



Asia/Pacific Group  
on Money Laundering

**APG Typologies Working Group**

**ASIA/PACIFIC GROUP ON MONEY LAUNDERING  
(APG)**

**ANNUAL TYPOLOGIES REPORT 2003-04**

# CONTENTS

<b>INTRODUCTION</b>	<b>1</b>
Background	1
The APG’s mandate for undertaking typologies work	1
Typologies Framework	1
The Typologies Working Group	2
APG Typologies Workshop 2003	3
Typologies project groups	3
External typologies opportunities	4
Further APG Typologies Work: 2004-05	4
<b>SECTION I</b>	<b>5</b>
<b>Summary of Regional Methods and Trends</b>	<b>5</b>
Introduction	5
Methods	5
Currency exchanges/cash conversion	6
Currency Smuggling	6
Use of credit cards, cheques, promissory notes, etc.	6
Purchase of portable valuable commodities (gems, precious metals etc.)	6
Gambling activities (casinos, horse racing, Internet gambling, etc.)	8
Structuring (Smurfing)	9
Wire transfers	9
Underground banking and alternative remittance services	10
Abuse of non-profit organisations	10
Purchase of valuable assets	10
Co-mingling (business investment)	10
Use of nominees, trusts, family members or third parties	11
Use of foreign bank accounts	11
Use of false identities	11
Use of professional services (lawyers, accountants, brokers etc.)	12
Association with Corruption	13
Uncommon Methods	13
Commodity exchanges	13
Investment in Capital Markets	13
Use of shell companies/corporations	13
Use of offshore banks and corporations	14
Use of informal financing networks (“Hui”, “arisen” etc.)	14
Use of the Internet	14
Use of violence/coercion	14
Criminal knowledge of and response to law enforcement/regulations	14
Further methods or techniques	14
Trends	14
Counter measures	15
Co-operation	16
Conclusion	17
<b>SECTION II</b>	<b>19</b>
<b>Terrorist Financing Issues</b>	<b>19</b>
Abuse of Wire Transfers	19

Methods and Trends	20
Case Studies	21
Policy Implications	21
The Financial Action Task Force and the relation between wire transfers and terrorist financing	22
Abuse of Non-Profit Organisations (NPOs)	23
Nature of the Problem	23
Characteristics of NPOs	24
Methods and Trends	24
Policy Implications	26
Case Studies	27
The Financial Action Task Force and the Abuse of NPOs	30
Conclusion	32
<b>SECTION III</b>	<b>33</b>
<b>SECTION III</b>	<b>33</b>
<b>Cash Courier Issues</b>	<b>33</b>
Nature of the Problem	33
Methods and Trends	33
Case Examples	34
Policy Implications	35
Conclusion	35
<b>SECTION IV</b>	<b>37</b>
<b>Corruption Issues</b>	<b>37</b>
Introduction	37
The threat from corruption-related money laundering	37
Diversity across the region	37
Impacts of corruption and money laundering	37
Recent developments in the global standards	38
What the APG has done	39
Key findings from 2003 Typologies Workshop	39
Prevalent methods	39
Case Studies	40
Difficulties encountered in combating corruption-related money laundering	42
Conclusion	42



# INTRODUCTION

## **Background**

In June 2002, the APG Secretariat prepared a report on money laundering trends and techniques in the Asia/Pacific region. A further report was produced by the Secretariat in September 2003. Both reports received positive feedback.

In September 2003, APG members endorsed a new APG Typologies Framework, which called for the production of annual APG Typologies Reports. In December 2003, during the APG Typologies Workshop in Kuala Lumpur, the APG Typologies Working Group undertook to prepare the Annual Typologies Report 2003-04 with assistance from the APG Secretariat. That report follows.

## **The APG's mandate for undertaking typologies work**

In broad terms, APG 'typologies' work is a description and/or analysis of the nature of money laundering and the financing of terrorism, including methods and trends. Since its establishment in 1997, the APG has used this work to develop a better understanding of the money laundering environment in the Asia/Pacific region.

The information contained within has many uses for the APG, for example: this typology information is used to support policy setting, implementation work (particularly in the law enforcement sector), assessment work and the APG's input to the AML/CFT standard setting processes.

The APG consistently receives requests from members and observers, multilateral donor organisations, AML/CFT standard setting bodies and implementing agencies, for contextually relevant case studies and analyses of methods and trends in the money laundering and terrorism financing environment in the Asia/Pacific region. As the regional focal point for AML/CFT matters, the APG is the best-placed body in this region to collect, analyse and share such information and case studies.

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's (FATF) 40 Recommendations and eight Special Recommendations. Effective implementation of the revised global standards benefits from jurisdictions' understanding of the threat and risks related to money laundering and terrorist financing.

## ***Typologies Framework***

The APG Business Plan 2003-04 establishes an APG Typologies Collection and Analysis Framework to achieve integrated collection, analysis and distribution of

typologies information, intelligence and case studies relating to money laundering and the financing of terrorism in the Asia/Pacific region.

In order to ensure that the APG's work remains practically focused on the region's current situation, an integrated approach is needed to maintain an accurate picture of the money laundering and financing of terrorism environment, particularly in the Asia/Pacific region.

A Typologies Framework has been established to increase the quality and quantity of information collected. This is being achieved through:

- supporting a standing APG Typologies Working Group which is undertaking in-depth studies;
- continuing to conduct Annual Typologies Workshops; and
- selecting further topics to be studied as typologies projects.

Future consideration will be given to the APG establishing an APG Research Liaison Advisory Group to promote academic research on AML/CFT issues.

### ***The Typologies Working Group***

During the 2003 APG Annual Meeting, members decided to establish an APG Working Group on Typologies, as part of the Typologies Framework, with clear terms of reference to:

- i. Conduct a series of in-depth studies on particular typology topics
- ii. Support a network of APG Typology experts (e.g. on alternative remittance systems)
- iii. Provide practical advice on the APG Typologies collection and analysis Framework.

Meetings of the APG Typologies Working Group are open to all APG members and observers. The Working Group does, however, have core members to progress its work. The following members of the Typologies Working Group were confirmed during the inaugural meeting of the Working Group in Kuala Lumpur in December 2003:

- Indonesia (Co-Chair)
- New Zealand (Co-Chair)
- Australia
- Chinese Taipei
- Fiji
- Germany
- Hong Kong, China
- India
- Japan
- Korea
- Palau
- Philippines
- United States
- Egmont
- FATF
- Chairs of typologies project groups

### ***APG Typologies Workshop 2003***

Building on previous successful APG Typologies Workshops, and as part of the new APG typologies framework, Malaysia hosted the APG Typologies Workshop in Kuala Lumpur on 8 and 9 December 2003. 140 participants representing 25 member jurisdictions, eight observer jurisdictions and six international and regional organisations attended the Workshop. The Typologies Workshop was chaired jointly by Datuk Zamani Abdul Ghani, Assistant Governor Bank Negara Malaysia and Rick McDonell, Head APG Secretariat.

Major topics covered over the two days of the Workshop included:

- i. *Terrorist financing methods*: particular aspects of terrorist financing were the subject of examination; wire transfers, abuse of charitable institutions, and recent case studies of terrorist financing methods and trends
- ii. *Cash couriers*: included consideration of methods and trends with cash couriers, cash economy and trade-based money laundering issues
- iii. *Corruption issues*: money laundering trends and methods pursuant to corruption.

Special presentations were given on each of these topics. Breakout groups then discussed the topics of corruption and cash couriers in greater depth.

A separate comprehensive report on the Typologies Workshop 2003 is being sent to members and observers.

### ***Typologies project groups***

Several breakout sessions took place during the APG Typologies Workshop 2003. Pakistan and Hong Kong, China chaired the Workshop's breakout session on corruption-related money laundering issues, with over 45 participants taking part. Arising from this session a Typologies Project Group has been formed to prepare a scoping paper on corruption-related money laundering issues. The Project Group consists of Hong Kong, China, Pakistan and Malaysia, and has contributed to the preparation of this Typologies Report. The group is expected to present a preliminary scoping paper on key issues arising from its work so far, to APG Typologies Working Group during mid 2004.

The United States chaired the breakout session on cash courier issues. Over 40 participants took part in this session. A number of methods, trends and implementation issues were highlighted during the session. Arising from the session on cash couriers are the typologies that have been contributed to this Typologies Report. Further Typologies issues on cash couriers will be considered by the APG Typologies Working Group and by APG members during the 2004 APG Annual Meeting in Seoul.

### **External typologies opportunities**

The APG participated in and contributed to the FATF's 2003 Typologies Meeting in Mexico in November 2003. APG participants in the FATF Typologies Meeting included the six APG FATF members as well as Korea, India and the APG Secretariat. The 2003 FATF Typologies Meeting resulted in the FATF progressing its work on a number of money laundering and terrorist financing typologies including abuse of the insurance sector, abuse of non-profit organisations, wire transfers and issues of politically exposed persons.

The APG will continue to work with the FATF and FATF-style regional bodies to ensure closer co-operation and co-ordination of typologies work that it and these other bodies undertake.

### **Further APG Typologies Work: 2004-05**

The APG Typologies Working Group is scheduled to convene a meeting during the 2004 APG Annual Meeting to consider current tasks, future typologies projects, topics for the 2004 Typologies Workshop and other issues related to the Typologies Framework.

The 2004 APG Typologies Workshop will be held in Brunei Darussalam from 5<sup>th</sup> – 6<sup>th</sup> October 2004. Further details will be advised to members and posted on the APG website when available.

The APG Secretariat plans to significantly expand the typologies resources available via the APG website. This will include APG member documents in the secure members area of the website and a broader range of publicly available documents.

# SECTION I

## Summary of Regional Methods and Trends

### Introduction

In preparation for the 2003 Typologies Workshop in Kuala Lumpur, the APG Secretariat asked each jurisdiction for typology information, and provided a special pro-forma outline for these jurisdictional reports.

Only 25 (64%) of the current 39 member and observer jurisdictions submitted their Typology Reports for the Workshop in Kuala Lumpur. Approximately half of the 25 reports followed the outline provided by the APG Secretariat.

It was noted from the Typology Reports that the experience of AML/CFT enforcement amongst the jurisdictions in the region was very diverse, ranging from relatively new regimes to well established ones.

Terrorist financing (the abuse of wire transfers and the abuse of non profit organisations), the use of cash couriers in money laundering and money laundering related to corruption are not covered in this Section, but will be examined in their own specific sections of this report.

### Methods

Most of the jurisdictional reports received contained detailed information on methods used by money launderers in their respective jurisdictions and often outlined individual cases, which highlighted the diversity in complexity of money laundering cases reported.

While some reports noted schemes consisting of just one or two methods, other jurisdictions reported cases where investigators face complex money laundering patterns combining many different methods (which fortunately provide additional chances for detection).

Such diversity might be explained by the fact that some jurisdictions are still setting up efficient anti-money laundering regimes and as yet do not pose a real challenge to money launderers. Those jurisdictions with established anti-money laundering regimes make it more difficult for money launderers, forcing them to utilise more sophisticated and complex laundering methods.

The reports did not highlight one dominating method used to launder money nor any specific method unique to the Asia/Pacific region. This is not surprising given the broad political, economic, social and cultural diversity of member and observer jurisdictions.

A summary, by methods used, is as follows:

### **Currency exchanges/cash conversion**

This method was not commonly reported as being used, which is somewhat surprising given the number of cash-based economies and the proximity of other countries within the region. Of the cases that were reported, most of the currency exchanges used also offered other services such as alternative remittance, immigration consultancy or travel agencies.

