerging trends reported were:

- Opening of accounts with false identification.
- Selling *clean* accounts to third parties.
- Use of modern communication techniques.
- Use of foreign accounts.
- Cross-border remitting of funds.
- Pre-paid card/facilities.

Continuing trends

As far as continuing trends are concerned, the traditional methods of concealment were seen, including:

- Structuring.
- Use of false identification.
- Use of third parties to open up accounts.
- Engagement of cash couriers.
- Underground banking services/alternative remittance systems.

Counter-measures

Jurisdictions were asked to report on the impact of various counter-measures imposed. The results are outlined below:

The impact of legislative or regulatory developments on detecting and/or preventing particular methods and trends

Only a few jurisdictions reported a direct impact of a single legislative or regulatory measure. In most cases, more general measures to establish and/or improve already existing AML/CFT regimes were reported. Many jurisdictions are still in the process of drafting/passing legislation. Others face the challenges of establishing the necessary institutional framework. For example establishing an FIU or responding to challenges associated with implementing and enforcing the already existing legislation and regulations.

More experienced jurisdictions, however, were mainly fine-tuning their AML/CFT provisions. This is most likely to be a consequence of detected deficiencies, as well as obligations in relation to the revised FATF *40 Recommendations* and *Nine Special Recommendations*. The reported fine-tuning included measures such as:

- Redefining or extending predicate offences for money laundering and/or terrorist financing.
- Extending the reporting requirements to designated non financial businesses and professions (DNFBPs).
- Introducing the option to give awards to informants and competent officers in order to get more information and co-operation from the public.
- Improving asset forfeiture powers and procedures.
- Introducing or revising AML/CFT guidelines for financial institutions and DNFBPs.
- Adjusting identification requirements.
- Requiring certain documentation and records to be kept.
- Adjusting thresholds for reporting to competent authorities.
- Introducing or lowering thresholds for transactions via Automated Teller Machines.

Besides fine-tuning legislation and regulations, other counter-measures taken included:

- Increasing resources and training.
- Improving mechanisms for domestic or international co-operation.
- Setting up of special expert witness programs to co-ordinate requests for expert opinions.

- Establishing or increasing outreach and awareness raising activities.

One jurisdiction reports a new initiative to curb new money laundering techniques in respective of cross border movements of currency. In this case, the highest denomination of the currency of a neighbouring country was forbidden in order to reduce cross-border cash smuggling.

Statistics
Jurisdictions were asked to provide statistical data on the numbers of suspicious transaction reports filed, money laundering investigations initiated and prosecutions and confiscations in relation to money laundering.

From the data that was received, it was found that in most jurisdictions, the number of suspicious transaction reports filed has increased, at times substantially compared with last year, with only one country reporting a declining trend. Usually the reports contained no particular reason for this increase. Some jurisdictions, however, indicated that the rise was due to:

- Additional outreach activities.
- Awareness activities.
- Maturing processes amongst reporting entities.
- Introduction of new AML/CFT software within financial institutions.

There are other reasons that may have produced the increase in the numbers of suspicious transaction reports filed, for example, the inclusion of new types of businesses or professions as reporting entities. Without the detailed information from jurisdictions, however, this remains speculation.

The percentage of submitted suspicious transaction reports that finally eventuated in money laundering investigations for each jurisdiction varied between 1% and 100%. The average across jurisdictions was around 15%. The figures given for resulting prosecutions included all cases pending, together with previous cases. The figures, however, vary from about 3% to 80%, with the average being approximately 25% of investigations leading to prosecutions.

When trying to assess whether suspicious transaction reports have resulted in an increase in the detection of money laundering, the statistics are somewhat skewed. Many jurisdictions reported that while suspicious transaction reports did not necessarily initiate investigations, they were a complementary source of intelligence for cases that had already been instigated.

In some instances, the filing of a suspicious transaction report eventuated in investigations and prosecutions of predicate offending and not money laundering. These factors were not accounted for in the above assessment and should be considered in future analysis.

The category of seizures/confiscations related to money laundering was only addressed by one jurisdiction. It reported that approximately US$20.2 million had been frozen from which approximately US$12.5 million had already been

returned to the victims of a criminal pyramid scheme and another US$718,000.00 had been repatriated to a foreign jurisdiction.

