The Asia/Pacific Group on Money Laundering (APG)

APG Typologies Report 2008

11 July 2008

Available at www.apgml.org

CONTENTS

INTRODUCTION

Background

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

The APG's typologies work describes and analyses the nature of money laundering and terrorist financing. Since its establishment in 1997, the APG has undertaken typologies work to share information and support a better understanding of money laundering and terrorist financing methods, techniques and trends in the region.

Typologies of money laundering and terrorist financing allow governments to understand the nature of the problem and design effective strategies to address threats. Typologies help APG members to implement effective strategies to investigate and prosecute money laundering and terrorist financing, as well as design and implement effective preventative measures.

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

Recent Regional and Global Typologies Events

Indonesia hosted the 9th APG Typologies Workshop in November 2006. It was attended by over 200 participants, representing 34 jurisdictions and 9 international and regional organisations. The 2006 APG Typologies Workshop focused on:

- Vulnerabilities in the casinos and gaming sector;
- Vulnerabilities in the real estate sector;
- Illegal logging money laundering issues; and
- Settlement mechanisms in alternative remittance systems.

In December 2006, the APG participated in the joint Typologies Meeting between the Financial Action Task Force (FATF) and the Eurasian Group (EAG, the FATF-style regional body for Central Asia) in Shanghai, China. The FATF/EAG meeting focused on:

- Laundering the proceeds of narcotics trafficking;
- Missing trader intra-community fraud ("carousel fraud");
- Money laundering through the real estate sector; and
- Terrorist financing typologies.

In November 2007, the APG hosted a joint APG/FATF Typologies Meeting in Bangkok, Thailand. The joint workshop focused on:

- Money laundering threat analysis strategies;
- Proliferation financing;
- Vulnerabilities in the casinos sector; and
- Money laundering and terrorist financing vulnerabilities of on-line commercial sites.

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

SECTION I

INTERIM UPDATE
Vulnerabilities in the Casino and Gaming Sectors

Background

The APG and FATF are jointly studying vulnerabilities in the gaming and casinos sector. The project is examining:

a) Vulnerabilities in the gaming and casino sectors with an emphasis on legal sectors that have a physical presence;

b) Sector-specific money laundering or terrorist financing indicators; and

c) Policy implications for effective implementation of FATF standards in the sector.

The APG/FATF study will be completed in October 2008, when a comprehensive report will be published on the APG website.

Bangkok Typologies Meeting 2007 – Casinos Workshop

The 2007 APG/FATF Typologies Meeting included a workshop on casinos. The workshop noted that a large number of countries have a legal casino or gaming sector and citizens from an even wider number of countries participate in gaming through gaming-related tourism. Over 150 countries have some kind of legal gambling with over 100 countries having legalised casino and card room gambling.

There is a significant number of emerging casino/gaming markets, particularly in the Asia/Pacific region. Singapore and Papua New Guinea are two examples.

The APG/FATF workshop noted that many of the countries that have emerging casino markets have cash-based economies with governance challenges (Nepal, Sri Lanka, Papua New Guinea and Vanuatu are examples). Emerging casino markets are often in countries with weaker AML capacity.

The workshop discussed in detail a range of vulnerabilities common across casino and gaming sectors, and related policy issues, including

Gaming activities

- Intentional losses, buying winning chips/tickets from legitimate winners etc;

Casino Facilities and Services

- Casino chips – use as currency outside of the casino, use of 'dead' chips etc,
- VIP / High Rollers;
- Casino cheques;
- Refining, currency exchange, chip purchases etc;
- Junkets (casino-based tourism) – organised movement of people and money;
- Ancillary activities - loan sharking, prostitution, etc;
- People employed in the sector, including issues related to high-staff turnover;

Weak AML regulation and implementation

- The range and application of sanctions, including corporate criminal liability;
- Responsibility for internal policies to detect abnormal gambling behaviours; and
- Tools to use against casinos which are complicit or wilfully negligent in ML.

These issues will be discussed in detail in the October 2008 report on casinos.

SECTION II

TYPOLOGIES NOTE

Money Laundering and Illegal Logging

Introduction

In October 2006 the APG with the World Bank held a Special Seminar on illegal logging money laundering issues. The Seminar brought together APG jurisdictions, international organisations and NGOs to consider AML/CFT measures to address the proceeds from forestry crimes.

Statement of the Problem

- The financial backers for criminal timber extraction operate globally and benefit from enormous proceeds crime.
    - Illegal proceeds are laundered to benefit those who control the illegal timber trade.

- The World Bank estimates that illegal logging is worth up to US$15 billion per annum and accounts for up to 25% of forest removals worldwide.
    - Every year 10 million hectares of forests are destroyed, driving environmental changes.
    - Industrial timber exports are around US$150 billion per year.

- Forestry crime is a transnational issue and includes money laundering to help realise the profits of this crime.
    - Illegal logging and associated money laundering are closely connected. In the Asia/Pacific region, the two are linked to corruption and bribery, organised crime; smuggling offences, bank and other fraud.
    - Associated corruption affects customs, tax, law enforcement, military etc.

- It is a challenge to harness political commitment to act to combat money laundering associated with illegal logging.
    - There are barriers to understanding the nature of the problem and to endorse options to take effective action.

- The APG notes the risks of politically exposed persons related to the illegal timber trade.
    - Politically exposed persons are a challenge for investigating corrupt regulators, police or military officers that may be involved with the illegal timber trade.

- APG members highlight the need to integrate anti-money laundering and asset forfeiture tools into efforts against forest crime and related high-level corruption.
    - Effective money laundering legislation and preventative measures provide strong tools to detect the profits and investigate and prosecute the persons behind illegal logging and prevent financial markets from abuse.

- Corruption may stop issues of money laundering and illegal logging from being considered a national priority.
    - As an example, corruption has an effect on the response to illegal logging in Indonesia, despite some committed officers, and undermines trust between those authorities responsible for the enforcement and prosecution of relevant offences.

Some Possible 'Red Flag' Indicators

- Unexplained wealth of forestry officials (indicated by purchase of high value goods such as luxury vehicles) may be a red flag for bribery of officials involved in the sector.
- Trade transactions to finance timber business (extraction, shipping, milling etc) to a high risk country – i.e. where no legal forestry concessions are in operation.
    - For example, in Cambodia there are no legal concessions for logging and or commercial exploitation of forests by any foreign companies.
- False or questionable statements on bank loans, letters of credit, customs and shipping documents associated with the timber trade.
- Sources of cash used for loggers, food, chainsaws, trucks, heavy equipment, shipping etc.
- Involvement with politically exposed persons or military, police, or other law enforcement by:
    - timber brokers,
    - forestry officials,
    - licensed concession-holders outside contract,
    - wood processing companies, shippers, exporters, customs officials, and
    - financial institutions.

AML/CFT responses to the proceeds of illegal timber extraction

The FATF 40 Recommendations are relevant to combating money laundering that is associated with illegal logging and other forms of illicit resource extraction:

- Environmental crimes are in the "Designated Categories of Offenses" that the international standards require to be predicate offences for the ML offence;
- In some jurisdictions, illegal logging has been listed as a predicate offence, for example in Indonesia and recently in Malaysia.
- FATF requires countries to put in place preventative measures to deal with financial risks from "Politically Exposed Persons".
- Criminal prosecutions and asset forfeiture are a powerful deterrent and will result in recovery of substantial assets.
- The international standards call for coordination between relevant authorities to investigate and prevent money laundering.
- International coordination is essential to investigate and prevent money laundering and associated predicate crimes.

Opportunities for Action

The APG's work with the World Bank, NGOs and other organisations has identified a number of opportunities on which to take action:

- Involve forestry ministries in AML/CFT national coordination committees (NCCs).
    - A number of APG jurisdictions include natural resource ministries/agencies in AML coordination mechanisms.
    - For example, in response to identified money laundering associated with illegal fishing, New Zealand includes the Fisheries Department in its AML NCC.
- Financial intelligence units (FIUs), relevant forestry and law enforcement agencies need good working relationships to share information and to work with other stakeholders.