#### **Example: Lao Peoples Democratic Republic**

As the Lao P.D.R. is basically a cash economy, people in general prefer to hold foreign currency cash, namely US dollar and Thai baht. These currencies are the preferred means of payment domestically, especially for the purchase of high value assets such as real estate and motor cars. Informal or black currency exchange markets are prevalent and well organised which may not only provide cash conversion services but may also provide alternative remittance and other informal banking services.

### **Currency Smuggling**

Refer to Section III of this Report.

### **Use of credit cards, cheques, promissory notes, etc.**

The use of credit cards in money laundering was reported as being the source of illicit funds rather than as a vehicle to launder those funds. However, the use of a “stored value” card to launder funds was seen as an emerging method.

#### **Example: Australia**

Travelex now issue a debit card called a ‘Cashpassportcard’ with an AU\$25,000 (US\$18,000) value limit. The holder of a Cashpassportcard was found to have regularly loaded value by paying cash just below the AU\$10,000 (US\$7,500) reportable limit. A second card linked to the same account was sent overseas where the funds were withdrawn through ATMs. The process was repeated, with more than AU\$100,000 (US\$70,000) laundered through the scheme.

Where cheques and travellers’ cheques were noted, they were reported being used as instruments in commission of the predicate fraud offence. This fraud offence usually involved the misappropriation of funds by a trusted official within an organisation being defrauded.

The use of promissory notes was not a common medium used in the laundering process. It was only mentioned briefly in two reports. The first mentioned this medium forming part of the “supporting” documentation for a financial scam. The other jurisdiction cited the notes being used as one of many forms of donation payments made in relation to the abuse of non-profit organisations in the financing of terrorism.

### **Purchase of portable valuable commodities (gems, precious metals etc.)**

The purchasing or use of gold bullion and other portable valuable commodities still continues to be seen in the APG region. These types of commodities are seen as easily traded. Depending on the jurisdiction, these commodities can either be

directly used to obtain other valuable property, such as vehicles and real estate, or can be quickly sold to provide the funds for the purchase of such assets.

**Example: United States of America**

In January 1999, the El Dorado Task Force (EDTF), under the auspices of ICE's SAC/New York, initiated Operation Meltdown, an undercover investigation targeting gold suppliers in the New York area. The EDTF received information from a documented informant that numerous businesses in the New York area were laundering narcotics proceeds through the sale of gold and other precious metals. According to the information, a jeweler would receive narcotics proceeds (cash) and would either provide gold pellets (shots) or melt and mold the equivalent value of gold into various items.

The EDTF identified jewellers that molded gold into the following items: bolts, nuts, cones and wrenches. In some cases the gold was secreted into jewellery machines which were then shipped to Colombia. Once the gold was received in Colombia, it was resold for cash, thus completing the laundering cycle.

During the course of the investigation, confidential sources of information and undercover agents delivered purported narcotics proceeds to several jewellery stores and received either gold shot or disguised gold in return. Undercover agents and confidential sources delivered more than US\$1 million dollars in cash to different wholesale and retail businesses. In return for the cash, the undercover agents and co-operating witnesses received more than 100 kilograms of gold, which they told the suspects would be smuggled to Colombia.

On 4 June 2003, ICE SAIC/New York agents assigned to EDTF conducted a takedown that included the arrest of 11 suspects for money laundering violations and execution of eight search warrants. To date Operation Meltdown has seen 23 individuals arrested and 6 guilty pleas under Title 18 USC 1956 Violations have been entered.

To date, 140 kilograms of gold (estimated value of US\$1.4 million); approximately US\$1 million in loose diamonds; \$2.8 million in U.S. currency; 118 kilograms of cocaine; 3 molds in the shape of cones, wrenches and screws; 6 guns and 2 vehicles have been seized.

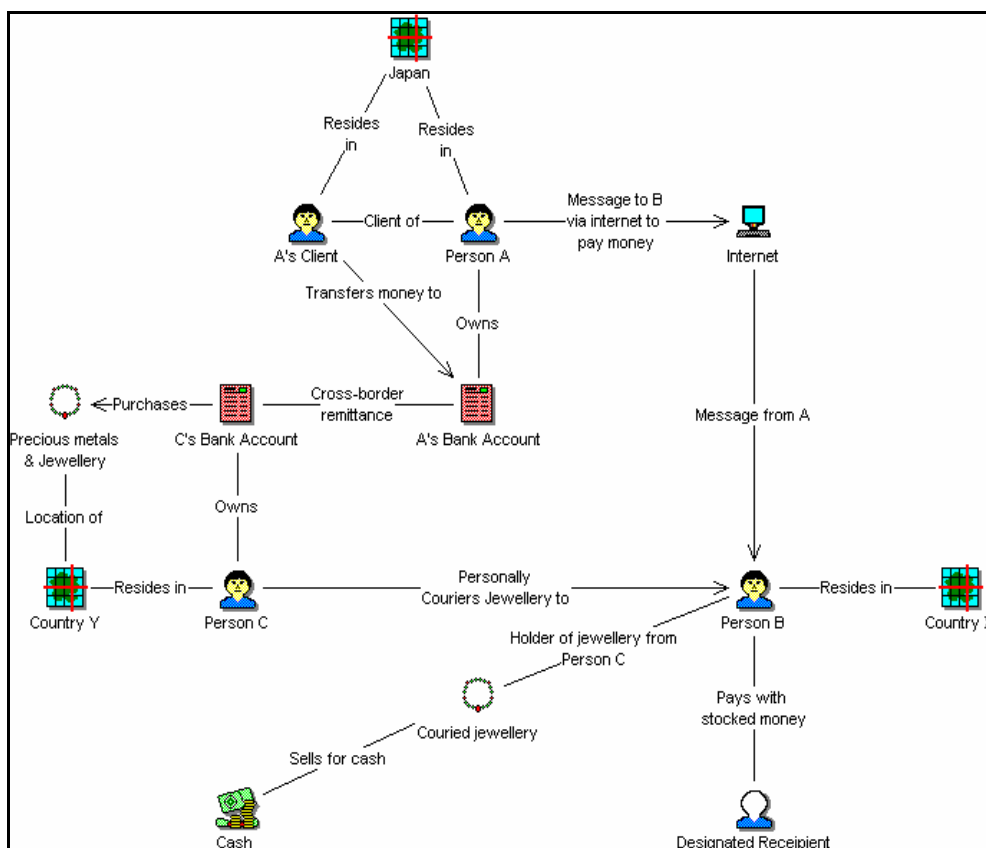
**Example: New Zealand**

The purchase of portable valuable commodities such as gems and precious metals has not been a significant method employed in laundering in New Zealand in recent times.

Last year, however, one case of a person charged with the manufacturing and selling of methamphetamine has uncovered the use of this method. Upon the arrest of this person, searches were carried out of storage facilities that he was using. These searches revealed that he had jewellery, gold, silver and platinum bars worth a total value of NZ\$400,000 (US\$24,400). After the suspect's arrest it was established that his girlfriend was in the process of purchasing real estate and had paid the deposit with NZ\$50,000 (US\$30,500) cash. When paying the deposit, she advised the conveyancing solicitor that the cash had come from the sale of gold bars that her grandmother had owned.

Whereas the above two cases were directly related to the trading of illicit drugs, Japan reported the purchasing and reselling of precious metals and jewellery for settling of illegal alternative remittance payments. See i2 chart below.

*i2 chart showing illegal alternative remittance payments*



- Originator A in Japan, upon a remittance request from a client residing in Japan, directs him/her to transfer the amount of remittance and a commission to the bank account of A.
- Payer B who is in country X receives payment directions from A by the Internet, the telephone, facsimile, etc., and pays the specified amount of money to the designated recipient out of the stocked money.
- On the other hand, A carries out cross-border remittance of the money collected in Japan regularly to the bank account of accomplice C in country Y.
- C takes out the money from his bank account and purchases precious metals and jewellery in country Y. C carries these precious metals and jewellery into country X by means of wearing them on the body, putting them into carry-on bags, etc., and hands them to B.
- B cashes the precious metals and jewellery thus brought in and fills up shortage of money.

***Gambling activities (casinos, horse racing, Internet gambling, etc.)***

In this category the use of casinos in the laundering process was most prominent. The methods used by the launderers in relation to casinos included:

- exchanging large amounts of small denomination bank notes for larger denominations without gambling
- purchasing gambling chips with cash followed by little or no gambling
- exchanging chips back to cash or to a casino issued cheque
- wiring funds to a casino account followed by a withdrawal by casino issued cheque
- inserting significant numbers of bank notes into a slot/poker machine and collecting payment of the built up credits by way of a casino issued cheque
- loaning funds for gambling to legitimate businessmen with repayment of the funds being a discounted amount. (a relevant case study from Australia is set out under “use of professional services” [page 15]).

In previous years the use of other gambling activities, such as Internet gambling and lotteries had been used by launderers in the Asia/Pacific region, these methods were not reported in the 2003/2004 year.

### ***Structuring (Smurfing)***

Many of the jurisdictions with threshold reporting requirements commented that structuring/smurfing was common method employed by launderers to try and evade detection.

Of interest was the structuring of transactions reported in jurisdictions that did not have any threshold-based transaction reporting. It is unclear from the reports if the structuring occurred as the launderers mistakenly believed there was a threshold that would automatically trigger cash transaction reporting, or whether they believed that the lower value of the transaction would not arouse as much suspicion as a larger one.

#### **Example: Hong Kong China**

Syndicate Y was Hong Kong-based and was engaged in importing drugs to jurisdiction Z directly from a drug source country. It employed a sophisticated money laundering cell in jurisdiction Z to launder the profits generated from the importations and to transfer them back to Hong Kong.

The money laundering cell employed a number of frontmen to remit structured amounts of monies from jurisdiction Z to Hong Kong through normal banking systems. The frontmen used false identities to effect the remittances. The money laundering cell also employed several frontmen in Hong Kong to open bank accounts to receive the structured remittances and to withdraw them in cash to break the audit trail.

The cash was then handed over to syndicate Y. In the first three quarters of 2003, the syndicate remitted over HK\$40 million (US\$5.1 million) to Hong Kong from jurisdiction Z. The money laundering cell charged Syndicate Y a commission for laundering and moving funds. Intelligence suggested the money laundering cell also served many other criminal syndicates in transferring illicit funds out of jurisdiction Z.

### ***Wire transfers***

Refer to Section II of this report.

### ***Underground banking and alternative remittance services***

Underground banking, alternative remittance services and informal financing networks have been the subject of considerable study by the APG in recent years. Cases are still being reported in the region. Almost all jurisdictions within the region are in the process of implementing the recommendation and best practices issued by the FATF<sup>1</sup> and the APG<sup>2</sup>. In most cases, the reports emphasised the strong potential for misuse of these systems by launderers, but that they had only actually been misused on a few occasions.

### ***Abuse of non-profit organisations***

Refer to Section II of this report.

### ***Purchase of valuable assets***

Acquiring valuable assets is usually one of the main goals sought from the commission of high value predicate offences such as serious fraud and high level drug trafficking. It is understandable, therefore, that many jurisdictions reported that the purchase of valuable assets has occurred.

Valuable assets were reportedly used either to provide legitimacy to the offenders'/launderers' illicit income (legitimate cash related businesses), (also forms part of the "mingling" category below), or merely the "spoils" acquired from illicit accumulation of wealth (expensive real estate/vehicles etc). One jurisdiction also reported the reinvestment of the proceeds of crime by purchasing real estate to provide another locality to manufacture more prohibited drugs.