International co-operation and information sharing

Jurisdictional responses to international co-operation and information sharing ranged from building informal contacts to becoming members of international organisations, such as the APG, Egmont Group or Interpol, to setting up a network of bilateral agreements to enable international co-operation and information sharing.

Responses were generally a reflection of the different stages of AML/CFT regimes within the region. The main instrument for co-operation between jurisdictions was the signing of a Memorandum of Understanding (MoU). The number of MoUs signed seemed to have slightly increased compared with last year.

Providing technical assistance (TA) was reported as another very important form of co-operation between jurisdictions. In the respective cases, more developed jurisdictions and donor organisations were assisting other APG members/observers in setting up robust AML/CFT regimes. Most of the time this is done bilaterally, although in some cases a more regional TA approach was being undertaken, such as the IMF Pacific FIU project.

Other successful forms of international co-operation occurring within the region were noted as being the sharing of seized funds between jurisdictions and the stationing of a liaison officer in another jurisdiction.

The reports submitted indicated that the exchange of information had increased compared with the previous year. To most jurisdictions, international information sharing is a crucial part of their work. One jurisdiction reported international information sharing in 70% of all AML/CFT investigations carried out. The sharing of information had proven to be very useful and successful and has already eventuated in some important arrests and seizures.

While most jurisdictions reported that both incoming and outgoing requests for the exchange of information were responded to in a timely and proper way, there were a few jurisdictions with the impression that information sharing for them was more or less a *one-way street*.

While they are doing their best to answer requests from abroad, their own requests were either not being answered in a timely fashion, with the necessary detail required, or not at all. The main reason for this lack of reciprocity is seen to be that these jurisdictions had no FIU or their FIU had not yet become a member of the Egmont Group.

Given that only 16 of the 39 members and observer jurisdictions of the APG are members of the Egmont Group, this approach seems to be a crucial obstacle for the free exchange of information. Solutions could include,

however, a bilateral MoU, direct contact with law enforcement agencies abroad or for APG members of the Egmont Group to assist others to attain Egmont Group membership. Yet for some jurisdictions, these are only real solutions if sufficient TA and training is provided to achieve these aims.

Conclusion

The quantity of jurisdiction reports received by the APG Typologies Working Group from APG jurisdictions this year was slightly down from 2003-04. The quality of these reports varied considerably.

Analysis of the methods reported demonstrated that no particular method had been used individually and most money laundering cases involved a mixture of methods that made it more difficult to detect cases.

Limited research or studies on the methods and trends of money laundering and/or terrorist financing (ML/TF) has meant that there is only partial information on the correlation between methods of ML/TF and predicate offending.

Comments have been made that money obtained through fraud is often laundered via third parties; structuring has been connected to the proceeds from illicit drugs; fraud from the sex/slavery trade and foreign bank accounts for cases involving tax evasion or fraud.

There were a number of emerging and continuing trends seen within the region. No declining or obsolete trends were observed. Jurisdictions in the Asia-Pacific region have very diverse AML/CFT regimes that range from *developing* to *well-established*. The counter-measures employed, therefore, also vary accordingly.

Jurisdictions without AML/CFT laws have considered drafting such regulations and/or issued AML/CFT regulations by their central bank as an important counter-measure. Jurisdictions with established AML/CFT regimes have considered fine-tuning individual pieces of regulation as a major counter-measure.

International co-operation and information sharing were seen as crucial in the fight against money laundering and terrorist financing. The developmental stage of a jurisdiction's AML/CFT regime appears to dictate how the issue of international co-operation is tackled. The approach ranged from building informal networks to providing technical assistance and training.

The international exchanges of information had increased from the previous year. Membership of the Egmont Group, entering into bilateral MoUs or direct contact with law enforcement agencies in other jurisdictions were seen as ways to further enhance exchange mechanisms.

SECTION II

PACIFIC ISLANDS - SUMMARY OF METHODS AND TRENDS

Introduction
As the Asia/Pacific region is so diverse and has varying degrees of population, financial sector development, GDP, as well as AML/CFT regimes, it was suggested that the APG Typologies Working Group look at breaking the regional methods and trends summary into relevant jurisdictional categories.