    - Intelligence on illegal logging, forest smuggling, illicit trade, and associated financial activities are often found in media reports and the investigative work of NGOs and from international organisations (e.g. the World Bank).

- Support international cooperation to investigate and identify risks in the sector.
    - AML/CFT regulators need to share information with international counterparts on risks associated with illegal logging across the region.
    - For example in Cambodia there are no legal concessions for logging and/or commercial exploitation of forests by foreign companies.

- Foreign counterpart FIUs should be aware of the risk profiles of logging sectors in order to advise their financial sector on risks associated with logging business.
    - The example in Cambodia requires regional financial institutions to be aware of high risks and to monitor for and report suspicious transactions.

- Ensure guidance is given in preventative measures that address risks from the logging sector.
    - Guidance on risks from illegal forestry should be included in KYC/CDD guidelines issued to financial institutions and other reporting entities for AML/CFT compliance.
    - Guidelines should include “Red Flag” indicators for financial institutions, lawyers and accountants.

- Establish specialist inter-agency AML and illegal logging ‘strike-forces’/task forces of dedicated law enforcement and regulatory resources.
    - These allow a combined strategic approach to target abuse in the sector and focus on investigation, prosecution, freezing and confiscation of proceeds of crime. Indonesia is considering a strike-force response.
    - Dedicated task forces help build trust and cooperation and support information sharing.

- Develop and share a best practices guide for investigators and prosecutors - to provide specialised capacity to investigate and prosecute money laundering associated with illegal logging.
    - Training investigators, prosecutors and judges, including how to conduct financial crime investigations, is essential.

- Support cooperation with NGOs, regional timber importers, and other stakeholders in the sector to support the development of a culture of AML/CFT compliance in the sector.
    - NGOs and legitimate timber sector are key partners for competent authorities in combating money laundering in the sector.

International responses

The APG’s work to consider issues of laundering the proceeds of forest crimes follows a range of broader regional and global responses including:

- Bali Ministerial Declaration on Forest Law Enforcement and Governance (Indonesia, China, Cambodia, Lao PDR, Papua New Guinea, Thailand, Philippines)
- EU Action Plan for Forest Law Enforcement Governance and Trade (May 2003);
- China-UK Letter of Intent (May 2004);
- China-Indonesia MOU (December 2002);
- Norway-Indonesia Letter of intent (August 2002);
- Africa FLEG Ministerial Declaration (16/10/2003);

- Japan-Indonesia MOU (June 2003);
- US President's Initiative on Illegal Logging (February 2002); and
- APG Typologies Workshop, Brunei (October 2004).

CASE STUDIES

INDONESIA

Case Study 1

During 2004 – 2005, a high-ranking officer of district forestry services, Mr. X, received an incoming transfer from several forestry companies for total amount of Rp30 – Rp100 million. It was indicated that those companies operate illegal logging activities in P Island. Therefore, in order to protect their illegal timber businesses and to obtain timber transportation documents (known as SKSHH), they regularly paid bribes to Mr. X. Based on Mr. X's credit card transactions, it was found that he frequently made transactions at jewellery shops and travelled to Singapore several times.

Case Study 2

Ms. A and Mr. B opened seven current accounts in Bank P on August 2001. Then, Ms. A authorised Mr. B and one foreigner (Mr. C) to withdraw money from her account whenever they needed. Mr. B and Mr. C are known as timber exporters to Singapore and Malaysia. From 2001-2004, they received money transfers worth a total amount of US$11 million from several timber companies in Singapore and Malaysia. Mr. B and Mr. C got logs from Papua and East Kalimantan. To prevent detection and seizure by local government officials, Mr. B periodically transferred money to private accounts of forestry government officers and law enforcers to pay bribes to avoid enforcement actions.

MALAYSIA

Mr M, a suspect involved in drug trafficking activities, had the criminal proceeds derived from his illegal activity kept with his sister-in-law, Ms BB as his nominee. Ms BB owned a business in selling/servicing tyres and declared she earned a monthly and daily income of RM6,000 (equivalent to approximately US$1,740) and RM2,500 (equivalent to approximately US$725) respectively. However, her income could not be verified with any legal documents.

Ms BB opened an account with Bank ABC which regularly received cash deposits. She also placed personal fixed deposits and joint fixed deposits with five other individuals totalling RM1 million (approx. US$290,000).

It was also revealed that Ms BB is shareholder and director in Company XYZ together with two other individuals and Ms BB made multiple cash deposits into the company account of Company XYZ. A banker's order of RM1.3 million (approx. US$377,000) was paid via a solicitor firm to pay Company KLM for a timber concession of 300 hectares to launder the illegal proceeds

SECTION III

REAL ESTATE – REGIONAL VULNERABILITIES

Introduction

Over a number of years APG jurisdictions have highlighted vulnerabilities and reported case studies of money laundering involving the real estate sector.

During 2006, the Financial Action Task Force (FATF) studied vulnerabilities in the real estate sector globally. At the same time the APG focused on real estate in the Asia/Pacific region and contributed a regional perspective to the FATF study.

The comprehensive report on the FATF study on the real estate sector was published in June 2007. It is available via the FATF website: http://www.oecd.org/dataoecd/45/31/40705101.pdf .

The FATF study identifies characteristics of the real estate sector that may be attractive for money laundering and possibly terrorist financing. The detailed report sets out case examples of basic techniques such as: the use of complex loans or credit finance; the use of non-financial professionals; the use of corporate vehicles, and several other techniques. The report also highlights risk indicators which may assist the private sector in implementing AML/CFT preventative measures.

The FATF study highlighted:

- The common use of wire transfers to channel funds in money laundering cases involving real estate.
- Due to the worldwide market growth of real-estate-backed securities and the development of property investment funds the range of options for real-estate investments has also grown.
- Money laundering transactions can be camouflaged in genuine commercial transactions among the huge number of real estate transactions.
- Emerging markets have particular vulnerabilities for misuse of the real estate sector, due to an absence of accurate average market price for real-estate; prices vary across sectors and districts.
- Real estate transactions generally involve, in some stage of the process, legal intermediaries, and the report notes a number of vulnerabilities from the role of intermediaries.

Some Regional Observations by the APG

Regional observations from the APG's recent work on the real estate sector were made:

- The real estate sector is an attractive destination for illicit funds.
- A number of jurisdictions report very significant increases in real estate prices, and sectors with fast rising prices are attractive to criminal investment for money laundering.
- A number of countries note real estate as being particularly associated with criminal proceeds associated with corruption and narcotics as well as a variety of other predicate offences.
- Politically exposed persons are an issue in relation to land-zoning, development approvals etc.

- Corruption is an issue in many countries, particularly for regulatory agencies related to real estate;
    - Land titles offices or equivalent are highly susceptible to corruption in countries with low capacity, low levels of pay for staff and weak transparency.
- Money-laundering related real estate transactions involve a complex mix of money laundering and tax evasion and such cases may represent significant losses of taxation revenue.
- Money laundering in the real estate sector typically involves the use of nominees or front companies.
- There is a common trend for combined 'off the books' settlement transactions, which involve formal payment at significantly undervalued prices, combined with a cash component which is not declared to the authorities.
- A number of countries where it is illegal for foreigners to own real estate note common techniques of using third parties to hold real estate on behalf of offshore beneficial owners;
    - These are wide open to abuse for money laundering.
- There is a lack of good information on land values and therefore fair market price to allow financial institutions to recognise under-valued transactions.
- Many Asia/Pacific jurisdictions have an underdeveloped or emerging real-estate agents sector and regulation of the real-estate agents sector is typically weak in jurisdictions with developing economies.

CASE STUDIES

CANADA

Integrating cash in real estate investment: An individual associated to an Outlaw Motorcycle (Biker) Gang took out a legitimate $200,000 mortgage with a domestic financial institution to purchase a property valued at approximately CAD350,000. The individual claimed to have obtained 15 promissory notes, valued at $10,000 each, which he put towards the purchase of this property as a down payment. The lenders of these promissory notes were associates of the mortgage holder and there was no evidence that any money had been loaned.

The mortgage holder took out an additional $150,000 mortgage on his property, which was registered in the name of another individual. Police interviewed this lender and it was learned that he had not loaned any money to the mortgage holder and was unaware of the existence of this mortgage.