### ***Co-mingling (business investment)***

Co-mingling legal and illegal funds appears to be a quite common method in the region. In many cases the launderers either used established business they own or have purchased businesses specifically to aid in the laundering process.

#### **Example: Malaysia**

In a two-year period a group terrorised the country with daring robberies at private and public premises. The robbers' main targets were jewellery and pawnshops. During the period, the total haul of ill-gotten proceeds from the criminal activities came to RM22 million (US\$5.8 million).

The robbers' proceeds were laundered by acquiring various types of businesses such as seafood restaurants, car accessories and electrical shops. The bulk of the laundered proceeds were invested in the jewellery business where the leader of the gang allegedly owned jewellery shops in Kuala Lumpur. Following investigations by the police, several movable properties allegedly owned by the gang members were seized.

<sup>1</sup> [http://www.fatf-gafi.org/SRecsTF\\_en.htm#VI.%20Alternative](http://www.fatf-gafi.org/SRecsTF_en.htm#VI.%20Alternative)

<sup>2</sup> APG Typologies Working Group on Alternative Remittance and Underground Banking Systems: *Alternative Remittance Regulation Implementation Package*

**Example: Palau**

Palau is currently investigating the use of local businesses for the laundering of money. It is suspected that at least two local businesses are involved. The preliminary investigation has revealed that these businesses receive illicit funds in exchange for goods and services that are never provided. The funds are then laundered through these otherwise legitimate companies and repatriated to offshore entities as profits from the local business.

***Use of nominees, trusts, family members or third parties***

The region continues to see the use of trusts, family members and third parties in money laundering as a common practice. These entities are predominately used for the purposes of either concealment/layering of funds or for protection of assets from confiscation laws.

**Example: Singapore**

"Chan" was a customer service executive at a branch of a foreign bank. His role was to manage the day-to-day banking operations of the branch and has authorised to singly approve transactions for up to S\$55,000 (US\$32,000). Between 27 May 1995 and 17 January 2003, "Chan" fraudulently transferred, on 103 occasions, a total of SG\$462,570.07 (US\$269,586) from the bank's fixed interest account into a savings account belonging to his mother, which was with the same bank.

Investigations revealed that "Chan" would raise fictitious debit vouchers to debit the bank's fixed deposit interest account. He would also raise a fictitious credit voucher to credit the amount into a savings account. After preparing the vouchers, "Chan" would pass them to one of the bank tellers at the front desk. "Chan" was authorised to raise and sign such vouchers, which are usually used for adjustments required in crediting customer's interest. As such, the teller would not raise any questions and would transfer of funds.

"Chan" knew that he could not directly use his own bank account to receive the misappropriated funds arising from the fictitious vouchers. To avoid suspicion, he used his mother's account to complete the debit and credit process. Subsequently he would withdraw the monies in cash through an ATM. "Chan" deposited a total of SG\$354,959.76 (US\$206,870) into his own bank account over the period 30 May 1995 to January 2003. "Chan" had concealed the source and ownership of the monies representing his criminal proceeds and thereby committed an offence of concealing his proceeds of crime.

***Use of foreign bank accounts***

Several jurisdictions reported criminals laundering funds through bank accounts held in other countries. Two jurisdictions instead experienced cases of foreign criminals resident in other countries using bank accounts in their jurisdiction.

The use of foreign bank accounts can be seen as an effective method to hide illicit funds. They are relatively easy to set up and access, while affording the holder of the account the possible protection of less stringent AML reporting regimes or difficulties for the enforcement of asset confiscation.

***Use of false identities***

Several jurisdictions noted this method was regularly employed in the laundering process. The most common circumstance was in opening bank accounts with forged documentation. Often this documentation was in the form of foreign passports, some being very professional forgeries. Comment was made that it was difficult for bank staff to detect forgeries as most were unfamiliar with foreign

passports and the quality of the forgeries made them difficult to detect by a lay person.

**Example: Japan**

A number of fictitious bank accounts were opened by using false identification documents. Additionally, there were several cases where accounts were opened legitimately then granted or sold to a third party. It is highly likely that these accounts were used for concealing profits obtained from illegal loan sharking, Internet scams or other criminal activities.

Due to the prevalence in the use of false identities in fraud and money laundering, some jurisdictions in the APG region are either running or are implementing identity theft/fraud projects.

***Use of professional services (lawyers, accountants, brokers etc.)***

There were few jurisdictions that noted this method for the period.

As various jurisdictions in the APG region create more robust AML regimes, launderers may start to utilise the services of professionals such as lawyers, accountants and brokers. In the early stages of most AML regimes, considerable emphasis is placed on the mainstream banking sector as this is seen as the best sector to confront money laundering. As the banking sector becomes more robust, launderers require other avenues in which to introduce their proceeds of crime. Lawyers, accountants etc are seen as a viable avenue as they can not only act as a conduit to facilitate the placement stage, but can also assist in providing the tools to set up more sophisticated money laundering schemes or asset protection regimes (i.e., trusts, offshore accounts and entities).

**Example: Australia (*This case also provides a relevant study for the section on use of 'gambling activities' (page 11 of this report)*)**

This case involved the production of large quantities of amphetamines in several states of Australia. The suspects laundered most of the proceeds of the manufacture of the amphetamine with the assistance of several people in Australia. The Australian-based entities deposited cash supplied to them by the wife of the main suspect (usually in structured amounts) into their own accounts. The funds were drawn from the accounts using cheques payable to the suspect's wife or a company or business over which she and her husband had control. The Australian-based entities were also instructed to send some of the money to overseas accounts by international transfer. Money was often moved through different accounts, before being telegraphically transferred offshore. The case involved approximately AU\$5 million (US\$3.5 million).

Over AU\$1 million (US\$700,000) was also laundered by the group through an accountancy firm. The firm was initially approached on the basis that one of the suspects had substantial funds overseas, which he wished to repatriate to Australia. At the time, the suspect was a bankrupt and money could not be held in his own name. Advice was sought from the accountants to devise a structure to enable the repatriation of the funds and acquisition of real estate.

The accountants were given AU\$20,000 (US\$14,000) to be used as a deposit on a real estate purchase. The accountants were aware of reporting thresholds and deposited the money into bank accounts in amounts less than the AU\$10,000 (US\$7,000) reporting threshold. The accountants recommended a number of money laundering schemes to the principals of a drug ring. Their standard modus operandi was to launder the money into a number of bank accounts in amounts less than the reporting threshold of AU\$10,000 and to then draw cheques on those accounts.

The accountants used 15 different bank accounts to receive the cash. These included personal accounts, the bank accounts of other, unwitting family members, the accountants' business accounts (including trust accounts), and the bank accounts of corporate entities established for the purpose.

Two other methods used to launder the funds were use of bookmakers and gamblers.

In the case of the bookmakers, the modus operandi was to attend race days with substantial amounts of cash. The principal would seek out a bookmaker he knew, express his discomfort at carrying such a large amount in cash and ask them to hold his cash for him until he either used it for bets or collected it at the end of the day. He would then leave it with the bookmaker and deliberately not collect it at the end of the day. Early the following week he would contact the bookmaker and ask him to post him a cheque for the money.

The accountants had a business association with a wealthy businessman who was a frequent gambler at Australian casinos. The accountants approached the businessman and offered to provide cash at short notice to him or his associates for gambling at casinos. The accountants offered to accept 95% of the value of the cash they provided on the basis that the gambler later repaid the money by depositing money into a foreign bank account which had been set up for the purpose.

### ***Association with Corruption***

Refer to Section IV of this report.

### **Uncommon Methods**

The following methods were either not commonly found in the period reported on, or not reported as being used at all. However, these methods still warrant mention and consideration within this section.

#### ***Commodity exchanges***

Only one report noted this method. Palau reported that a current investigation had revealed that locally grown cannabis crops were being exchanged for crystal methamphetamine, which is mostly produced outside that jurisdiction.

#### ***Investment in Capital Markets***

This method was not commonly found within the region over the time period covered by this Report. Where the use of capital markets was found, the offending related to the perpetuation of fraud and not used in the laundering process.

#### ***Use of shell companies/corporations***

This method was not commonly found within the region over the time period covered by this Report. No specific cases were received.

### ***Use of offshore banks and corporations***

No reports were received of this method being used in the period covered by this Report.

### ***Use of informal financing networks (“Hui”, “arisen” etc.)***

This method was not commonly found within the region over the time period covered by this Report. No specific cases were received.

### ***Use of the Internet***

The use of the Internet was only mentioned in the reports in respect of fraud or advance fee scams, not to assist in the laundering process.

### ***Use of violence/coercion***

The use of violence or coercion to facilitate unwilling third parties to engage in money laundering was not reported as occurring within the APG region.

### ***Criminal knowledge of and response to law enforcement/regulations***

No specific cases were reported, however, two jurisdictions commented that organised criminals are continually evolving their techniques to avoid being detected. In order to do so, they gather information on law enforcement techniques, knowledge of relevant legislation and loopholes that might be exploited, for example, structuring transactions to avoid transaction reporting regimes or verification of identity, or concealing valuable assets and proceeds of crime to avoid confiscation.

### ***Further methods or techniques***

Some reports listed methods not mentioned in the outline given by the Secretariat. One of these methods is incorrect invoicing in international trade. Some of the cases given were related to the misuse of schemes set up by governments to promote the import and/or export of certain goods and services, which constitute more or less fraud cases rather than the laundering of funds from predicate offending.

## **Trends**

APG jurisdictions were also asked to provide information on general or continuing tendencies or patterns relating to specific methods of money laundering. Initially, jurisdictions were asked to report particularly on patterns of association of types of money laundering with certain predicate criminal activities. If the illegal proceeds from gambling, for example, are typically invested in other assets or are transferred abroad, is this done via wire transfers or by cash couriers? The jurisdictions were further asked to report on the frequency of, or the increase in, particular laundering methods.

Few reports detailed the correlation between specific predicate crimes and laundering methods unique to those kinds of crime. The few cases that did address the issue, at least in part, cannot be generalised. There were comments

that structuring was observed in connection with the sex/slavery trade, that foreign accounts were used in cases of tax evasion/fraud and identity fraud is mainly used for the misuse of card and payment systems. However, these observations were generally not commonly shared by all jurisdictions. It is considered that this issue should remain on the agenda for the Typology Working Group.

In order to establish a trend, data gathered over at least two or more periods of time is required. As this is the first time that data has been collected in specific categories, it is very difficult to analyse specific trends. However, the general trends arising in the Asia/Pacific region include the structuring of transactions, the use of false identities, co-mingling of legal and illegal funds, the use of gambling activities and the uses of nominees, trusts, family members and third parties.

### **Counter measures**

APG jurisdictions were asked to provide information on significant legislative, regulatory or law enforcement responses taken by their jurisdiction to address special money laundering methods or trends.

Only a few jurisdictions noted specific counter measures for single methods or trends, such as establishing up a special law enforcement division for gambling-related crimes. The vast majority of jurisdictions submitted more generalised reports on overall legislative or regulatory measures undertaken recently to meet international requirements, or to follow best practices.

The answers provided evidence of the different stages of AML regime each jurisdiction are presently at. Almost all are currently improving their AML regime. Those jurisdictions without appropriate legislation are either outlining drafts, are in the process of passing new legislation through parliament, or drafting new laws or amending existing ones to cope with the latest developments.