Due to resource issues, however, only an analysis of the Pacific region has been completed. To ensure some consistency in the definition of *Pacific*, the membership details for the Pacific Islands Forum Secretariat (PIFS) were utilised.

Out of the 15 members of PIFS, only nine jurisdictions are members of the APG and the analysis is restricted to those nine jurisdictions.

Unfortunately, of those nine only seven provided reports reports. For that reason, the analysis is based on seven typologies reports from:

- Australia
- Cook Islands
- Fiji Islands
- New Zealand
- Palau
- Republic of Marshall Islands (RMI)
- Vanuatu

The small number of data sets pre-determines the validity of the analysis. This analysis is very much *quantitative* rather than *qualitative*. The results can only identify common threads rather than typologies specific to the Pacific region. With such a small data set, the analysis consisted of simple comparisons across jurisdictions, collation of the typologies identified and typologies specific to the Pacific region.

Methods
Jurisdictions were asked to provide examples/case studies of methods and facilitation activities under the following categories:

Jurisdiction	Australia	Cook Islands	Fiji Islands	RMI	New Zealand	Niue	Palau	Samoa	Vanuatu
Association with corruption (proceeds of corruption and bribery of officials)	N	N	**Y**	N	**Y**	N/A	N	N/A	?
Association with illegal logging activities	N	N	N	N	N	N/A	N	N/A	?
Currency exchanges/cash conversion	**Y**	N	**Y**	N	**Y**	N/A	N	N/A	?
Cash couriers/currency smuggling (concealment, security, amounts etc.)	**Y**	**Y**	**Y**	N	**Y**	N/A	**Y**	N/A	?
Structuring	**Y**	**Y**	N	N	**Y**	N/A	N	N/A	?
Use of credit cards, cheques, promissory notes etc.	**Y**	N	**Y**	N	**Y**	N/A	N	N/A	?
Purchase of portable valuable commodities (gems, precious metals etc.) or purchase of valuable assets (real estate, race horses, vehicles etc.)	**Y**	N	**Y**	N	**Y**	N/A	N	N/A	?
Commodity exchanges (barter/reinvestment in illicit drugs)	N	N	N	N	N	N/A	**Y**	N/A	?
Wire transfers	**Y**	N	N	N	N	N/A	**Y**	N/A	?
Underground banking services/alternative remittance services	**Y**	N	N	N	N	N/A	**Y**	N/A	?
Trade-based money laundering (false invoicing)	**Y**	N	N	N	N	N/A	**Y**	N/A	?
Gambling activities (use of casinos, horse racing, internet gambling etc.)	**Y**	N	**Y**	N	**Y**	N/A	N	N/A	?
Abuse of Non-Profit Organisations (NPOs)	**Y**	N	N	N	**Y**	N/A	N	N/A	?
Investment in capital markets	**Y**	N	N	N	N	N/A	N	N/A	?
Mingling (business investment)	N	N	**Y**	N	**Y**	N/A	**Y**	N/A	?
Use of shell companies/corporations	N	N	**Y**	N	**Y**	N/A	N	N/A	?
Use of offshore banks and offshore businesses	N	N	**Y**	N	N	N/A	N	N/A	?
Use of nominees, trusts, family members or third parties	**Y**	N	**Y**	N	**Y**	N/A	**Y**	N/A	?
Use of foreign bank accounts	**Y**	N	N	N	N	N/A	N	N/A	?
Use of false identification	**Y**	**Y**	**Y**	N	**Y**	N/A	**Y**	N/A	?
Use of professional services/gatekeepers (lawyers, accountants, brokers etc.)	**Y**	N	N	N	N	N/A	N	N/A	?
Use of the internet (encryption, payment systems, online banking etc.)	**Y**	N	N	N	N	N/A	N	N/A	?
Criminal knowledge of and response to law enforcement/regulations	**Y**	N	N	N	**Y**	N/A	N	N/A	?

Other methods/emerging methods, (use of informal financing/micro financing networks) 'Hui', 'arisan' etc.	**Y**	N	N	N	N	N/A	N	N/A	?

Trends

Trends are the general or continuing tendencies or patterns relating to the methods of money laundering and/or the financing of terrorism.