The individual demolished the existing house on the property and built a new house. Architects and builders were paid in cash (sometimes in briefcases full of cash). In total, police established that an additional $400,000 to $500,000 in cash was paid to construct the home, which is now valued at over $1 million.

Mortgage brokers involved in predicate crimes and ML: A provincial regulatory agency responsible for the real estate sector received reports from financial institutions of irregularities related to mortgages involving the same mortgage broker. Search warrants executed at one of the mortgaged properties revealed a marijuana production operation. Investigations identified additional mortgage brokers, all from the same ethnic community, who appeared to be involved in securing numerous suspicious mortgages through major Canadian financial institutions as well as smaller credit unions.

The most prolific of the associated mortgage brokers had secured 900 mortgages over a period of 18 months. This individual was also discovered to have registered second mortgages on some of the properties on behalf of a company in the name of his spouse. This mortgage broker's fees for securing the 900 mortgages were $2 million.

HONG KONG, CHINA

Dissipating realisable assets to avoid confiscation: Ms Y, the head of a pirated optical disc syndicate, was arrested. Shortly after her arrest, to prevent her assets being restrained and confiscated, she sold her property to a friend at a price which was grossly undervalued. The transaction was an apparent attempt to dissipate her realisable assets. She had further appointed her brother to be her attorney to represent her in the whole property transaction. The profit of selling the property was deposited into her brother's accounts and was finally dissipated. The purchase of real estate is commonly used as part of the last stage of money laundering (integration). The case study illustrates the use of a third party to disguise the realisable assets for the purpose of staying away from confiscation.

REPUBLIC OF KOREA

Off the book real estate transactions: Company A sold land it owned for KRW 6 billion. *Person B*, president of the company, underreported the proceeds from the sale by drawing up a false contract with a price lower than the actual price. He then embezzled the difference between the true price and the reported price by depositing it in three accounts held by *Person C*, an employee of *Company A*. *Person B* made a significant capital gain from the sale of the land, which the company bought at a cheap price at auction in 1997 when the land price plummeted because of the Asian financial crisis.

Laundering through real estate-related fees/payments: Person X, the former president of a conglomerate, also holds a senior position at a university. He owns a commercial building. He signed a false contract with the university pretending that the university was renting the commercial building to use as a dormitory. He then embezzled a total of approximately 2.5billion won from the university in 71 transactions by disguising the money as a guarantee deposit, maintenance fees, and construction costs.

NEW ZEALAND

Investing drug proceeds in real estate: An offender used the proceeds of cannabis sales to place deposits on two residential properties that he subsequently rented. Substantial quantities of cannabis were found at his address, as well as a rented storage facility. He was later convicted of drug-related offences and money laundering.

PAKISTAN

Corruption and laundering related to real estate: Mr. X became member of the Assembly and Chairman of the Local Development Body. Soon after assuming the offices, he started making investments in real estate. The mode of acquisition of real estate was as follows: Mr. X owned a small piece of agricultural land. During his term in office he purchased a big piece of land valuing millions of rupees in the names of spouse and son. The purchase was hidden by showing it as an exchange, i.e. Mr. X recorded the exchange of his small piece of agricultural land with a bigger portion of land owned by Mr. Y at approximately equal value. In fact the land originally belonging to Mr. X was never given to Mr. Y, as Mr. X had purchased Mr. Y's land.

Mr. X afterwards sold the newly acquired land to Mr. Z at the market rate. The proceeds of sale were shown to have been spent on the purchase of further properties. In fact the sale

was again a sham transaction. Mr. Z was a relative of Mr. X and had no resources to purchase the property. The property at all times remained under the use of Mr. X. The entire exercise was undertaken to launder corrupt proceeds by showing them as proceeds of sale of property.

***Investing proceeds of corruption in real estate using nominees**:* An official responsible for deduction of tax from the salaries of employees and for payments made to vendors and service providers was found to have forged documents and used fake bank documents to embezzle over 19 million rupees.

The accused had converted the embezzled amount into real estate by investing in a new housing scheme where he purchased a number of plots in his wife's name, in order to avoid detection. The accused was in possession of an expensive car, which was linked to proceeds of crime.

VANUATU

Vanuatu FIU recently assisted a foreign jurisdiction where the proceeds of fraudulent activity committed in that jurisdiction had been wired to bank accounts in Vanuatu. The offender spent time living in Vanuatu and operated as a property developer. He was involved in several developments and businesses associated with the Vanuatu tourism industry. Proceeds of crime were intermingled with other funds then wired to Vanuatu using the developments to mask both the source of the funds and their ultimate disposition.

CAMBODIA

Cambodia is a developing economy undergoing a property boom. Foreigners are precluded by law from buying real estate. A money launderer uses a nominee local to purchase real estate on his behalf. At the time of purchase, he has the nominee sign both the purchase and sale contracts. The sale contracts have no details for the price or name of the future buyer.

It is common practice for real estate transactions to be conducted in cash and in US dollars (estimated at 60% of transactions arranged by real estate agents in Cambodia), with cash transactions up to USD1million in Phnom Penh. Up to 70% of transactions are directly between the buyer and seller without the use of a real estate agent. Furthermore, Cambodia has no independent property valuation system. The price of property is determined by the buyer and seller which can be easily abused for money laundering purposes.

THAILAND

French press reports in September 2007 indicated that 27 people were standing trial accused of running a prostitution ring whose profits were laundered via a luxury property development in Thailand. It is alleged that a double bookkeeping system was used in hostess bars to embezzle funds, which were invested in a property development in Thailand.

SECTION IV

OVERVIEW OF CASE STUDIES ACROSS THE REGION

The 2008 APG Typologies Report includes an overview of collected case studies from across the Asia/Pacific region. This is not an exhaustive list of case studies submitted to the APG. The cases reported do not represent all matters that were submitted, nor are they the largest or most serious cases. Rather, these cases studies present a cross-section that illustrates the diversity of typologies across the region.

Alternative remittance services/underground banking

AFGHANISTAN

Afghanistan's FIU noted a number of trends in relation to the conduct of hawala in Afghanistan and the typical settlement process.

For remote and volatile areas, hawaladars prefer to rely on the transfer of physical money, most often by local people. For transfer of funds to or from Europe, physical transfer of cash is not used for settlement.

For hawaladars, transfers take place based on collateral placement. Because of CDD requirements, transfers through banks take place only to companies and generally in relation to trade finance.

For some hawaldars they may ultimately take two or three years to make a balance against counter transactions.

PAKISTAN

Settlement mechanism for alternative remittance: A large number of suspicious transactions were detected by the Audit team of the State Bank of Pakistan in a commercial Bank-X operating in Pakistan. These abnormal transactions included foreign remittances (both inward and outward). Hundreds of pay orders and demand drafts amounting to billions of rupees were issued from some accounts in a matter of days. One individual account showed a turnover of more than 4 Billion rupees in a year.

Preliminary investigations have revealed that these accounts were opened using fake/fictitious names at various branches of the Bank-X for the purpose of settlement of hawala/hundi transactions.

INDIA

Invoice manipulation for false uncut diamonds: India reported a case of laundering foreign exchange through a scheme which appeared to be importing rough diamonds for polish and re-export. The group made a trial run to understand systems and procedures of re-export with small quantities of genuine diamond imports. They utilised bank accounts in the names of nominees at various banks and deposited cash and transferred to a master account. The group subsequently prepared forged documents to show large imports of diamonds. By submitting forged import documents to banks they successfully remitted huge amounts of foreign exchange abroad. The cash for the foreign exchange remittances were made available by the hawaladars in India.

Export of cut and polished diamonds: Diamond exporters in India typically have offices in Singapore, Hong Kong, Dubai, the USA and Antwerp. The money laundering scheme established separate export bills for the same stones to be exported through a chain of offices with remittances coming from India. One consignment is exported from India to Singapore. A fresh export bill is made for export to Dubai, then another to the US, then a final export bill from the US to Antwerp by respective offices. The export bills are discounted within a period of three days from the date of export by the India exporter and they get around 80% of the export proceeds. Likewise the Singapore office also gets the export bill discounted on their export of the same consignment to Dubai and so on till the consignment reaches Antwerp. Thus each office gets liquid funds of around the 80% of the export value within a period of 20-25 days taking into consideration the time of delivery by the courier.