Some jurisdictions noted they were expanding their list of predicate crimes, changing the definition of money laundering, adding new sectors to include jewellery stores, lawyers, auditors, etc., increasing penalties and fines or trying to make forfeitures easier. Others noted establishing new cash transactions reporting systems, amendment to existing ones and the introduction of electronic reporting systems in some jurisdictions

Many jurisdictions reported recently establishing or are in the process of establishing, an FIU. Often the administrative capacities had been improved by increasing the workforce or restructuring organisations. Some countries combined the strength of different agencies to form task forces, sometimes including members of the banking industry. Other jurisdictions set up new databases, issued updated manuals/guidelines or carried out various awareness raising and outreach activities.

Since the initiatives above are relatively recent, their results were unable to be clearly identified in the reports. It will take some time until jurisdictions can evaluate if such initiatives have produced the desired results.

Jurisdictions did not provide or comment on the total number of cases directly derived from suspicious or unusual transaction reports, but did highlight some cases they deemed typical or interesting to share. It appears the vast majority of cases were developed from STRs.

Three jurisdictions reported research or studies undertaken on money laundering methods and trends. One jurisdiction is currently looking into the extent of money laundering in their country; another is studying the issue of cross border cash couriers while the one is undertaking a project to diagnose the causes of corruption to identify remedial measures.

The statistical data provided in the reports for the of number suspicious or unusual transaction reports, the number of investigations and prosecutions and seizures/confiscations is insufficient to make robust analysis or conclusions. Approximately half of the reports contained statistical figures, however, they cover different periods of time from a few months to many years. An increase in STRs can be due to a number of reasons: new legislation, improved investigation tools, additional outreach activities, better compliance by banks or even increased activities of money launderers.

There does, however, appear to be a steady increase over recent years, in all the categories mentioned in the above paragraph. Some jurisdictional reports even show a dramatic increase. The ratios given on the number of STRs that lead to investigations, the number of investigations that result in prosecutions and the number of cases that culminate in seizure or confiscation of assets vary substantially. On average about 3%, but in some countries up to 25% and in one case, even 100% of the STRs lead to investigations. About one out of five investigations lead to prosecution, and the total volumes of assets seized/confiscated measured in millions of US dollars. Further analysis should be carried out to learn more from the successful jurisdictions, however, this would require disclose of necessary detailed information.

## **Co-operation**

Almost every jurisdiction emphasised the importance of international co-operation (i.e., administrative, law enforcement and judicial co-operation) and outlined their efforts to improve this. International co-operation is often achieved by establishing an FIU, attaining membership to the Egmont Group of FIU and entering into memoranda of understanding for intelligence sharing with other FIUs. But there are also many other ways reported in which jurisdictions can co-operate with each other, including informal contacts established at seminars/workshops, improving working relations with neighbouring countries to formal agreements, both on a bilateral as well as on a multilateral basis. One important form of co-operation is

the provision of technical assistance. There are some cases reported where member/observer jurisdictions are assisting each other, but much of their technical assistance is provided by sources outside the region, such as the IMF, World Bank etc.

Information exchange between jurisdictions seems to be increasing significantly since many countries have put necessary legislation in place and have, or are establishing avenue to assist requests from abroad. Information exchange ranges from extradition requests to requests for legal assistance. While the vast majority of jurisdictions recognise the advancements already made or planned for the near future, a few criticise the reluctance of some countries to share information.

Few jurisdictions reported in detail any impediments/difficulties they faced in their efforts to strengthen international co-operation. Some, however, cite the lack of the necessary resources. The main hurdles reported concerned the special confidentiality and retroactivity provisions demanded by their counterparts.

## **Conclusion**

Analysis of the reports submitted, identified there is neither a dominant single method to launder money nor a method unique to the Asia/Pacific region. Almost all these methods known to and outlined by the Secretariat occurred in the region. The cases reported are generally quite complex and include a variety of methods, which are sometimes hard to detect.

There also seems to be no strong correlation between the methods used and specific predicate crimes. The reporting of widespread use of false identifiers and the observance that many cases were detected because of unusual transactional behaviour of customers highlights that effective customer identification procedures, are effective AML measures. There were some methods reported which should be considered more closely, for example the consequences of false invoicing as well as gambling related issues.

The data provided on trends did not reveal anything new or unique. Based on jurisdictions' findings, however, the use of false identifiers, the operation of fraudulent investment schemes, the use of the Internet and the misuse of other technical advancements, mainly by alternative remittance systems, are increasing.

The countermeasures undertaken by the various members/observers to combat money laundering appear to depend on the status of the AML regime in each jurisdiction. While some countries concentrated on drafting or introducing necessary legislation, others amended already long established AML statutes to remain in line with international standards. Many countries also improved their administrative capacities, including efforts to establish an FIU. Various awareness raising and outreach activities were also reported, depending on the resources available to the relevant authorities.

The statistical data provided indicates a steady increase over recent years in the number of STRs received, number of those STRs which lead to investigations, number of investigations which resulted in prosecutions, and the number of cases where assets had been seized or confiscated.

Almost every APG jurisdiction acknowledged the importance of international co-operation and have worked on the necessary legislation and resources to comply with the increasing number of international requests to share information or for assistance. Most countries seem to be satisfied with the extent of co-operation achieved, but there are also countries that criticise the reluctance of some jurisdictions to share the requested information with them.

## SECTION II

### Terrorist Financing Issues

#### Abuse of Wire Transfers

Many electronic financial transactions that are conducted by financial institutions for the purpose of transferring value between persons or entities can be broadly defined as wire transfers. In the great majority of cases, this process is facilitated by domestic and international financial institutions, acting on instructions from the sending person or entity, where the sender instructs the institution to make funds available to a recipient. In some cases, the sender and recipient are one and the same.

Wire transfers have long been regarded as one of the more popular and convenient means of transferring money across international boundaries. The speed it is accomplished makes it an ideal mechanism. The global Society for Worldwide Interbank Financial Communications (SWIFT) accounts for the great majority of traffic in terms of instructions for international wire transfers.

The sheer volume of wire transfers globally raises the possibility of criminals and terrorist groups hiding their transactions within the large number of wire transfers that occur on a daily basis. The speed and efficiency with which funds can be moved between jurisdictions appeals to criminal groups and financiers of terrorism. These issues present significant challenges to international law enforcement in its capacity following the money trail, freezing and seizing illegally acquired funds or funds intended to be used in the financing of terrorist activity.

Although misuse of wire transfers are just one stage in possible money laundering or terrorist financing processes, the analysis of wire transfers can potentially identify links between previously unknown associates, organisations and countries. It can also assist in establishing links between known terrorist organisations and individuals. While both forms of analysis may often appear to be 'needle in a haystack' exercises, there are encouraging signs that technology-assisted analysis is increasingly providing solutions for law enforcement and security agencies around the world.

Recent advances in payment systems provide greater security of transactions by enabling traceability through automatically generated electronic records. However, the lack of consistent approaches in the recording of transactional details relevant to wire transfers make them a popular avenue for moving illicit funds.

Once funds move across international borders the money trail becomes difficult to follow. It is well known that countries with limited government supervision, particularly in the banking sector, are known havens for terrorist groups seeking to escape detection. As terrorist groups are motivated by ideology not profit,

systems such as Western Union, despite their high transaction fees, have gained popularity because of the convenience with which funds can be transferred and collected worldwide.

Services offered by remittance dealers and underground banking systems are also popular among the criminal element as the anonymity offered suits those who want to remain anonymous or escape scrutiny.

A further complication relevant to terrorist financing within the financial system is the irregular and often small size (relatively low values) of each wire transfer. This makes it even harder to distinguish terrorist financing from legitimate funds transfers, as well as challenging established profiling techniques that have over the years been used to detect and monitor traditional money laundering activity. Nevertheless, there is some evidence that 'structured' wire transfers are being used by financiers of terrorism.

### **Methods and Trends**

Recent information suggests that the following methods are increasingly being used to disguise owner, beneficiary and other information relevant to the wire transfer of funds:

- Use of third parties to open accounts solely to receive funds from overseas and subsequent remittance to other overseas accounts.
- Non-residents opening accounts and then operating the accounts through remote banking service e.g. telephone banking to receive and remit funds through wire transfers.
- Cash being deposited into accounts belonging to associates in structured amounts. Money then being moved through different accounts before being electronically transferred overseas.
- Money being laundered with the assistance of an accountancy firm. Funds being transferred into personal, company, trust accounts etc. before being used to convert into assets.
- Structuring transactions to avoid significant cash transaction reporting requirements, particularly in conjunction with transfers of funds to known drug source countries.
- Operating a money laundering cell where frontmen remit structured amounts of monies back using false identities. Others being recruited to open accounts in false names to receive the remittances and then withdraw the funds in cash to break the money trail. The money laundering cells charge a fee to crime syndicates and other organisations

## Case Studies

### Case Study 1

After a tip received by law enforcement, an investigation was conducted into an 'illegal money transmitting business' or 'hawala'. Based on the financial evidence, simultaneous search warrants were executed at three of their business premises.

Analysis of the documents seized showed that the business had wired over four million dollars to Jordan, Syria, Iran, Saudi Arabia, Chile and Ukraine. The scheme involved a conspiracy to deposit money from expatriate Iraqis living in the United States into the subject's account and then wire the money to Jordan. The funds were then primarily illegally smuggled into Iraq in violation of the embargo order and provided to the designated beneficiary.

### Case Study 2

In September 2003, the owner of a Washington-based money transfer service, sent more than \$12 million dollars to Iraq in violation of the Iraqi Sanctions Act.

Investigations revealed that in 1996 the subject initiated money laundering operations to facilitate worldwide purchase of various commodities. An illegal money transfer business started by the suspect in 1998 utilised over 30 domestic agents throughout the United States. Over a twenty month period, in excess of \$28 million was collected and wire transferred to Iraq through Jordan and various other Middle Eastern countries. The target receiving money in the Middle East utilised these funds to purchase commodities from businesses worldwide.

### Case Study 3

A money service business received cash deposits from both sympathisers to a terrorist cause as well as drug dealers (often terrorist groups use the same channels as drug dealers to remit funds as they are secure, tried and tested. Also many terrorist organisations use drug dealing to finance their activities). The cash was collated and either sold to a wholesale bank note dealer or paid into a bank account and the proceeds wired to the beneficiary who would work for a front company or use false identification to collect the funds.

### Case Study 4

A well-known "pillar of society" in an ethnic community would collect cash from family and acquaintances and then pay it into his bank account. He would later draw cheques on his account and pay them to a foreign exchange bureau in order that an electronic wire transfer to the home country would be arranged. Most of the money would go to the relatives of the remitters, although some would be skimmed off for the 'liberation' struggle.

## Policy Implications

Consistent with the recently revised FATF 40 Recommendations, and in particular the need for increased customer due diligence by financial institutions, it is suggested that financial institutions should carry out some form of account monitoring. This especially applies to wire transfers so institutions will gain a better understanding of their customers' normal patterns of transactional activity. If suspicions are raised due to lack of a legitimate business purpose or unusual

patterns, a suspect activity report should immediately be submitted to the FIU. Monitoring processes should include automated processes that review transaction amounts, business types and geographic locations.

With respect to FATF Special Recommendation Seven<sup>3</sup>, it is also suggested that, meaningful information is obtained on the 'originator' of the wire transfer. A primary identity could aid law enforcement authorities in their analytical and investigative processes. This information would also enable the recipient financial institutions to make initial assessments of potential criminal or terrorist connections and further facilitate reporting to the FIU.