Jurisdiction	Research or studies undertaken on money laundering methods and trends	Association of types of money laundering or terrorist financing with particular predicate activities (corruption, drugs, fraud, smuggling, terrorist training etc.)	Emerging trends	Continuing trends	Declining trends
Australia	Several (most posted on Attorney Generals website)	Many offences under the securities legislation (ASIC Illegal importation of drugs, fraud and tax evasion)	Increased use of credit/debit card or stored value facilities; alternative payment systems via internet; using Australia Post to wire funds (regularly using false names)	Traditional methods continuing; use of third parties to open accounts solely to receive funds from overseas and resend overseas; structuring cash deposits; nominees to provide *clean names*; front companies; bank drafts using cash; high-value betting (casinos); multiple financial institutions	None
Cook Islands	None	None	None	None	None
Fiji Islands	**Did not utilise pro-forma**				
Marshall Islands	None	None	None	None	None
New Zealand	Co-chair of APG Typologies Working Group	Techniques used in money laundering are the ones that the launderers are most comfortable with	Use of stored value cards; internet	Currency exchanges/cash conversion; cash couriers/currency smuggling; credit cards/cheques; purchase of portable valuable commodities; purchase of valuable assets; gambling activities	None
Palau	None	Prostitution rings and small drug operations	Increase in number of bank license applications; criminal abuse of threshold requirement for suspicious activity reporting	None	Use of Palau for counterfeiting and/or money laundering efforts
Vanuatu	**Did not utilise pro-forma**				

Emerging trends

Australia

A juvenile opened an e-gold account to enable him to receive the proceeds of internet banking thefts from an offshore associate. He then attempted to redeem the value of the e-gold by requesting the e-gold dealer to provide him with Australia Post money orders. In an effort to conceal his identity he informed the dealer that he had lost his passport and requested that the dealer call Australia Post and inform them that a person matching his description would present himself to collect the money orders at a particular time. It is believed that he was not going to send money offshore but would keep the proceeds for himself. He has been arrested and prosecuted.

The Australian High Tec Crimes Centre (AHTCC) was instrumental in the arrest of a person in Perth who was involved in laundering the proceeds of internet banking theft. He stole funds over a period of 12 months and used his bank account to launder AU$60,000.00. In one instance he received AU$10,000.00, which he withdrew from his bank account and sent to criminals in Eastern Europe using Western Union. He also opened a number of bank accounts with different banking institutions and sent the account numbers to contacts in Eastern Europe, allowing them to directly withdraw money via the internet from the Australian accounts.

New Zealand

Since the last APG Typologies Meeting, New Zealand has experienced the internet being used to perpetuate a scam called *phishing* (pronounced fishing) and the subsequent laundering of funds obtained from the scam.

As mentioned in Section I of this report, *phishing* scammers send potential victims an email purporting to be from the victim's bank. The email advises that their bank is updating its online security. The email has a hyperlink to a fake bank website where the victim enters in their online banking identification and password.

Once this is obtained, the *phishing* scammers then transfer money from the victim's account to a *mules* account, which is usually in the same country. The *mules* will then transfer this money overseas to places like Estonia, Latvia, Russia etc. In New Zealand's experience, the *mules* were recruited by an email convincing them that they were forwarding money from the sale of plasma televisions. For completing this service the *mules* received 5% commission.

Palau

A Greek investor who purportedly owns a bank in Moldavia recently contacted persons affiliated with a local bank, which has had its license revoked, to offer his assistance in re-capitalising the bank and allowing the bank to become licensed. Details are not clear at this time but the investor is interested in getting a bank license to facilitate offshore banking, that is, to finance shipping operations and provide services to maritime merchants.

The FIC has received a recent inquiry into the possible application for a license in Palau to facilitate offshore gaming (on luxury cruise ships) off the coast of Japan. The purpose of the venture is to revert income to a Palau entity and deposit earnings in the proposed Palau bank in order to lessen the tax burden on the company and to avoid other legal impediments existent in Japan.

Continuing trends

Australia

AUSTRAC information assisted in identifying real-estate which had been purchased with illegally obtained company funds. A large number of bank cheques in the amount of AU$9,500.00 were used by the defendants to buy the property. These bank cheques were purchased over a period of days by the defendant from numerous banks in the suburbs of Perth.