The time-period for realisation of export proceeds is around 180 days. In certain cases, the diamonds after reaching the Antwerp are smuggled back/imported into India and the process is repeated again, at least 4-5 times. Thus in case of invoice of $100,000 total amount of cash funds available in the hands of the cartel is around $320,000 in each cycle and if repeated five times the amount reaches $1.6million. The funds are made available at premium to the persons involved in invoice value manipulations and used for alternative remittance.

HONG KONG, CHINA

Nominee account used for remittance: In early 2000, an STR triggered an investigation into the recipients of structured remittances from jurisdiction 'A'. Investigation showed that the remitters worked for a seafood company in jurisdiction 'A'. The elder brother of the owner of the seafood company's was based in Hong Kong, and he was found to have recruited new migrants to Hong Kong and to open nominee accounts to receive structured remittances from jurisdiction 'A'.

A six-year investigation found that the source of the structured remittances was drug proceeds and resulted in the successful prosecution of the elder brother and his accomplice in Hong Kong. It was estimated that a total of HKD110 million passed though these accounts.

MACAO, CHINA

Use of casino accounts for alternative remittance: A merchant in Country A could not perform a large remittance to Country B due to its foreign exchange control. With the help of a junket promoter, he transferred the monies to the VIP room of a local casino, which informed an underground remitter in Country B (by phone, fax or email) about the amount and beneficiary of the funds. This remitter would then arrange payment of the fund to the beneficiary. For Country B citizens who wished to gamble in this casino of Country A but had difficulty in bringing in cash, they could arrange alternative remittance through this remitter who would then inform details of these customers to the VIP room. When these citizens arrived at the VIP room they could immediately obtain the amount required for gambling. Both the VIP room and the remitter would perform reconciliation for net settlement, and basically no transfer of monies between two sides was required.

*****

Cash Couriers/Currency Smuggling
(bearer negotiable instruments, concealment, security, amounts etc)

AUSTRALIA

Use of airline pilots as cash couriers and use of alternative remittance: Investigation revealed that a number of remittance agents located in both Melbourne and Sydney had acted in concert with each other and received large amounts of cash from members of organised crime syndicates.

The majority of the funds were sent out of Australia utilising the banking system

CANADA

Trends with the use of professional cash smuggling syndicates: Canada noted typical currency smuggling operations commencing with money broker being contacted by the drug trafficking organisation who needs to repatriate its dues. A contract is then settled at a determined price. The next step involves the group responsible for picking up the money in various cities. As an example, during the course of an investigation, it was determined that one group flew to Country A from Country B to pick up money in various Country A cities and gathered all the money in a safe house located close to the border. Their fees were 1% of the amount carried. A second group was responsible for carrying the money across the border into Country B. Each member of the group carried less then $10,000 of Country B currency and was paid $200 each for every trip. The fees for crossing the border were also substantiated in another investigation.

Use of students to courier bearer negotiable instruments: The criminal organisation responsible for laundering drug-proceeds in Country A used students to purchase multiple cashiers' cheques. These cheques were then glued in magazines that were sent, via a courier service, in Country B. The reason provided by the students at the financial institutions/money service businesses is that the money came from a grant provided by a Country B company. The cashiers' cheques were to pay for their tuition fees. A total amount of $3 million went through the courier service using this technique.

CHINESE TAIPEI

Cash couriers related to alternative remittance: Chinese Taipei Customs and FIU identified an underground banking operation utilising cash couriers. Mr. Yu, was identified as having carried 487.45 million Japanese Yen, USD93,000 and 3.6 million in Korean Won out of Chinese Taipei in 14 departures over approximately 12 months related to alternative remittance. While all these monies were not proceeds of crime, investigations of a fraud case identified the movement of proceeds of a bank fraud case through the underground. Mr Lin et al, defrauded domestic banks with false letters of credit by instructing these banks to wire USD 42.8 million to the shell company Lin et al set up. They remitted the proceeds back to Chinese Taipei via Mr Yu and the under ground banking system he was associated with.

REPUBLIC OF KOREA

Settlement mechanisms for alternative remittance: Person A received 2,000 counterfeit 500 Indian Rupee notes (about USD 20,000) in Beijing, China from Person X, who is a Chinese citizen. He carried the notes into Korea. Person A changed the counterfeit notes into Korean Won at a bank in Korea. Person A laundered the illegal proceeds by remitting them to Person X in China through alternative remittance system (ARS) between Korea and China. He repeated the process again later. He brought 10,000 counterfeit 500 Rupee

notes (about USD 100,0000) into Korea, converted them into Korean Won, and then sent them to China through ARS.

NEW ZEALAND

Smuggling cash disguised in cigarette packets: New Zealand Customs Service spoke to a Chinese National transiting through Auckland Airport from Samoa to Bangkok. NZ customs detected cash being couriered by the person. Located in his luggage was a sealed carton of Pall Mall cigarettes. The carton contained ten sealed packets of cigarettes. Each cigarette packet in turn contained USD2,000 cash.

On examination, the cigarettes and packaging had been professionally sealed and were no different from standard packaging.

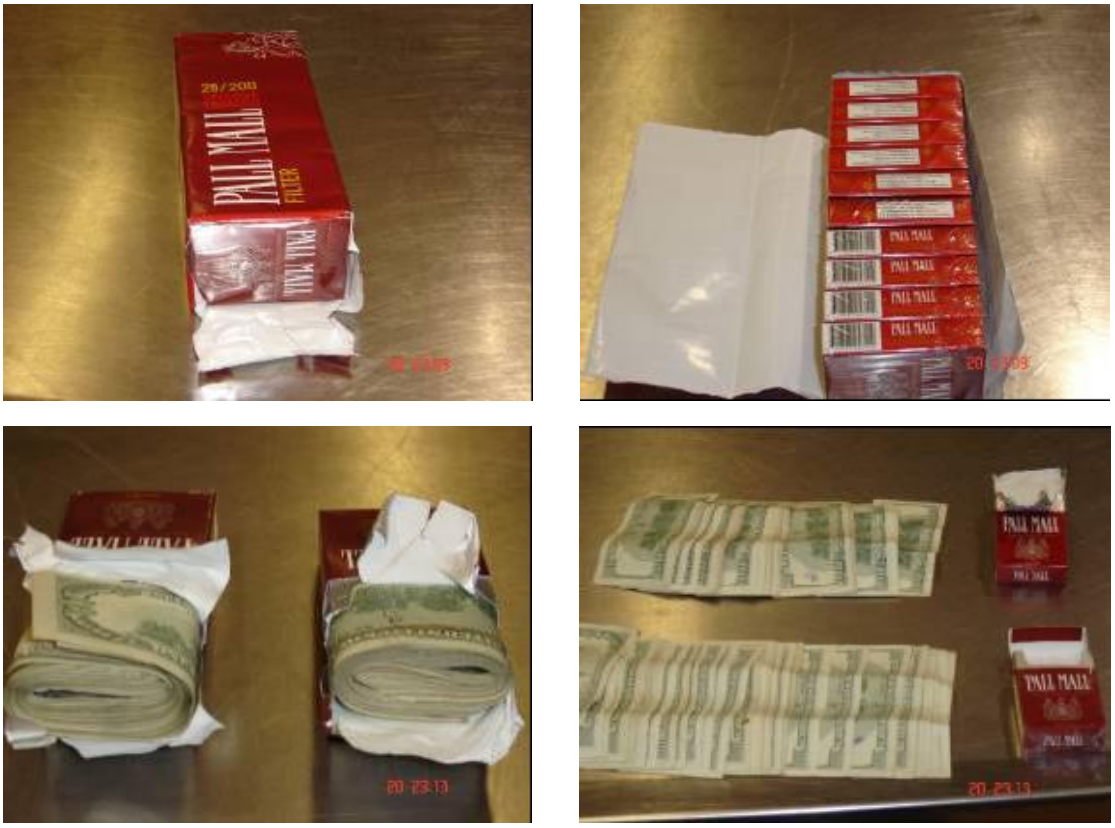

Photo: New Zealand Customs –detection of cash courier at Auckland airport

PAKISTAN

Cash couriers for alternative remittance: During a random check by Lahore Customs Authorities a passenger failed to declare currency. Based on suspicion his luggage was checked which led to the recovery of Euro 185,000, UAE Dirham 225,000 and Saudi Riyal 200,000. The accused claimed that he was a registered importer of electronics and other goods from Dubai, China, Hong Kong etc and had registered business, M/s ABC Company. Computerised import record of Revenue Authorities confirmed that no imports had ever been made by this concern.