Investigations into terrorist financing continue to be frustrated by wire transfers through jurisdictions that either do not demand or enforce transparency of these financial transactions nor do they have efficient information sharing mechanisms in place to communicate such information to law enforcement authorities from other countries.

In these cases, it is suggested that banks could have a threshold of monitoring funds transfers and keep records of the transactions and supporting documents that could be produced as and when required by law enforcement or for on-site inspections by the domestic AML/CFT regulator.

Efforts should also be made to encourage transparency reporting and international sharing of information to address the problems of abuse of wire transfers by terrorist groups.

### **The Financial Action Task Force and the relation between wire transfers and terrorist financing**

During 2003, the FATF focused on the misuse of wire transfers for terrorist financing as part of the FATF 2003 Typologies Meeting. APG members and the APG Secretariat contributed to that meeting. Arising from that meeting, the following policy implications related to wire transfers were highlighted by the FATF in their FATF-XV Typologies Report<sup>4</sup>:

- The inclusion and retention of meaningful originator information on a wire transfer can assist the fight against terrorist financing and money laundering in several ways:
- Transactions that contain full information assist beneficiary financial institutions to identify potentially suspicious transactions. (These would require extra diligence and potential onward reporting to an FIU);
- When reports on unusual or suspicious wire transfers are received by an FIU, those that contain complete information can be more thoroughly researched and analysed; and

---

<sup>3</sup> [http://www.fatf-gafi.org/TFInterpnotes\\_en.htm#Special%20Recommendation%20VII](http://www.fatf-gafi.org/TFInterpnotes_en.htm#Special%20Recommendation%20VII)

<sup>4</sup> See [http://www.fatf-gafi.org/pdf/TY2004\\_en.PDF](http://www.fatf-gafi.org/pdf/TY2004_en.PDF)

- Ensuring that originator information is readily available assists the appropriate law enforcement authorities to detect, investigate and prosecute terrorists or other criminals.
- Having “complete and meaningful” information on the originator of a wire transfer message available to financial institutions and competent authorities is critical to being able to detect or prevent terrorist and criminal use of the wire transfers.
- The consensus of FATF experts at the Meeting was that the existence of a threshold for SR VII requirements – from an operational perspective – could hinder the detection of what might be relevant transactions (falling below the US\$3000 de minimis threshold). It was also noted that the lack of a threshold could also serve as a deterrent to the use of wire transfers by terrorists or criminals by making the risk of detection greater.
- The FATF experts also acknowledged, however, that in the absence of other specific indicators, the lack of a threshold could lead to an excessive number of transactions being reported to the FIU.
- A potential solution for finding additional indicators would be to encourage the development of information technology systems that could look for objective indicators within wire transfers.

## **Abuse of Non-Profit Organisations (NPOs)**

### **Nature of the Problem**

A non-profit organisation (NPO) is an organisation that exists for educational or charitable reasons, and from which shareholders or trustees do not benefit financially. NPOs play a vital role in the community. These organisations complement the activity of governments and business sectors in supplying a broad spectrum of public services and improving quality of life.

NPOs can take on a variety of forms, depending on their resident jurisdiction and legal systems. Within Asia/Pacific region, law and practice recognise various forms of NPOs including non-profit associations, informal financing networks, non-governmental organisations (NGOs) and charitable organisations.

Basically, NPOs aim to provide help for the needy or to support particular social groups or causes (religious, social or cultural). Trust and goodwill are key factors in the work of NPOs. Donations and contributions to NPOs often reflect the community's trust and goodwill for the work and services many NPOs undertake. However, the misuse of NPOs for the financing of terrorism is becoming recognised as a crucial point in the global struggle to stop such funding as its source. This issue has captured the attention of the APG as well as international organisations and national authorities.

Moreover, in the context of work on more targeted typologies, this Section focuses mainly on NPO issues that are still not well understood, such as current trends and methods for the abuse of NPOs.

### **Characteristics of NPOs**

The common and broad definition of NPO is a tax-exempt organisation that serves the public interest. In general, the purpose of this type of organisation must be charitable, educational, scientific, religious or literary. Legally, an NPO is one that does not declare a profit and instead utilises all revenue available after normal operating expenses, in service to the public interest.

These organisations can be unincorporated or incorporated. An unincorporated NPO can not be given federal tax-exempt status. When an NPO is incorporated, it shares many traits with “for-profit” corporations except there are no shareholders.

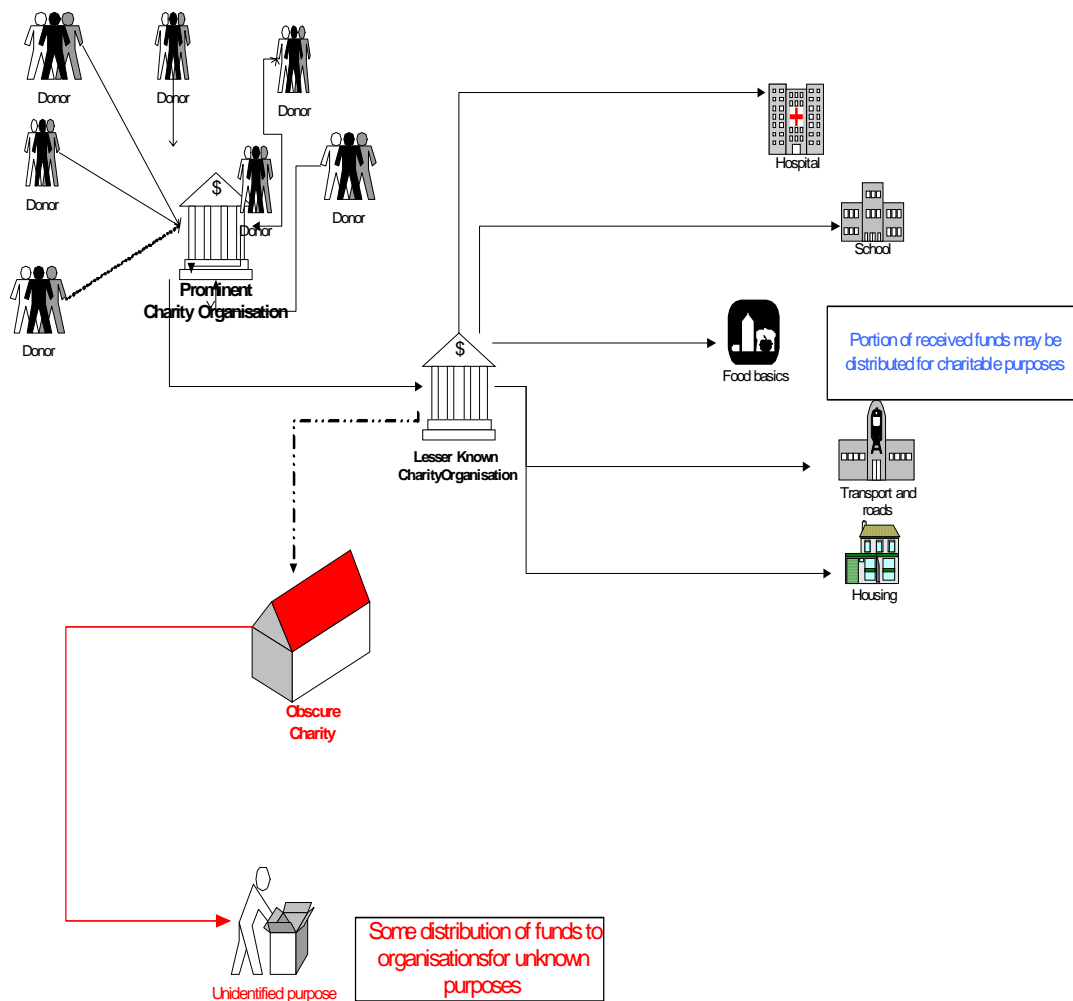
There are a variety of legal forms an organisation can take, including a partnership, association, trust or corporation; however, the most popular form of non-profit organisation by far is a corporation. In a few jurisdictions, it is common for NPOs to be organised as legal trusts or unincorporated associations.

### **Methods and Trends**

NPOs can play an important role in providing services to people in need. However, these organisations have been shown, in a number of cases to have been abused by those involved in terrorism and other illegal activities due to a lack of accountability by the organisations. In many countries NPOs are poorly covered by regulation and are not required to be registered. They are also not required to report to the government about the level of cash going into or out of the organisation.

The result is that the level of understanding about the cash flow of these organisations is limited. The following should provide a rough guide of the type of activity that can occur, resulting in fund flows from legitimate donors to unidentified purposes.

The flow chart below demonstrates possible fund flows through NPOs.



- The process begins with people from across the world donating funds to charity organisations (domestic or international donations).
- These organisations are able to collect large amounts of funding because they are well recognised, their work or function is trusted which garners the goodwill of many in the community.
- NPOs, in particular charities, may have elaborate and often layered structures to effectively undertake their fundraising and charitable works. While this may be an efficient and effective way to achieve their objectives, it does provide further opportunities for abuse by terrorist financiers
- Sometimes these organisations may directly supply funding to particular projects, but often they will pass on the funding to lesser-known charity organisations. This approach enables the prominent charity organisations to focus on the collection of funds, leaving the lesser-known NPOs to focus on the expenditure of the funds.

- The lesser-known charities often focus on the distribution of the funds. They will establish projects, such as the provision of hospitals, schools, food and health supplies, housing and transport and roads. It is expected that a large proportion of the funds is spent on these projects in order to maintain a good public profile. The remaining funds may then be sent on to more obscure charities to support other projects.
- The more obscure charities will spend some of the funding they receive on organised projects that are in the public arena. The remaining funds go to unidentified purposes. Due to the lack of reporting requirements, a charity or NPO can spend the funding in ways that are virtually untraceable by authorities.

The actual level of funding being spent on unidentified purposes is difficult to predict. In Australia, where the majority of NPOs are registered for tax purposes 51% of funding is goes towards the compensation of employees and 35% is spent on the purchase of goods and services<sup>5</sup>. This shows that in Australia at least 86% of funding by NPOs is being distributed directly to projects and administration of projects that can be directly assessed in the public domain.

Although analysis of the 2003 jurisdictional reports found no specific trend or preferred method of abuse of NPOs for terrorist financing, wire transfers and alternative remittance services are a popular method of transferring money across and within national boundaries. Such mechanisms are the most likely vehicles for moving funds that could be potentially linked to terrorist financing. There are several wire transfer trends seen in terrorist financing investigations, including:

- using “nominees” to provide clean names to terrorist financing transactions or accounts
- using front companies
- using multiple financial institutions; and
- avoiding mainstream financial institutions, through the use of licensed money remitters, thereby avoiding or reducing the risk of reporting.

Law enforcement and intelligence agencies have been receiving unverified reports that many organisations under investigation are using larger amounts of cash to minimise financial paper trails. The nature of NPO operations and alternative remittance systems may offer a good combination of services that can be abused by terrorist groups.

### **Policy Implications**

Clearly there are weaknesses in regulation and supervision of NPOs that can be exploited by terrorist groups. Compulsory registration and continuous monitoring

---

<sup>5</sup> Australian Bureau of Statistics Catalogue Number 5256.0 Australian National Accounts: Non-Profit Institutions Satellite Account 1999-2000.

of these NPOs would make their activities and funding more traceable and identifiable. In the current environment, it is possible that donors are unwittingly giving money to NPOs for unknown purposes that are possibly unacceptable to the donor. Increased reporting would assist in ensuring that NPOs use the funding in an acceptable manner to maintain the level of funding by donors. It would also be easier for authorities to trace funds that are being used for illegal activities.