An individual structured 21 separate withdrawal transactions of AU$9,900.00 from her Australian account while her son deposited 21 transactions of AU$9,900.00 into his accounts within the same period. In the following two weeks, the son conducted a further seven withdrawal transactions of AU$9,900.00 from his account. It is believed these transactions were structured to avoid the FTR Act reporting requirement.

AUSTRAC identified a number of bank accounts and businesses believed to be laundering proceeds derived from alleged criminal activities. It was also found that the alleged money launderers were using the casino as a preferred method of laundering millions of dollars accumulated from their activities. The methods used to launder the money included purchasing and cashing out chips without playing, putting funds through slot machines and claiming credits as a jackpot win and playing games with low returns but higher chances of winning such as *Baccarat*.

An overseas false identification syndicate has been transferring money between members and depositing altered cheques into the subjects account. The use of false identification allowed the individuals involved to conduct the transactions under multiple names in an attempt to avoid the attention of law enforcement agencies. Other individuals also attempted to open accounts to deposit altered cheques.

New Zealand

An investigation into a drug courier in New Zealand, who was importing methamphetamine from Malaysia, ended in a search warrant executed at his address. The search located six kilograms of methamphetamine, NZ$100,000.00 in cash and a cache of jewellery, including seven Rolex watches. It is believed that this courier had made approximately NZ$400,000.00 from his drug related activities and that a significant proportion of this money was used to purchase jewellery.

Recently, the use of gaming machines (pokies/slot machines) in casinos has been seen as a new method employed by launderers. The launderer inserts a significant number of banknotes or coins into a machine, builds up the credit meter, plays a couple of spins and then pushes the collect button. Over a certain limit, the machines do not pay out coins and either cash or a casino issued cheque is given for the credit that has been accumulated.

Conclusion

Only those jurisdictions with well established AML/CFT systems seem to have the necessary capacities to issue a comprehensive typologies report on methods and trends in their jurisdiction.

The countries without AML/CFT laws and regulations, or an FIU do not appear to have the capacities to effectively monitor their AML/CFT situation. For future reference the following criteria would benefit the analysis:

- Existence of a law and its *maturity*.
- Issuing regulations/guidelines in the absence of law or to support the law.
- FIU establishment and development.
- Already carrying out examinations (by supervisors or FIUs).

It is clear that with such a small number of responses, any trends are limited to submissions by Australia, New Zealand and Palau in respect of emerging trends. Some jurisdictions failed to provide any report and others did not utilise the pro-forma, which means analysis would be time consuming. For this exercise those reports have not been included in the analysis.

To claim that this report provides analysis on the trends specific to the Pacific region would be incorrect. This report basically summarises the reports from Australia and New Zealand, as well as some valuable input from Palau.

The information gathering process needs to be reassessed and further resources allocated for more accurate analysis.

SECTION III

USE OF WIRE TRANSFERS FOR TERRORIST FINANCING AND MONEY LAUNDERING IN THE ASIA/PACIFIC REGION

The APG Typologies Working Group is undertaking an in-depth analysis of typologies of wire transfers used for terrorist financing or money laundering in the Asia/Pacific region.

Current case study material on wire transfers was sought from APG jurisdictions. The response, however, did not provide sufficient submissions to undertake a comprehensive and *robust* analysis. As a result, reference has been made to cases reported in the 2003 and 2004 typologies jurisdiction reports to include in the analysis.

Findings
Wire transfers, whether through main/central banks, smaller community banks or registered remittance dealers, offer a quick and effective method of transferring funds from one location to another.

A review of case studies noted that wire transfers have been used by people and organisations involved in terrorist financing and illegal activities including drugs, various types of fraud, tax evasion, people smuggling, vice/prostitution and dealing in contraband, such as cigarettes or counterfeit goods.

The analysis of the allocated case studies did not identify any patterns in the use of wire transfers that could be attributed to any one particular illegal activity or to entities located in a particular country. Variations in the use of wire transfers may be attributed to the level of awareness of money laundering techniques by the entities involved, amount of money required to be moved and regulation of the financial system in the country.

Regardless of the illegal activity involved, there appears to be a sense of *urgency* to move and launder the funds so as to avoid detection by regulators and law enforcement agencies. This often involves sending the money offshore, out of the reach of local law enforcement agencies.