He later admitted to previous instances of transfer of foreign currency. Passport entries revealed that in the last 2 years he had undergone 37 foreign trips. On the basis of evidence obtained, Customs officials were also arrested in relation to the matter. Seized foreign currency was confiscated.

Foreign Exchange Companies involved in cash courier activities by using falsified or parallel currency export documentation. The case involves two representatives of the same company taking two different flights to Dubai arriving at the same time, both carried letters for the export of foreign currencies. One declares a small amount of currency, but smuggles a large amount of currency. The second person carries the exact same amount of currency in the same denominations, but all declared. Two persons carrying currency, with identical details of Foreign Currency enables the couriers to control a situation in case the smuggling courier is apprehended by Customs, then they will attempt to exchange export declarations which contained identical details of currency.

During investigation it was observed that the exchange company in question had adopted the same modus operandi over at least eleven trips between Pakistan and Dubai. It was estimated that over USD18 million could have been smuggled in this way before being detected.

PHILIPPINES

Smuggling proceeds of corruption: A & B are children of C, a politically exposed person (PEP), who was responsible for disbursing government funds in his agency. On departing for Country 1, A and B were caught with an amount exceeding $20,000 hidden in the pockets of pants folded inside their baggage. Both A & B had failed to declare the amount in the appropriate foreign currency and the money was seized. Country 1 also alerted the authorities of Country 2, the country of origin of A and B. C and his spouse D claimed that the money discovered on their children belonged to them and was intended as a deposit for the purchase of a property located in Country 1.

This incident triggered an investigation into the extensive travel history of C and D and their children A and B (both unemployed). It was found out that on previous occasions of entry into Country 1 they, either together or separately, brought into the country, money amounting to hundreds of thousands of dollars. Country 2's authorities also revealed extensive bank transactions with respect to the accounts under the names of C, D, A and B, either individually or jointly held by them, amounting to millions of pesos and hundreds of thousands of dollars. Comparison of the volume of bank transactions made with the declared/known sources of income of C and/or D indicates that the transactions were not commensurate to, and were in fact far beyond, their financial capacity.

Both A and B currently face prosecution for such failure to declare in Country 1. A, B, C and D are currently charged with plunder and are under investigation for money laundering in Country 2. All known accounts and other assets of the family remain frozen.

*****

Currency Exchanges/Cash Conversion

CANADA

Professional launderers operating money exchange business: A recent investigation demonstrated that the main target operated a complex set up of currency exchanges and money remitters. The target also used other currency exchanges in order to "diversify" the money laundering activities.

An investigation determined that a known drug trafficker was associated with an owner of a currency exchange located in Country A. This owner was defined as a financial pivot. He used his bank in Country B to store the profit of the drug dealer. The money was repatriated on demand when needed. The currency exchange was also used by the drug trafficker to convert his Country A currency's drug proceeds to Country C currency since purchasing cocaine in Country D required Country C's currency. The currency exchange owner's Country C currency needs were looked after by Country A marijuana exporter who collected Country C currency but needed Country A currency.

Recent trends: Intelligence reports from FIUs indicated that money launderers were using money service businesses extensively in Canada to convert hundreds of millions of dollars into Canadian currency. These typically involve professions money laundering groups servicing drug-trafficking organisations exporting marijuana from Canada to Country A. Typical techniques involve exchanging pre-arranged amounts which vary from $100,000 to $1.5 million per transaction. The individuals, after collecting monies to be exchanged from numerous sources, negotiate rates according to daily market yields.

REPUBLIC OF KOREA

Use of bank and non-bank financial institutions for conversion: Person A gained illegal proceeds from fraud and handed over the illegal funds to his accomplices *C, D, E* and *F*. The accomplices converted the money into U.S. dollar and Chinese Yuan at commercial banks. Then they visited various money exchange booths in the airport to convert the USD and the Chinese Yuan back to Korean Won.

NEW ZEALAND

Use of foreign exchange houses: During the course of an investigation into a pseudoephedrine imported from China, New Zealand police identified an offender depositing large amounts of cash through a number of foreign exchange dealers in the Auckland Central Business District. A proceeds of crime investigation resulted in the identification of more than NZD4.1 million cash laundered through three foreign exchange outlets over a short period of time.

Professional launderers operating money exchange business: Another investigation identified an unrelated foreign exchange dealer laundering the proceeds of a major methamphetamine drug distribution network. A search warrant of the premises located NZD2.1 million of hidden cash. The foreign exchange dealer was subsequently charged with money laundering.

AUSTRALIA

Money exchange business assists in structuring: The case involved collusion between the head of a money exchange business and the money launderer, Mr B. Mr B purchased a large amount of travellers cheques, but the head of the money exchange business recorded each transaction as being below the reporting threshold of AUD10,000. Mr B completed the travellers' cheques sales documentation in false names and did not sign the travellers'

cheques. The transactions had been recorded as separate amounts, all less than AUD10,000, even though a much larger amount had been initially provided by Mr B. Investigations showed that the larger transaction over AUD10,000 was broken into smaller amounts and each amount was recorded in different exchange rates to conceal the true amount of the transaction and thus avoid the reporting requirements.

*****

Trade-Based Money Laundering

AUSTRALIA

Tax fraud and use of offshore accounts: Directors of a company were involved in purchasing large quantities of duty free cigarettes and alcohol to sell on the domestic market contrary to their export-duty free status, thus avoiding tax obligations. The company generated false receipts which an export company detailing their alleged cigarette exports. Investigations confirmed that no such exports had ever been made.

Payment was made for the cigarettes on a cash-on-delivery basis. A large number of the company's sales occurred over the internet from customers paying via credit card. A majority of the sales on the internet were illegitimate and came from three different email addresses. Payments for these orders were made from one of two credit cards linked to Belize bank accounts. One card was held in the company's name. The money in the Belize bank account was sent there by one of the directors using several false names from not only Australia but also Belize, Hong Kong, and Vietnam. The director conducted structured wire transfers under false names and front company accounts. The funds were purchased at well known banks with multiple transactions occurring on the same day at different bank locations and all of the cash transfers conducted in amounts of just under AUD10,000 to avoid the reporting threshold.

CANADA

Laundering of drug proceeds through trade using grain as commodity: A broker was used as an intermediary between the Canadian company supplying the grain and a Colombian drug cartel. Drug proceeds were introduced into the banking system using "smurfs" who would make bank deposits or purchase bank money orders or postal money orders.

The broker settled a contract with the Canadian company to supply grain to a Colombian company. Upon settlement of the contract, the Canadian company would get paid by way of letter of credit and third party cheques or electronic funds transfer (EFT). 70% of the value of each contract was covered by way of a L/C and 30% being forwarded by way of third party cheques or EFT. The 70/30 split was used to defraud the Colombian Government by reducing the amount of tariff required to be paid. The actual value declared equalled the amount of the L/C (70% of the total value). It was found a total of 39 financial institutions were used for L/C or EFT for a total dollar value of $35 million. Furthermore, 63 bank accounts at 53 different financial institutions were used to forward funds by way of cheques and 21 postal outlets were used to purchase 31 postal money orders for a total dollar value of $1.2 million. Once paid, the grain would be exported to Colombia. The Colombian cartel would get their share from the Colombian importer once the grain was sold on the local market.

FIJI

Invoice manipulation: A Fiji company was found to be sending goods to its sister company in another Pacific Island country. The local company used their own invoice and since the

goods were under the value of FJD20,000 no export licence was required. Goods were mostly bought from another local company. All exported goods were not reflected on the invoices and the export entries did not show full contents of the container. The matter came to light when the other Pacific Island country's customs department held some containers due to suspicion.