Generally, funds destined for the financing of terrorism are taken from the “grass roots” donor collection level in prominent non-governmental organisations and charities. These funds are managed by terrorist supporters, often occupying a small number of key positions in the organisation, such as its president or treasurer. The funds are then distributed through sometimes complex layering schemes that can involve a number of other lesser known non-governmental organisations, charities, individuals, as well as commercial entities. These layering processes are international.

NPO funds often transit through a number of different countries or jurisdictions before arriving at the intended destination. While these funds are in transit, they may be split into smaller sums for diversion to multiple locations or conversely commingled with other incoming sums to form larger amounts from different sources. Funds are distributed to humanitarian relief projects throughout the world, such as foodstuff packages, hospitals or health care aid, education facilities, immigration assistance, etc. However, some funds are distributed to other NPOs for unknown purposes, therefore it is difficult to ascertain where the funds were spent. This is clearly a risk for possible terrorist financing.

The methods of exploiting NPOs of terrorist financing vary from case to case. Various methods of layering and disguising funds can be used simultaneously to avoid detection. Through financial intelligence, the collection of money transfers could provide a money trail of NPO financing. This would aid in establishing the relationship between the persons or entities on either side of the transaction. It may also provide possible indicators of where individuals may fit within the structure of a terrorist group.

## Case Studies

Following are some cases relating to the abuse of NPOs from the 2003/2004 APG jurisdictional reports.

**Example: United States of America**

**Benevolence International Foundation, Inc. (BIF)**

BIF is a U.S.-based, tax-exempt charitable organisation whose stated purpose is to conduct humanitarian relief projects throughout the world. BIF was incorporated in the State of Illinois on 30 March 1992. Although BIF is incorporated in the United States, it has operated around the world, in Bosnia, Chechnya, Pakistan, China, Ingushetia, Russia, and other nations. BIF has operated as Benevolence International Fund in Canada and as Bosanska Idealna Futura in Bosnia.

On 14 December 2001, the FBI seized financial and business records from BIF's Illinois office. The FBI also searched the home of Enaam Arnaout, BIF's Chief Executive Officer and a member of the Board of Directors, and seized certain effects. On the same date, the United States issued an order blocking BIF's assets and records pending further investigation. On 18 October 2002, the United States designated BIF under Executive Order 13224 for its support of the al Qaida terrorist organisation. On 10 February 2003, the United States convicted Arnaout of fraud and racketeering. He was sentenced to 11 years and 4 months in prison for diverting more than US\$315,000 of charitable donations to terrorist organisations. Prior to these actions, BIF had consistently supported al Qaida and other terrorist organisations, both directly and through its leadership and precursor organisation, Lajnat Al-Birr Al-Islamiah (LBI).

In 1987, a wealthy associate of designated terrorist Usama bin Laden, founded the precursor organisation to BIF, LBI, which translated from Arabic means "Islamic Benevolence Committee." The purpose of this organisation, at least in part, was to raise funds for the Mujahideen, then fighting in Afghanistan, and the organisation also provided cover and immigration assistance to fighters travelling in and out of Pakistan.

In the early 1990s, in an effort to attract more donations and deflect scrutiny from LBI, LBI's founder created and incorporated Benevolence International Foundation ("Al Bir Al Dawalia" in Arabic) in the United States. Under its new name of Al Bir Al Dawalia, the organisation engaged in financial transactions on behalf of al Qaida. When a foreign government began to scrutinise BIF's operations in or around 1993, the founder of LBI and BIF resigned as director of BIF and Arnaout assumed control of the organisation. Although the founder of LBI and BIF was removed from BIF's public filings by 1995, he maintained an influential role in the organisation.

Substantial evidence documents the close relationship between Arnaout and Usama bin Laden, dating from the mid-1980s. An article in the Arab News from 1988, reporting on bin Laden's activities at the "al Masada" mujahideen camp in Afghanistan, included a photograph of Arnaout and bin Laden walking together. In a March 2002 search of BIF's offices, Bosnian law enforcement authorities discovered a host of evidence linking Arnaout to bin Laden and al Qaida. Among the files were scanned letters between Arnaout and bin Laden, under their aliases. In one handwritten letter, bin Laden indicates that Arnaout is authorised to sign on bin Laden's behalf. Various documents also established that Arnaout worked with others - including members of al Qaida - to purchase rockets, mortars, rifles, and offensive and defensive bombs, and to distribute them to various mujahideen camps, including camps operated by al Qaida.

BIF has provided additional support for and has been linked in other ways to al Qaida and its operatives. First, BIF lent direct logistical support in 1998 to Mamdouh Mahmud Salim, a bin Laden lieutenant present at the founding of al Qaida. Salim was indicted for conspiring to kill U.S. nationals. Testimony at the 2001 trial of *United States v. Bin Laden*, et al, implicated Salim in efforts to develop chemical weapons on behalf of al Qaida in the 1990s.

As early as 1992, Salim and bin Laden made efforts to develop conventional weapons and to obtain nuclear weapons components. BIF is also linked to Mohamed Loay Bayazid, who was implicated in a U.S. embassy bombings trial for his efforts, approved by Salim, to obtain weapons components on behalf of bin Laden in 1993-1994. Bayazid's driver's license application, dated 12 September 1994, identifies his address as the address of BIF's Illinois office. In the late 1990s, Saif al Islam el Masry, a member of al Qaida's majlis al shura (consultation council), served as an officer in BIF's Chechnya office.

**Example: United States of America**

**Palestinian Islamic Jihad (PIJ); Sami Al-Arian and Associates**

The FBI-Tampa office initiated a long-term investigation against Sami Al-Arian and other members of the Palestinian Islamic Jihad (PIJ). PIJ was declared a "specially designated Terrorist Organisation" by the United States in January 1995. The investigation focused on Al-Arian and his associates' financial support of the PIJ from U.S.-based fundraising events during 1988 through 2002. In addition, the investigation sought to establish their culpability for the over 100 murders (including two U.S. citizens) conducted by this terrorist organisation through violent acts in the Middle East.

The FBI's financial analysis of over 90 bank accounts held by Al-Arian and associates, evidence obtained via subpoena, search warrants, intelligence techniques and through witness interviews, pinpointed the US-based funding mechanisms used by the PIJ to support the organisation and its terrorist activities as follows:

PIJ financed the organisation by obtaining funding from state sponsors (Iran, Sudan, Syria, Lybia) through Iranian Embassy channels in Damascus, Syria. The money was then sent to the Occupied Territories by couriers. Funds were also sent to "straw" accounts set up in Arab Bank branches in the Occupied Territories. In addition, money was raised in the U.S. through mosques and front companies controlled by PIJ operatives including ICP, WISE, and IAF. The collected funds were then sent to the Middle East through straw accounts and money hangers. The funds were then wire transferred from the PIJ leadership in Lebanon to operatives in the Occupied Territories. The investigation also revealed that money was sent from U.S.-based PIJ members to accounts of PIJ family members of "martyrs" in the Middle East.

On 19 February 2003, a Federal Grand Jury in the Middle District of Florida indicted Al-Arian and seven co-defendants for alleged violations of the RICO Act and providing material support to a terrorist organisation, among other violations.

On 20 February 2003, the FBI in Tampa, Florida and Chicago, Illinois arrested Sami Al-Arian, Hatem Fariz, Sameeh Hammoudeh and Ghassan Ballout. In addition to the arrests, the FBI executed seven search warrants on the residences and businesses of Al-Arian and his associates. The remaining four defendants are currently fugitives in Syria, Lebanon, Gaza Strip and the United Kingdom.

A trial date of January 2005 has been set for this case in Tampa, Florida. Al-Arian and Hammoudeh have been detained until the trial, while Fariz and Ballout were released after providing sizeable bonds.

**Example: United States of America**

**Money Transfer to Iraq Using a Non-Profit Organisation**

A Federal Grand Jury in Syracuse, New York, indicted Rafil Dhafir and others as part of a conspiracy to transfer money to Iraq through an NPO. Rafil Dhafir, Maher Zagha, Ayman Jarwan, and Osameh Al Wahaidy were indicted on 26 February 2003, for their role in conspiring to transfer funds to Iraq in violation of the International Emergency Economic Powers Act. The indictment alleges that from approximately 1994 to February of 2003, the defendants conspired to violate Executive Orders and Treasury Department regulations by transferring funds and other economic resources to Iraq.

The indictment further alleges that the defendants operated an NPO called 'Help the Needy', and solicited contributions from people in the U.S. The money received as donations was deposited to New York banks, and then laundered through bank accounts at the Jordan Islamic Bank in Amman, Jordan. The indictment alleges that the defendants conspired to funnel over US\$2.7 million through the Jordan Islamic Bank, and that Dhafir directed cheques as large as US\$100,000 to individuals located in Baghdad.

**Example: United States of America**

**Holy Land Foundation for Relief and Development**

Holy Land Foundation for Relief and Development (HLF) was established in 1989 as a U.S.-based, tax-exempt charitable organisation to solicit donations in aid of the Palestinian people in the West Bank and Gaza. HLF was originally known as the Occupied Land Fund (OLF) and was incorporated under that name in California in 1989 by three founders, all of whom continued to run the organisation until its designation in December 2001. In 1992, OLF relocated to Texas and registered as HLF. Although headquartered in Texas, HLF maintained branch offices and representatives scattered throughout the United States, the West Bank and Gaza.

On 4 December 2001 the United States designated HLF, the largest U.S.-based Islamic charity, under Executive Order 13224 for its role in supporting the HAMAS terrorist organisation. Prior to its designation, HLF raised millions of dollars for HAMAS, directing its funds to Islamic committees and other charitable organisations that are part of HAMAS or controlled by HAMAS members. In addition, the officers and directors of HLF are HAMAS members or have acted for or on behalf of HAMAS.

Some of the links to HAMAS include the fact that Mousa Abu Marzook, a known HAMAS political figure and former leader of the HAMAS security apparatus, donated US\$210,000 to the HLF in 1995. Marzook himself was designated as a terrorist by the United States in 1995, and deported. He is currently believed to be residing in Syria and to be actively involved in terrorist funding activities. In addition, other information linking HLF to HAMAS revealed that HAMAS leadership met with HLF executives to discuss the need for HAMAS fundraising functions to occur in the United States and the primary role HLF would hold in these activities. FBI investigations determined that a substantial amount of the funds raised by HLF were transferred to support HAMAS activities in the Middle East. HLF raised approximately US\$13 million dollars in contributions in 2000.

To date, some APG jurisdictions have no reported or suspected cases involving the abuse of NPOs for terrorist financing. However, they fully support measures to combat the threats posed by terrorism financing. They ensure that their financial system is not open to abuse by terrorists and not used as a conduit for terrorist financing. They have issued the law and regulation pursuant to the UNSCR 1333 and 1267 to freeze accounts belonging to terrorist organisations as well as to criminalise terrorism and terrorist financing.

**The Financial Action Task Force and the Abuse of NPOs**

On 11 October 2002 the FATF released the *International Best Practices on Combating the Abuse of Non-Profit Organisations*<sup>6</sup>. When combined with The Forty + 8 Recommendations on money laundering, this publication sets out the principles, guidelines and suggested practices that would best aid authorities to protect genuine NPOs. This includes NPOs that engage in raising or disbursing funds for charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of “good works” from being misused or exploited by the financiers of terrorism.