Due to the need to move funds quickly, there will often be an element of *risk* that the entities involved may undertake, which is one area that can be capitalised on by FIUs and law enforcement agencies. One of the primary issues for criminals is to conceal the source of the funds. The main methods identified included:

- Structuring - keeping amounts below the reportable limit.
- Smurfing - using other people, for example, family members or unrelated individuals, such as students, to conduct transactions.

- Shell companies - sending and/or receiving funds making the transaction appear business-related.
- Co-mingling - combining illegal funds with legitimate business activity.
- False invoicing - falsifying the amount owed so that it exceeds the actual value of goods imported.
- False identification - remitting funds and/or establishing and operating accounts locally or overseas using false identification.
- Charities or Non-Profit Organisations (NPOs) - *Skimming* a proportion of donated funds from the account to be used for unrelated purposes.

In considering the overseas destinations where criminal funds were transferred, the possible reasons for the decision could be based on the:

- Source of the commodity, either to pre-purchase commodities or to move proceeds of crime.
- Location of the principals/financiers of the criminal group.
- Weak AML/CFT regulations in the banking sector to avoid detection.
- tax havens to avoid detection and repatriation.
- Major financial hubs, which may be in an attempt to *lose* the transaction in a high-volume environment.
- Location of traditional trading partners, which may attempt to make the transaction appear legitimate.

It is also possible that once the funds arrived at the overseas location, part or all may have been forwarded on to another destination. The analysis of case studies also noted a reliance on smaller community banks and registered alternate remittance dealers to remit funds. The possible reasons behind the use of these entities as opposed to the larger banks and financial institutions included:

- Quick, cost effective with *no questions asked*.
- *Trust* element of dealing with people of their shared background and culture.
- Ability to reach remote regions where established mainstream institutions do not operate.
- Concerns over corruption in the local banking system.

These considerations would also be relevant to the use of hawalas or other underground banking systems.

Methods and trends

From the case studies analysed, the following indicators drew suspicion to the actual transaction:

Structuring the amount to avoid the reporting requirements of that country.

An individual was fraudulently collecting unemployment benefits under several false names. Over a period of 12 months he had accumulated over US$200 000.00. In an attempt to launder these funds he remitted the proceeds in amounts of $9 500.00 to accounts he held in another country.

Successive transfers (either on the same day or over a period of two to three days) from multiple customers to the same recipient.

A group of individuals associated with a cigarette smuggling syndicate attempted to remit the proceeds of their activities to a financial controller located in another country. A suspicious transaction report was submitted by one of the banks after three successive customers, each with a note detailing the same recipient's name and account number, requested a wire transfer to that recipient.

Multiple originating customers who share common identifiers, for example, family name, address, telephone number.

While analysing the financial activities of a narcotics syndicate, it was established that funds were being remitted back to the principal importers by a large network of originating customers. These transactions were being conducted at various branches of several financial institutions with three or four transactions being conducted on the same day. A common link was identified between the originating customers who had provided the same or similar address details at the time of the transactions. There were some variations in the street number and slight variations in the spelling of the street name. It is suspected that several of the names were fictitious and may have in fact been the same customer using various aliases.

Funds sent to or received from a country of interest (known to be a tax haven, have lax banking regulations or is a source of narcotics or centre of other illegal activity), especially where there is no logical business or personal relationship with the other country.

The taxation office in Country X was investigating the activities of a number of businesses from the one locality who had each filed large losses on their annual returns. Inquiries noted that the businesses all used the services of the same accountant to lodge their returns. Further investigation into the financial activities of the accountant noted a large number of wire transfers to Country Y, known to be a tax haven. It is alleged that the accountant was assisting the business owners to evade paying taxes on their earnings.

Stated occupation of originating customer is not consistent with amount of money being remitted, for example, students or backpackers.

A syndicate who were importing narcotics recruited university students and backpackers to assist with remitting the proceeds from the sales of the drugs back to the organisers. Each person was paid a small commission for their services and it is believed that they had no knowledge of where the funds had come from. This network was detected after a number of suspicious transaction reports were submitted on some structured transfers.

High volume of wire transfers from persons or organisations that do not hold accounts with the institution.