HONG KONG, CHINA

VAT fraud and invoice manipulation: Company A requested a local bank to send a TT of USD to a UK company for the importation of mobile phones, high value but low volume goods. An invoice showing as VAT free was provided by Company A. Shortly after the transfer, Company A requested to call back the TT. The local branch liaised with their UK head office regarding suspicion that the UK company was avoiding VAT. The bank subsequently lodged an STR. The case demonstrates the importance due diligence by the compliance officer and the modus operandi of a typical MTIC carousel fraud.

REPUBLIC OF KOREA

Over invoicing for VAT fraud: Jewellery wholesalers and retailers issued/received tax receipts when there was no trade in order to get illegal VAT refunds. To do that, they made up false documentary evidence of financial transactions.

Over invoicing for VAT fraud: The Korean government exempts certain jewellery wholesalers and retailers that fit certain conditions from VAT on gold bars used as a raw material for jewels. Wholesalers and retailers exploited the exemption to obtain illegal VAT refund. They disguised tax-free gold bars as taxable ones and exported them to other countries.

Over invoicing: Person A imported computer power equipment with zero-tariff rate from *Company B*. He reported higher import price than the actual price. He wire-transferred the reported price to *Company B*, and *Company B* transferred back the difference between the real price and the reported price to a bank account under the name of *Person A*'s sister in law. In this method, *Person A* embezzled a total of USD 72,063 in 16 transactions.

Related customs fraud cases

Pakistan - *Customs fraud and corruption:* A Karachi based Group of Companies was sponsored by an ex-official of Customs Department and within 3 – 4 years became a leading exporter of leather jackets and polyester stitched fabrics.

Customs & Excise received information that the companies were involved in over-invoicing of low graded exports; claiming inadmissible Customs rebate against fake exports; claiming Sales Tax Refund against fake exports; and misuse of Duty Tax Remission for Exports (DTRE) Scheme which is meant for genuine Manufacturers cum Exporters.

Malaysia - *Customs fraud and use of agents' accounts:* Company A awarded forwarding agent C a contract for shipment of turbine spare parts and related equipment (goods) from country Z for its power plants in Malaysia. The goods imported were subjected to payment of import duties, which are identified against specific tariff codes declared on the Customs Declaration Form. Any incidental expense following the importation is to be paid by the forwarding agent C and it is claimable in full from Company A.

Upon shipments of the goods, forwarding agent C declared all the 4 shipments to the Royal Malaysia Customs on 4 separate Custom Declaration Forms. Subsequently, three of the shipments were exempted from payment of duties due to a pre-endorsed privilege granted

by the government on the selective imported items. Forwarding agent C thus, ended up paying duties for the one remaining shipment. However, an employee of the forwarding agent C, Mr. Y had held back this information from Company A. He forged additional Customs Declaration Forms with falsified contents. In the declarations, the number of shipments of the goods were inflated whilst amount of duties payable were overstated to approximately RM4 million (USD1.11 million). These Customs Declaration Forms with falsified contents were then submitted to Company A for full refunds and were honoured accordingly. Refunds were made in full into forwarding agent C's corporate account.

Thereafter, the money refunded was withdrawn from the corporate account in equal amount to the fraudulent refunds and credited into Mr Y's personal accounts without the knowledge of the forwarding agent C. It was later traced that Mr Y had used the money for his personal investments and purchase of personal assets. Some monies went into accounts of other individuals who were his accomplices and abetted in this fraud.

Republic of Korea - *Under invoicing:* Person A imported sea squirts through Busan Harbor from a Japanese retailer and reported the price as 100 Japanese Yen per kilogram when the actual price was 180 Yen. He underreported the price by a total of KRW 450 million in 75 similar trades and evaded KRW 110 million of customs duties in total.

*****

Abuse Of Non-Profit Organisations/Charities

SRI LANKA

Abuse of NPOs for terrorist financing: The LTTE has used a number of NPOs for terrorist financing. One identified charity used by LTTE is the Tamil Rehabilitation Organisation (TRO). The Sri Lanka FIU has frozen a large number of bank accounts relating to TRO.

PHILIPPINES

Abuse of NPOs to launder proceeds of corruption: The AMLC received a number of STRs from a bank concerning two non-government organisations (NGOs) and a government agency. The bank reported the movements of money and cash by the subjects as "very unusual" – the transactions had no underlying legal or trade obligation, purpose or economic justification.

The government agency is primarily engaged in rural development. PEP A is the authorised cheque signatory for the government agency. The two NGOs have varied purposes, including support all government projects that benefit the poor.

A month before the national election in 2004, and in 2005 the government agency made several large transfers to the NGOs ranging from P20M (USD400,000) to P40M (USD800,000) per transfer. Almost immediately upon receipt of the funds, the NGOs issued cheques made payable to "cash" for the same amount received. The respective senior officers of the two NGOs personally went to the bank to cash the cheques. It is believed that the funds were originally sourced from government funds which were utilised to fund ghost purchases of seeds, including districts which are highly urbanised or with no arable agricultural land, and subsequently siphoned to fund election campaigns.

MALAYSIA

Cooperative abused for money laundering: Mr X is a shareholder and a director of Company M, a money-lending company. Mr. X is also a financial controller of a cooperative body and in-charge of the cooperative's financial affairs. The Cooperative provided a medical care scheme for its members whereby members are entitled to a fully subsidised medical treatment with a range of panel clinics endorsed by the Cooperative. The panel clinics would bill the Cooperative for medical expenses incurred by the members.

The banks submitted STRs on numerous cheques that were drawn from the Cooperative's checking account as payments into Mr X's credit card accounts, as well as to a Company M of which Mr X has a direct interest. The financial intelligence gathered from the STRs was disclosed to the enforcement agency for their investigation.

The investigation revealed that the Cooperative has record of large and long-outstanding medical bills with the panel clinics. Mr X agreed for the payment of the medical bills to be charged to his personal credit cards and to Company M, his intention being to maintain good relationship with the panel clinics as the clinics could be paid sooner. The Cooperative would refund Mr X either in full or in tranches at a later stage via deposits of money into Mr X's credit card accounts. Company M was refunded accordingly by cheques issued by the Cooperative.

This arrangement opens a way for collusion between Mr X and the panel clinics. The panel clinics began to issue false medical bills and charged to Mr X's credit cards and Company M. These fake invoices were co-mingled with other legitimate medical expenses to in order to avoid suspicion and detection. Thereafter, Mr X and his company claimed for refunds on those fraudulent medical bills from the Cooperative. The proceeds were traced to move between Mr X's personal banking accounts and Company M's checking accounts with local banks as well as into funding of Company M's business operations and purchase of personal tangible assets.

CANADA

Abuse of NPOs for Terrorist Financing

As discussed in previous typologies reports, terrorist groups have utilised non-profit organisations (NPO) or charities in order to provide or facilitate:

A cover to falsify records of employment
International travel
The means to identify, recruit and train fighters for "the cause"
A medium to finance terrorist operations
A network to smuggle weapons
A meeting place
An opportunity to network/conspire
Access to mainstream society and funding from individuals and organisations that believe they are funding legitimate causes
Access to corporate offices and communications equipment.

Canadian law enforcement and intelligence agencies have discovered that supporters of a variety of terrorist groups use Canada as a base to raise monies for their causes abroad. These supporters range from loose collections of individuals with limited fundraising capacity to well-organised groups capable of raising substantial sums of money. In some cases, the charity itself was a sham that existed to funnel money to terrorists. However, in other cases the abuse of a charity occurred without the knowledge of donors, or even of members of the management and staff of the charity itself. Besides financial support, some charities have also been used to provide cover and support for the movement of terrorists and illicit arms.

A common means of raising terrorist funds in Canada is through community solicitation and fundraisers, often in the name of a charitable organisation. In some cases, the public is led to believe that they are giving for a good cause, usually to alleviate the poverty or suffering in their homeland. However, in many situations, the donors are sympathetic to a group and its causes and readily give money without questioning its end use.