The publication focuses on three main areas of operation and oversight of NPOs:

- *financial transparency*: stresses the need for proper accounting practices, independent auditing of financial accounts, as well as the preferred use of bank accounts to channel funds;

<sup>6</sup> See [http://www.fatf-gafi.org/pdf/SR8-NPO\\_en.pdf](http://www.fatf-gafi.org/pdf/SR8-NPO_en.pdf)

- *programmatic verification*: mentions the need to provide accurate information to potential providers of funds, the need to verify that financed projects have actually been carried out, and that the funds were in fact received and used by their intended beneficiaries; and
- *administration*: stresses the need for NPOs to document their operations and to have boards of directors (or other forms of supervisory bodies) capable of proactive verification measures.

During 2003, the FATF focused on the abuse of NPOs as part of its 2003 Typologies Meeting, which included contributions by 8 APG members and the APG Secretariat. Arising from that meeting, the following policy implications related to NPOs were highlighted by the FATF in their FATF-XV Typologies Report<sup>7</sup>:

- Additional measures will likely need to be developed to reduce the vulnerabilities of NPO to misuse for terrorist financing purposes.
- There are significant differences in the NPO oversight and transparency regimes between jurisdictions. Some jurisdictions have done very little while others have implemented far-reaching regulatory systems requiring detailed record keeping and reporting, external auditors, licensing, the mandatory use of authorised bank accounts, permits for international transactions, and detailed customer due diligence requirements for banks (with regard to NPOs).
- Many countries have some kind of regulation and oversight of those NPOs that have been granted a full or partial tax-exempt status by fiscal authorities. In certain countries, these authorities may even play an important and active role in the oversight of such organisations.
- The prevention of criminal abuse of NPOs (money laundering and fraud) is another reason to increase regulatory oversight of the NPO sector
- Most countries can only dedicate a limited part of its resources to the regulation and oversight of the NPO sector, which in some cases consists of hundreds of thousands of organisations that handle a significant percentage of the GDP of a country. This is particularly the case in many developing countries, where NPOs play a particularly crucial role in the economy.
- In most countries, a large percentage (up to 90%) of the total number of NPOs consists of very small organisations. For these smaller NPOs, it can be difficult to carry a substantial administrative burden that would be required for complying with detailed government regulation. Even for larger organisations, there are limits to what can be considered a reasonable compliance burden, since the resources of NPOs are by their very nature scarce in relation to the often essential services they provide. Furthermore, some countries have certain legal or even constitutional provisions that prevent or limit the imposition of regulatory requirements on certain categories of NPOs.

<sup>7</sup> See [http://www.fatf-gafi.org/pdf/TY2004\\_en.PDF](http://www.fatf-gafi.org/pdf/TY2004_en.PDF)

## **Conclusion**

Although a variety of methods are used to finance terrorist organisations and activities, the most effective means of raising funds is through community solicitation and fundraisers, often in the name of a NPOs with charitable status. Terrorist supporters often occupy a small number of key positions in an NPO, such as its treasurer. These people can divert funds to terrorist causes for extended periods of time unknown to the broader membership and donors.

Furthermore, terrorist supporters transmit funds abroad by cabling funds to banks and individuals abroad, sometimes via an informal fund transfer system.

All jurisdictions should take proactive measures to decrease the risk of misuse of NPOs by terrorist supporters or terrorist groups by strengthening regulations and supervision of NPOs in compliance with international best practices.

With the growth of transactional crimes and emergence of new terrorist techniques, enhanced by the advent of new technology, continued international assistance is needed to increase closer co-operation and co-ordination networks and international information sharing in trailing how funds are raised, moved, and used by terrorist organisations.

## SECTION III

### Cash Courier Issues

#### Nature of the Problem

Reporting by intelligence and law enforcement indicates 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. Indeed, over many years, APG typologies exercises have repeatedly highlighted the key role that cash smuggling often plays in money laundering operations. *Cash smuggling* may include the use of couriers, of bulk cash movements or of informal money remitters.

These methods are distinct and should be differentiated. Bulk cash smuggling, for example, is generally associated with crimes that generate enormous profits such as drug trafficking, and involves containerised cargo shipments. Cash couriers can also involve large quantities of cash; however, the amounts smuggled are generally lower. The cash smuggling related to some informal money remitter operations is usually only one part of a larger money movement scheme. The APG has focused its work on the use of couriers. The APG agreed that law enforcement experts in the region should address this issue to provide a sound basis on which to combat this problem from an AML/CFT perspective.

Because many jurisdictions have introduced strict AML controls on the formal financial sector, organised crime and terrorist groups are increasingly reluctant to use regulated financial institutions to receive and transfer money. Instead, these groups are turning increasingly to services that operate outside the formal financial sector, such as couriers, to minimise the risk of detection by governmental authorities. Indeed, mounting evidence shows that the more effective that controls are within the formal payment system, the more criminals will tend to resort to moving cash. In addition, cash couriers are used in jurisdictions with less-established or unreliable financial sectors. Individuals using this method to move funds may prefer to remain anonymous and that the movement of funds remain unrecorded.

#### Methods and Trends

In cash smuggling operations, couriers will travel over roads, through airports or by sea with loads of cash, often stuffed in boxes, suitcases and concealed compartments in vehicles. Vast and porous borders within the region make the job of detecting couriers even more difficult. Couriers also use privately-owned boats and clandestine roads to smuggle money thereby circumventing the official border "check points".

The use of commercial airlines is also a preferred method used by cash couriers for the following reasons:

- The passenger (courier) can stay close to his money during transport,
- Many foreign destinations can be quickly reached;
- Little pre-planning is required.

Thailand estimates that over \$US70 million per year is smuggled out of Thailand via plane. Land border crossings also offer advantages to the courier such as a decreased customs presence at outbound checkpoints and that the courier often has a car in which to conceal the currency. The APG experts have identified the following key methods in trends in the region:

- the use of co-ordinated, multi-jurisdictional couriering syndicates
- common connections between cash couriers and trade-based money laundering
- major regional financial centres 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
- the use of cash couriers to support underground foreign exchange operations.

### Case Examples

#### Money Laundering

On 10 September 2003, Laura Camara was indicted in the Southern District of Texas for conspiring to transport U.S. currency from Houston, Texas, to Reynosa, Mexico. As part of the conspiracy, Laura Camara met with an unindicted co-conspirator in Reynosa, Mexico, to arrange for the transportation of U.S. currency. As part of the conspiracy, Camara picked up a Chevrolet van and drove it from Reynosa, Mexico, to Houston, Texas. While in Houston, Texas, Camara gave custody of the van to an unindicted co-conspirator. Camara received the van back on the next day, and drove the van southbound until police stopped her. Camara was indicted for one count of conspiracy to launder money for attempting to transport US\$919,882.00 from Houston, Texas, to Reynosa, Mexico.

As mentioned earlier, cash couriers have been detected as playing a significant role in the deployment and flow of the international financing of terrorism.

#### Terrorist Financing

The activities of Jemaah Islamiah (JI) in South east Asia clearly show the critical role of cash couriers in support of their terrorist operations. JI avoided using the conventional banking system for the reasons noted above. The funding for the Bali bombings that took place in October 2002 were provided by Al-Qaida's chief of operations to JI's head of operations (ie., Hambali), who was hiding in Thailand in 2002. Hambali passed US\$30,000 to the perpetrators of the Bali bombings in two batches using several cash couriers. The couriers took several weeks to complete the runs. The funding for the JW Marriott Hotel bombing in Jakarta was also provided by Hambali from Thailand. Again, a total of US \$30,000 of Al-Qaida's funds was sent to Indonesia in April 2003 through a string of couriers.

## **Policy Implications**

They key to detecting cash couriers relies almost exclusively on customs and border security officials. Because many Customs officials around the world lack the ability to detect cash or do not even think to look for it, specialised training and equipment are needed to detect cash both inbound and outbound. This is an area where the APG can work with relevant international bodies, such as the Oceania Customs Organisation (OCO). Specific technical assistance should be developed to increase the capacity to detect cash at the borders (e.g., airports, train and bus stations). For example, customs authorities should develop the use of canine units that are specially trained to “sniff out” currency. X-ray technology and other sophisticated equipment should also be employed when trying to detect cash. In addition, other law enforcement officers can be trained to carry out “consent” searches of carry-on luggage while conducting roving patrols at transportation depots such as airports, bus and train stations.

APG experts recognised the importance of international measures to combat this problem. Approximately one-half of APG members do not have any type of reporting requirement on the international transportation of currency. However, the majority of these jurisdictions recognise the threat and are considering adopting measures in the near future. Jurisdictions should consider adopting cross-border reporting requirements as suggested by FATF Recommendation 19(a). Jurisdictions should also consider making it a criminal offence to knowingly conceal, transport or transfer currency with the intent to evade reporting requirements. Universal reporting thresholds should be considered with the goal of creating a level playing field for all jurisdictions. However, adopting a universal threshold presents challenges due to the reliance on cash in some economies and varying economic conditions in the region.

The issue of domestic law enforcement co-operation was raised by APG experts. Effective linkages between Customs, Immigration and the police should be established to respond to currency detections and to develop intelligence. Countries should ensure that information gathered from cash seizures is shared domestically. Customs authorities should also share information with their Financial Intelligence Unit (FIU) and other law enforcement agencies.

International co-operation was also addressed. Co-operation arrangements between jurisdictions are essential to allow proper responses to cash courier investigations. The importance of expedient information sharing to detect cash couriers was highlighted. Jurisdictions could consider, for example, entering into bilateral customs-to-customs information exchanges on cross-border report and cash seizures.

## **Conclusion**

Effective linkages between Customs, Immigration and Police should be established to respond to currency detections and to develop intelligence. Countries should ensure that information gathered from cash seizures is shared

domestically. Customs authorities should also share information with their FIU and other law enforcement agencies.

Cooperation arrangements between jurisdictions are essential to allow proper responses to cash courier investigations. The importance of speedy information sharing to detect cash couriers was highlighted. Jurisdictions could consider, for example, entering into bilateral customs-to-customs information exchanges on cross-border report and cash seizures.

# SECTION IV

## Corruption Issues

### Introduction

This Section provides a broad outline of the situation with corruption-related money laundering issues in the Asia/Pacific region.

### The threat from corruption-related money laundering

Since commencing its typologies work in 1997, the APG has identified corruption as being a significant risk factor for money laundering and the financing of terrorism in the Asia/Pacific region. The APG has long recognised that corruption in the region provides an enormous source of illicit money to be laundered and that corrupt activities are often an essential element in facilitating money laundering and terrorism financing activities. It is also recognised that corruption related money laundering issues are transnational, and that laundering the proceeds of corruption often occurs between jurisdictions.

### Diversity across the region

The enormous diversity of jurisdictions across the Asia/Pacific region is reflected in the nature of the issues of corruption in the Asia/Pacific.

Unfortunately, some jurisdictions in the Asia/Pacific are characterised by endemic corruption, while others have robust anti-corruption systems and relatively low levels of corruption. The 2003 Transparency International Corruption Perceptions Index (CPI)<sup>8</sup>, for example, provides an indication of the perception of comparative risks of corruption among 133 countries. Globally, six APG jurisdictions are included in the twenty highest on the CPI (perceived to be least corrupt), while four APG jurisdictions are included in the bottom twenty lowest on the CPI.