Two individuals, who were subsequently identified as being involved in a stock market manipulation/fraud, conducted a large number of wire transfers from the same branch of a bank located near their office. Neither person held an account with the bank but would come in with cash varying in amounts from $2 000.00 up to $40 000.00 and arrange to remit these funds to an account in another country. The funds were believed to be their share of profits made from the stock trades. In a short period of time they had remitted over $900 000.00.

Country of destination for wire transfer is not consistent with nationality of originating customer.

An individual from Country A produced his passport as proof of identity when establishing an account with a financial institution in Country B. Soon after opening this account, a number of cash deposits were made, which were subsequently withdrawn and transferred to Country C. Inquiries by local law enforcement agencies identified that this person was suspected of operating a number of fraudulent scams.

Large amounts of money which do not appear consistent with business activity of an organisation or the available wealth of an individual.

An employee of a trans-national trading company defrauded the company over a period of 12 months of more than US$4.5 million. The funds were remitted to her own personal account, as well as to those of other family members and friends in other countries.

The individuals involved in a drug syndicate sent the proceeds from drugs sales from Country A to Country B using a dry cleaning business as a front. The total amount remitted was over US$80,000.00.

Funds are withdrawn in cash immediately after being cleared.

A senior legal clerk in a legal firm was in charge of dealing with buying/selling transactions of stocks entrusted by clients. In his position the clerk was also authorised to open bank accounts on behalf of the clients. The embezzlement activities of this employee were detected by a bank after he remitted a large sum to his personal bank account and then immediately withdrew the funds in cash to purchase diamonds, jewellery and department store vouchers.

Funds are moved to another account locally or overseas immediately after being cleared.

Further investigations into the activities of the above senior legal clerk noted that he had also diverted some of the funds to an overseas shell company that he had established.

Conclusion

It is evident from the review of case studies that wire transfers are extensively used by individuals and organisations involved in various areas of illegal activity to assist in the laundering of proceeds or to provide funding for a particular cause.

A number of the indicators identified are common to various activities. While proactive monitoring of the indicators may initially make it difficult to confirm the underlying offence, additional analysis involving the location where funds

have been sent and/or the nationality of the entities involved may clarify the situation.

A combination of one or more of the indicators could be used to proactively detect possible cases of money laundering or terrorist financing. This could be achieved through:

- Educating reporting entities to be in a position to initiate the filing of a suspicious transaction report.
- FIUs that collect wire transfer reports monitoring the indicators to detect anomalies in the reporting patterns.

Each jurisdiction could define a more precise set of parameters and indicators for identifying suspicious wire transfer transactions based on case studies from their region.

SECTION IV

CASH COURIER ISSUES

The APG Typologies Working Group first addressed this issue at the December 2003 Workshop in Kuala Lumpur. A detailed description of the APG's findings is contained in the APG Annual Typologies Report 2003-2004, issued in June 2004. The APG's work was instrumental in the development of a new international standard to strengthen the world's counter-terrorist financing defences.

At the October 2004 Workshop in Brunei Darussalam, the APG Typologies Workshop assisted the FATF by addressing the development of a new recommendation on cash couriers, as well as additional guidance.

In October 2004, the FATF adopted *Special Recommendation IX* on cash couriers[1] and its interpretative note[2].

In February 2005, the FATF issued an international best practices paper on detecting and preventing the cross-border transportation of cash by terrorists and other criminals[3].

The APG believes that this new measure, which calls upon countries to implement cross-border currency reporting requirements and to confiscate funds transported in violation of such requirements, is a milestone in the fight against terrorist financing.

Nature of the problem
Reporting by intelligence and law enforcement continues to indicate that cash smuggling is one of the major methods used by terrorist financiers, money launderers and organised crime figures to move money derived from and/or in support of their activities. The majority of submissions from APG member jurisdictions this year have highlighted the key role that cash smuggling often plays in money laundering operations.

Methods and trends
In cash smuggling operations, couriers will travel over roads, through airports or by sea with loads of cash, often stuffed into boxes, suitcases and concealed compartments in vehicles. One Pacific Island jurisdiction noted that some smugglers will attempt to obtain VIP status at the airport in order to avoid detection by customs authorities.