Canada has been used as a throughway point for terrorist funds to be disbursed through layering schemes that can involve a number of other NPOs, individuals, and commercial entities. An NPO that has status as a registered charity in Canada gains favourable tax treatment and also gains an air of legitimacy in the community.

In some cases of abuse of charities for terrorist financing, charity networks are used to raise and transfer funds. This activity may be under the direction of those in leadership positions in the organisation. In some cases, one individual may act as part of the board of directors or trustees of multiple charities which can legitimately declare transfers of funds between themselves. In other cases, a small number of people may remain on the board of directors in key positions for many years while the rest of the members change. By controlling these positions or leadership, individuals are able to use charities or charitable networks to provide financial support to suspected terrorists.

In these cases, it is sometimes a challenge to determine if the individuals in the charity or the charity itself are responsible for the terrorist financing activity. In some cases, one individual may take control of the charity's finances without the awareness of the rest of the charity or the whole organisation may be aware and approve the ultimate destination of funds gathered through the community's donations and other means of fundraising.

Non-profit organisations used to transfer money to suspected terrorists

Canada reported identification of entities included on the consolidated list issued by the United Nations Security Council 1267 Committee. One of the organisations on the list had an address in Canada and authorities identified bank accounts and three individuals with controlling interest on the property at that address. One of the individuals (A) had a Canadian address that matched one of the addresses provided by the UN and the other two individuals had addresses in two different countries. A search by FINTRAC revealed that the Canadian individual (A) was linked to the organisation noted above, as well as to four other charitable non-profit international organisations with Canadian branches.

Reports received by FINTRAC detail multiple wire transfers sent from locations of concern to the Canadian branch of the above-mentioned charity and to the Canadian individual (A).

This case was identified as a case of potential terrorist financing because of:

- Inclusion on the United Nations Security Council Committee's Consolidated List (1333/2000)
- Media coverage on account holder's activities
- Sending or receiving funds by international transfers from and/or to locations of specific concern
- Possible client relationship to previous crimes

Use of Charities to Move Illicit Items

In other cases, charities have been used to move illicit items with the intention of supporting terrorist activity. Sometimes these illicit items are moved with other legitimate items. These legitimate items might be destined for legitimate or terrorist use. For example, items supposed to go to an orphanage could easily be used at a training camp (i.e. medical equipment, food, blankets, solar panels, etc). The urgency of the need for aid in war-ravaged or conflicted areas allows these organisations easy access into controlled areas.

As an example, charities have been used to move medical supplies and weapons. In one instance Canadian peacekeeping forces were controlling an area in Country K. A delivery truck identified with markings of an international aid organisation was randomly searched. The searchers discovered a shipment of weapons hidden behind medical supplies.

*****

Structuring ("Smurfing")

CHINESE TAIPEI

Structured transactions linked to bank fraud: A bank teller, Lai, targeted five of his customers and their fixed bank accounts in order to take advantage of one common feature: they had large sums of money but infrequent withdrawals. First, without the knowledge or permission of the customers Lai applied for credit cards in the name of these five accounts and then opened ten bank accounts in other banks in his own name. Then, using the visa card, he transferred money in small amounts over a period of time from these fixed accounts to his new-opened accounts. The sum of transferred money reached NT$ 23 million. To appropriate all the money he has transferred from his customers, he used various methods of money laundering, such as withdrawal from ATM, wire remittance, underground banking, stock purchase and overseas remittance. Lai was arrested after bank's report of his suspicious transactions.

INDONESIA

Structuring to avoid reporting thresholds: In March 2005, there were twelve (12) incoming transfers from Country J, known as a tax haven country, in amount of USD9,500 each into Mr. A's account at a foreign bank in Jakarta. After a money transfer was credited to his account, on the following day, he directly cashed the fund amounting to USD 9.500 each. This individual appears to be structuring transfers to avoid Cash Transaction Reports (CTRs) in Country J.

REPUBLIC OF KOREA

Structuring foreign wire transfers: Person A, president of a company importing cubic crystals, underreported the import price in 76 transactions and remitted the difference between the reported price and the real price in the name of a third party. *Person A* also made foreign currency transactions in the name of a third party without reporting to the Governor of Bank of Korea or the head of the foreign exchange bank to make investment in a titanium mine in a foreign country or when he made foreign currency deposits at foreign banks.

Person A divided the amount of money he remitted in several smaller amounts under USD 10,000 when he made the transactions in borrowed names. In conducting such transactions, *Person A* exploited the provision that remittance of less than USD 20,000 by a resident is exempt from the duty to submit documents proving the source of the foreign currency and is not reported to the National Tax Service.

HONG KONG, CHINA

Non-residents receiving structured remittances: In October 2006 an STR was filed against Ms X who was a resident of Jurisdiction A. In September 2006 she visited Hong Kong and opened a bank account by depositing USD140,000 in cash. Within one month, a total deposit of USD1,030,633 was made to her account. Majority of the deposits were made by means of structured remittances in USD9,972 from Jurisdiction B. The account was used

purely as a conduit, nearly all the money went straight out again. It was found that Ms X stopped to use the bank account once the money had been remitted to her account and withdrawn. Ms X was subsequently arrested for money laundering offence. It is an example of a non resident account being opened to receive structured remittances from overseas in avoiding the threshold of USD10,000 which may cause STR to be filed in some jurisdictions.

SINGAPORE

Structured transactions related to internet scams: Mr. Y received an email solicitation to apply online for the post of a "transaction manager" stating that he could earn thousands of dollars in commissions by simply receiving money and thereafter remitting it to Russia and Latvia. The solicitation was from a criminal syndicate who claimed falsely to be the representatives of Financial Investment Advisory Services ("FIAS"). FIAS, a bona fide organisation linked to the World Bank.

The criminal syndicate had set up a counterfeit website, www.fias.sg, which looked like the bona fide FIAS website www.fias.net. At the counterfeit website www.fias.sg, persons were recruited to launder illegal proceeds obtained through a bank fraud in Australia.

Upon his employment as a "transaction manager", Mr. Y, was instructed to receive money from Australia via remittance companies such as Western Union, Travelex and MoneyGram. Mr. Y was asked to send the money to Russia or Latvia via telegraphic transfer through the banks – likely routed back to the criminal syndicate via other "transaction managers" in Russia and Latvia.

Mr. Y was allowed to keep 5% of the amount remitted as his commission; the average amount per remittance was SD5000, equalling a commission of SD250 for each transaction. Mr. Y had performed at least 3 to 4 transactions per week and received up to SD1,000 in illegal proceeds.

The money which was remitted to Mr. Y was in fact the proceeds of a highly sophisticated internet scam. The victims were lured to counterfeit internet banking websites and requested to enter their user identification and password. The syndicate then gained access to the victims' bank accounts in Australia and made unauthorised withdrawals and fund transfers.

THAILAND

Structuring transactions related to heroin ring: AMLO received an STR made by a bank that Miss S, extra-marital wife of Mr. P, conducted many cash deposits and withdrawals involving 1-1.9 million baht in each transaction and taking only banknotes of small denominations to avoid reporting to the AMLO. The couple together held 70 accounts at various banks totalling a large amount of money. Mr. P had a history of drug involvement while Miss S had no such history.

Investigations found that the couple were major drug traffickers with direct contact with the Wa. The couple were arrested together with 3 other people and exhibits including 74 kilograms of heroine, Thai currency worth 15,463,520 baht, US currency worth 114,251 dollars and bank accounts worth 12,224,993 baht. Searches of 13 houses of people believed to have acted for the disposal of the couple's drug proceeds found 7,325,810 baht worth of cash and 9 bank books worth together 39,124,923 baht and many cars.

Structuring drug proceeds through discount stores: Mrs. O, a resident of Bangkok, who was under suspicion of drug involvement, conducted financial transactions with branches of banks located at discount stores. These frequent transactions did not involve large amounts of money. It was between 180,000-600,000 baht each time. Later, the woman was arrested

together with Mr. M and exhibits which included 60,000 amphetamine pills, 13 grams of ice, 1 motorbike, cash worth 6,000 baht, 7 gold objects, 1 notebook computer and 2 cash cards.