The Asia/Pacific region includes jurisdictions that have been judged as amongst the least corrupt systems in the world, however, those same jurisdictions are known to be attractive to money launderers as a destination for illicit money, including the proceeds of corruption. This reflects their large financial sectors and the transnational nature of corruption and associated money laundering.

### Impacts of corruption and money laundering

Corruption and crime have empirically been shown to impair economic development. On the other hand, effective AML/CFT systems promote stable financial systems and lead to reductions in corruption and crime. Strong AML/CFT

---

<sup>8</sup> The 2003 Transparency International Corruption Perceptions Index (CPI) ranks 133 countries in terms of the degree to which corruption is perceived to exist among public officials and politicians. It is a composite index, drawing on 17 different polls and surveys from 13 independent institutions carried out among business people and country analysts, including surveys of residents, both local and expatriate. The CPI focuses on corruption in the public sector and defines corruption as the abuse of public office for private gain.

regulation and enforcement raises the costs of corrupt and criminal activities as well as those of money laundering.

Understanding the key sources of corruption-related money laundering should be a priority, as they vary from county to country. They include drug trafficking; arms trade; illicit political funding; budgetary corruption, tax evasion etc.

The profits from money laundering have considerable political and development costs for countries, through their relationship to legal, financial and political (such as campaign financing) structures.

The proceeds of public sector corruption and related money laundering have been associated with high public debt. Illicit and looted proceeds of corruption have been observed to be of a similar magnitude to the size of external debt of some countries. Most often, such large-scale plunder is moved to an external jurisdiction to avoid detection and forfeiture.

### **Recent developments in the global standards**

The UN Convention against Corruption was signed in November 2003 and represents, a major new standard in combating corruption. The UN Convention against Corruption outlines a range of measures to combat all aspects of corruption and seeks to combat corruption by taking action against the financial aspects of corruption including money laundering and the proceeds of corruption (financial intelligence, seizure, forfeiture etc.) In this respect, it promotes effective implementation of the global AML/CFT standards as an important pillar in the fight against corruption.

In the preamble to the UN Convention against Corruption (2004), the UN highlights:

- the seriousness of problems and threats posed by corruption
- the links between corruption and other forms of crime, in particular organised crime and economic crime, including money laundering
- that cases of corruption involve vast quantities of assets
- that corruption is no longer a local matter but a transnational phenomenon effecting all societies and economies
- that international cooperation to prevent and control corruption is essential
- that a comprehensive and multi-disciplinary approach is required to prevent and combat corruption effectively and
- the UN's determination to prevent, detect and deter in a more effective manner, international transfers of illicitly acquired assets and to strengthen international cooperation in asset recovery.

### **What the APG has done**

The 2001 APG Typologies Workshop observed that money laundering methods are similar for a range of profit-based crime, including drug trafficking, corruption and organised crime. It was noted that the objectives of the criminals are the same, namely to:

- disguise the illegal origin of the proceeds of crime (including corruption)
- utilise the proceeds of such crime without detection.

The APG commenced detailed typologies work on corruption-related money laundering issues in late 2003. This was in response to the nature of threats from and responses to corruption in the Asia/Pacific region, including significant connections between corruption and money laundering, the financing of terrorism and the growing global momentum to tackle the financial aspects of corruption.

### **Key findings from 2003 Typologies Workshop**

- A wide variety of forms of corruption produce illegal revenue whose origins/ownership are concealed through money laundering
- Corruption is used as a key step in money laundering activities to procure the assistance of public and private sector officials (including bankers, accountants, law enforcement / government officials) for the purposes of obscuring such activities and ensuring access to profits.

### **Prevalent methods**

The 2003 APG Typologies Workshop did not focus on the details of particular money laundering methods associated with proceeds of corruption. The Workshop reiterated the finding from the 2001 APG Typologies Workshop that money laundering methods observed for proceeds of drug trafficking, and various other organised crimes were equally prevalent for laundering the proceeds of corruption.

The following methods were, however, highlighted during the workshop:

- Mingling
- Layering
- Shell companies
- Purchasing valuable assets
- Use of family members' accounts
- Disguising bribes as 'consultancy fees'
- Cash couriers, for example, smuggling cash out of the jurisdiction to be integrated back into the formal financial sector in another jurisdiction and returned to the country via the financial sector. The prevalent use of cash in some jurisdictions was highlighted as a significant risk factor.

During the APG Workshop, members particularly highlighted that the involvement of financial institutions in corruption-related money laundering results in an increase in customers being defrauded by corrupt bank officials, widespread institutional corruption and ultimately institutional failure.

## Case Studies

### **Example: Chinese Taipei**

Mr Chang Lin is the person in charge of Kuang-hung Construction Co Ltd. In 1996, the company planned to build Tai-ma Spring Resort in Taitung County. For lack of adequate finance and failure business achievement, the company approached Legislator Wang Yung for assistance in taking a bank loan. The scheme of investment also aroused Legislator Wang's interest, and thus a consensus was reached. In the capacity of convenor of the Finance Committee of the Legislative Yuan, Legislator Wang managed by August 1997 to help Kuang-hung to take a syndicated loan of some NT\$3 billion (approximate US\$ 80,600,000) from four banks for construction of the spring resort. In return of the favour, Legislator Wang was promised a 10% commission of the financing in the form of shares in the spring resort.

When construction of the resort structure was approaching its final stage and internal decoration was about to begin, Legislator Wang asked Mr Chang Lin to fulfil his commitment. If the shares were directly registered under the name of Legislator Wang, it would leave evidence of bribery. So they organised a new company called Success Co composed of Legislator Wang's son, Mrs Wang and Legislator Wang's secretary along with few figureheads under the control of Mr Chang Lin. The new company has a registered capital of NT\$800 million (approximate US\$ 23,000,000), out of which Mrs Wang, Wang's son and Wang's secretary have NT\$360 million (approximate US\$ 10,300,000) worth of shares.

In order to go through the capital-verification process, Legislator Wang further arranged an unsecured loan of NT\$800 million from Ping-an Bank which chairman is Wang's friend. Since it was an open credit involving a huge amount, the bank believed the risk was too high and that it agreed that the loan could be made available only by earmarking. That is to say shareholders of Success Co open accounts with Ping-an Bank first and later the preparatory office of Success Co open an account with the bank while the bank takes custody all passbooks and seals of the company's shareholders. Once the NT\$800 million loan is appropriated into the shareholders' accounts, the funds will be transferred to the account of the preparatory office of Success Co.

The practice requires Kuang-hung or its selected companies to remit a certain amount of funds into the shareholders' accounts. By then an equal amount of funds from the account of the preparatory office of Success Co will be transferred to Kuang-hung related accounts to be used as payment by Success Co for purchase of shares of Tai-ma Spring Resort. In reality, however, funds for purchase of shares of Tai-ma Spring Resort have never been there and that the NT\$800 million loan has never left the bank. That was the way Legislator Wang relied to obtain NT\$360 million worth of shares of Tai-ma Spring Resort, another venue of money laundering.

The case in question reflects the focus the Republic of China works on anti-corruption cases. To enforce the government determination to eradicate 'black gold', or corrupt money, the case, after having been investigated by the MJIB, was prosecuted by the Prosecutor's Office of Taipei District Court at the end of June this year on charges of violation of Corruption Penal Statute and MLCA. The prosecutor sought 10 years imprisonment for the Legislator Wang.

(The individuals and companies mentioned in this case are all sanitized).

**Example: Hong Kong, China**

An executive of a Hong Kong representative office of a foreign bank accepted advantages (approx HK\$3.51 million) (US\$450,000) as a reward for assisting a non-Hong Kong company in obtaining loans / credit facilities amounting to approximately HK\$390 million (US\$50 million). The advantages to be paid to the banker were included in the consultancy fees paid by the borrower to a BVI company, controlled and operated by an accountant. The advantage to the banker was paid by the accountant to him partly in the form of cash (HK\$, GBP and US\$) and HK\$ cheques which were deposited in his own account. Advantages were also paid in the form of a GBP Demand draft issued in favour of a third person. This Demand draft was deposited in a United Kingdom bank account and proceeds remitted by wire transfer to Thailand where it was then withdrawn in cash.

This case illustrates the use of offshore shell companies, accountants, foreign bank accounts and the disguise of bribe payments in the form of consultancy fees.

**Example: Hong Kong, China**

A former vice president of a securities and investment firm solicited HK\$2 million (US\$256,000) from the director of an investment management company as a reward for introducing clients holding shares in a listed company to facilitate a takeover. It was the intention to receive the amount in an offshore BVI company, in the form of consultancy fees.

This case again illustrates the use of off shore companies and the disguise of advantages in the form of consultancy fees.

**Example: Hong Kong, China**

A former general manager and credit manager of a local bank were convicted for accepting cash of HK\$512,000 (US\$65,700) and two Rolex watches and cash of HK\$100,000 (US\$12,800) and one Rolex watch respectively in return for granting mortgage loans and L/C facilities. The L/Cs drawn on the facilities were not supported by genuine trade transactions.

This case illustrates the receiving of bribes in valuable assets (expensive watches).

**Example: Hong Kong, China**

A former senior freight officer of an airline company accepted HK\$340,000 (US\$43,600) in cash from a forwarder as a reward for reserving cargo space. The cash was deposited in accounts belonging to his family member.

This case illustrates the use of family members in the receipt of corrupt proceeds.

**Example: Hong Kong, China**

A senior manager of a local bank, three shareholders and two employees of a money changer company have been charged with conspiring with persons believed to be money couriers. They dealt with large sums of cash (HK\$50 billion) (US\$6.4 billion) knowing that the money in whole or part represented proceeds of an indictable offence. The money brought in by courier to Hong Kong was partly converted to other currencies and then deposited in various nominated accounts. The senior manager of the bank was also charged with accepting advantages (US\$20,000) in loans from a shareholder of the money-changer company. The senior manager conspired with another bank officer to record cash deposits in the account of the money-changer as transfer deposits, in order to circumvent suspicious transaction reports.

This case illustrates issues of currency smuggling, currency exchange layering.

### **Difficulties encountered in combating corruption-related money laundering**

Financial aspects of corruption may be particularly difficult to detect and investigate (often from within the system and reflected in relatively low detection rates)

- Invisibility often reflects sophisticated money laundering techniques
- Corrupt 'insiders' often involved in preventing detection
- May involve politically exposed figures or wealthy business people

Corruption related money laundering is often transnational

- Funds and evidence may largely be in another jurisdiction
- Investigation requires cooperation and assistance from other jurisdictions

Corruption-related money laundering investigations may therefore be complex and resource intensive

- Often law enforcement agencies lack adequate resources to cope with complex cases

### **Conclusion**

The importance of strong and independent anti-corruption bodies having powers to investigate directly financial matters was highlighted as an important aspect of any regime to effectively combat corruption related money laundering. Pakistan was highlighted as a jurisdiction where the national anti-corruption agency has been serving as the jurisdiction's interim FIU. Hong Kong was highlighted as a jurisdiction in which huge advances had been made in tackling public sector corruption over the past 30 years, particularly through the leading role of the Hong Kong Independent Commission Against Corruption (ICAC).

The following essential factors for an effective anti-corruption agency were highlighted:

- *Independence*: ensures freedom from interference in conducting investigations
- *Adequate investigative powers*: including powers to investigate bank accounts, to require information, to restrain properties etc
- *Proactive approach to investigations*: including close cooperation with law enforcement agencies & regulatory bodies (especially FIUs), use of informants, surveillance and undercover agents
- *Specialist investigative capacities*: professional Financial investigators, Computer forensics
- *International cooperation*