Vast and porous borders within the region make the job of detecting couriers even more difficult. Couriers also use privately-owned boats and clandestine

[1] See the following website to obtain a copy of the *Nine Special Recommendations* on Terrorist Financing: http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf
[2] See http://www.fatf-gafi.org/dataoecd/5/48/34291218.pdf
[3] See http://www.fatf-gafi.org/dataoecd/50/63/34424128.pdf

roads to smuggle money thereby circumventing official border *check-points*. APG experts have identified the following key methods and trends in the region:

- Use of co-ordinated, multi-jurisdictional couriering syndicates.
- Common connections between cash couriers and trade-based money laundering.
- Major regional financial centres serving as destination points for the movement of cash through couriers.
- Connections between currency smuggling and currency counterfeiting.
- Connections between currency smuggling and casino junket operators.
- Use of cash couriers to support underground foreign exchange operations.
- Use of cash couriers by drug syndicates transporting the proceeds of narcotics.

Case examples

Money Laundering
A joint investigation involving law enforcement agencies in Australia, Hong Kong and Thailand related to a foreign brokerage company operating in Thailand that sold false share certificates to customers in various countries. Thailand authorities took action against this company for violating the Security and Exchange Act and defrauding the public. Thai law enforcement executed search warrants on the offices and seized approximately US$38,000.00 worth of Baht and a number of bank accounts in Thailand. Many bank accounts held by this group in Hong Kong were also seized by the Hong Kong Police. During the same period, another group of companies using the same modus operandi were discovered in Thailand. Thai authorities seized their bank accounts totalling approximately US$300,000.00 in Baht. The operators of these companies fled their premises and two individuals attempted to fly to Hong Kong carrying more than US$50,000.00 in Baht, which was seized at the airport by Royal Thai Customs.

Terrorist Financing
United States Federal Agents initiated an investigation on Abdurahman M. Alamoudi, for devising a scheme to obtain money from Libya and other sources overseas for transmission into the United States without attracting the attention of federal immigration, customs or law enforcement officials. In addition to a number of illicit transactions, on 16 August 2003, United Kingdom Customs officers seized approximately US$340,000.00 of undeclared currency on route to Damascus Syria. Alamoudi engaged in a number of illicit activities including making false statements to immigration officials about overseas travel; attempting to structure the importation of cash received from Libyan sources overseas and violation of a number of sanctions related to travel to and commerce with Libya. Investigators arrested Alamoudi on 28 September 2003 and on 30 July 2004, he pleaded guilty to three criminal violations relating to his activities domestically and abroad with nations and organisations that have ties to terrorism and his participation in a plot to assassinate a prominent Saudi Arabian official.

Implementation challenges

The key to detecting cash couriers relies almost exclusively on Customs and border security officials. Because many Customs officials around the world

lack the ability, or in some cases the legal basis, to detect cash or do not even think to look for it, specialised training and equipment is needed to detect cash both inbound and outbound.

The APG Typologies Meeting in Brunei included a training workshop on identifying and targeting cash couriers. Focus was placed on exploiting various methods of transporting bulk currency and negotiable instruments that may be utilised by criminal organisations.

The targeted areas covered were express courier hubs, airports, seaports, outbound cargo and passengers travelling to locations that pose an outbound threat. The Workshop also included a presentation on using *red flag* indicators to identify verbal and non-verbal signs of possible cash smuggling.

In order to stop cash couriers, law enforcement officials must evaluate the totality of the circumstances and be able to make quick decisions. These decisions should be based on an analysis of the subjects' behaviour, appearance, documents and responses compared to a known baseline of normal behaviour, patterns and trends.

Conclusion

Effective linkages between Customs, Immigration and Police should be established to respond to currency detections and to develop intelligence. Countries should ensure that the information gathered from cash seizures is shared domestically. Customs authorities should also share information with their FIU and other law enforcement agencies, to ensure leads are acted upon effectively and the appropriate enforcement action taken immediately.

Co-operation arrangements between jurisdictions are also essential to allow proper responses to cash courier investigations. The importance of speedy information sharing to detect cash couriers cannot be overstated. Jurisdictions should consider, for example, entering into bilateral Customs-to-Customs information exchanges on cross-border reporting and cash seizures.