*****

Wire Transfers

THAILAND

Wire transfers to nominee accounts: Mr. S, a rancher in Tak Province, opened an account and got an ATM card with a bank in that province. Later, deposits/transfers were made into the account from other provinces, totalling 5.48 million baht in 1 month. During that same period, more than 250 withdrawals through the ATM were made from the account in Supanburi Province. It is surmised that Mr. S has been employed to open the account by another person who wanted to block investigation of his own financial path. Incidentally, Tak and Supanburi are at high risk of drug involvement.

PAKISTAN

Wire transfers to shell companies: Pakistan received intelligence of alleged money laundering or possibly terrorist financing by a person named as Alpha and his real brother Beta. It was reported that accused have transferred over £270,000 from Country B to Pakistan.

Beta opened a bank in the name of a firm M/S XYZ Lahore, Pakistan. The company was incorporated, however no physical business activity was observed. Over £270,000 was received from a firm M/S UVW located in Country B in the bank account of M/S XYZ. It was later discovered that the firm M/S UVW is owned/related to Alpha, who is the brother of Beta, the beneficiary of the remittance.

Over £267,000 was immediately onward transferred by Beta to Alpha in his bank account in Lahore. Major payments were made within a very short span of time from the Bank account of Alpha from varying recipients/beneficiaries including the wife of Alpha and Alpha himself, using cheques, payments, ATM withdrawals and other modes.

Alpha claimed that he borrowed the money from his friend at Country B, and later he returned the money through hawala/hundi to the lender at Country B. Further funnelling of funds amounting to over £194,000 were recovered from Alpha during enquiry. A number of other bank accounts were also discovered owned by Alpha and Beta. All these accounts were linked with funds owned and related to Alpha, transacted by him in order to evade the identity of source and origin of funds.

*****

Investment In Capital Markets

MACAO, CHINA

Investment of unexplained funds in the capital market: Ms C declared herself as shareholder of a thread factory. Within a short period of time, there were cheques and cash in large denominations deposited into her account for investment in the Hong Kong stock exchange market. None of the cheques received were drawn in the name of the thread factory, instead they were drawn from an account of a jewellery store. As Ms C. declined to disclose the source of the funds and none of these cheques originated from the declared business, the bank decided to file an STR.

MALAYSIA

Stock manipulation and use of nominees: Mr T. a controlling shareholder of a company listed on the Kuala Lumpur Stock Exchange (KLSE) used 12 investors as a front for him to manipulate stock. Between March and May 2002, the price of XYZ had increased significantly from a low of RM1.00 to a high of RM6.00. The group of 12 investors had traded heavily on XYZ shares via 20 accounts maintained at 8 different stock broking firms.

Investigation revealed that 80% of the total volumes done for XYZ during the relevant period were carried out by these 12 investors with high instances of NCBO (no-change-in-beneficial-ownership) trades.

Proceeds of approximately RM50 million (USD14.5 million) were generated and deposited into the respective bank accounts of the 12 investors maintained at ABC Bank. In order to layer the illicit funds they were then immediately transferred to AAA Company before moving to MMM Company and finally to ZZZ Company (ZZZ later revealed to be owned by members of Mr T's family). The accounts of AAA, MMM and ZZZ were also maintained at the same ABC Bank and branch.

*****

Use Of Shell Companies/Corporations

HONG KONG, CHINA

In early 2004, the account of a British Virgin Islands (BVI) company (utilising the address of an international accountancy firm) recorded multi-million HK dollar cheque and cash deposits, dissipated means of cashier's orders to four other corporate entities. The directors of the BVI company were a married couple found also to be the directors of a locally listed company.

It was discovered that the couple's BVI company held substantial shares in the listed company and these shares had been used as collateral for a loan. The couple was successfully prosecuted for failing to advise the Regulator regarding a change in their holding in the listed company.

This case highlights the use of an offshore shell company account operated by a corporate service provider; fund layering and the use of cashiers orders (in an attempt to complicate the audit trail); to veil the activities of the beneficial owners.

REPUBLIC OF KOREA

Sham loans from shell companies: *Person B*, a controlling shareholder of *Company A*, obtained a bank loan with *Company A's* bank deposit as collateral. He used the loan to let *Person C* to take over *Company A*. *Person B* then obtained KRW 4 billion of additional loan by using *Company A's* land as a collateral and used the money to acquire managerial control over *Company D*. *Person B* then used proceeds from paid-in capital increase of *Company D* to acquire 100% ownership of *Company E*, which was only a shell company.

Sham business activity of a shell company: *Person A* took over *Internet Shopping Mall B*, a shell company, and gathered credit card holders in dire need of cash. *Person A* generated sales slips using a program of *Company C* pretending that the card holders purchased goods from the shopping mall when there was no such transaction. *Person A* sent the sales slips to credit card companies. Unaware of such scheme, the credit card companies made payment to *Company C*. *Company C* then subtracted its fees and

forwarded the rest to the bank account of the shopping mall. *Person A* obtained KRW 2.4 billion of illegal proceeds in total from 15 credit card companies.

MACAO, CHINA

Wire transfer to a shell company: Mr. T, who claimed to be a manager of a restaurant at the time of account opening, received frequent inward wire transfers from different countries denominated in USD. Upon receiving these USD payments, Mr. T would immediately convert them into HKD and withdraw them in lump sums of cash. Mr. T declared that these funds were for the settlement of goods, sometimes received on behalf of a shoe company located in Mainland China. In fact, a portion of the funds were deposited into an account of a construction material company. Since the frequent wire transfers in Mr. T's account did not correspond with his background, the bank reported the case to the Judiciary Police.

CHINESE TAIPEI

Nominees used to establish shell companies: Mr. Wang was the president of Enterprise LB, who utilised his family members, friends, employees of the enterprise to be the nominal president of 68 shell companies. By means of long term investing in, lending money to, being guarantor for, issuing company promissory note for, buying real estate from these companies, paying false trading loan in advance, buying company debts issued by these companies, and making false deals with these companies to abstract capital from the Enterprise A.

He also utilised false dealing data between shell companies to borrow money from banks, instructed the financial institution of the enterprise to lend money to these companies to make lose of Enterprise A. By way of the methods afore said, Mr. Wang abstract NTD 66,000,000,000 from the enterprise, to cheat NTD 131,000,000 from banks. He transferred NTD 564,000,000 from the enterprise to his account, and launder NTD 147,000,000 to overseas.

*****

Use Of Offshore Banks/Companies (trust and company service providers)

REPUBLIC OF KOREA

Offshore company and stock manipulation: *Mutual Savings Bank C* was in severe financial straits and needed a paid-in capital increase to survive but shareholders were not willing to provide capital for the bank. Being aware of such a situation, *Person B*, head of *Construction Company A*, embezzled a loan worth KRW24.7billion from *Company A* to set up *Private Equity Fund D*, a shell company located offshore in Delaware, US.

Person B then made an investment worth KRW34billion in the *Mutual Savings Bank C* through *Private Equity Fund D* by presenting *D* as a legitimate investment firm in the U.S. with USD 100 million of capital. After acquiring managerial control over the bank with the investment, *Person B* got an illegal loan worth KRW25billion from the bank. He also gained illegal profit of KRW300million by manipulating the share price.

PAKISTAN

Suspected money laundering of the proceeds of narcotics smuggling: 'Mr. X' has been convicted for narcotics offences in Pakistan and his assets amounting to Rs.867 million already forfeited under court orders.

In the first phase large sums of money were placed in the financial system, by routing monies through companies based outside the UK, and the onwards use of monies through intermediaries. These funds were paid through an offshore company 'Y' incorporated in the Bahamas, totalling GBP3.8 million, a large portion which was placed into the financial system by way of cash deposits.

In the second phase, monies were transferred through accounts of defendants in the UK into different bank accounts in Spain.

In the third phase they converted a large amount of cash into dollar banker's drafts at an exchange bureau in London, which was subsequently paid into another defendant's (W Associates) account in the Bank of Ireland. A large portion of this money was again transferred into the account of another defendant at the Bank of China. Major portion of this amount was then transferred to this defendant's account in the Royal Bank of Scotland.

The involvement of the narcotics money is revealed through a notice to the Customs and Excise of the UK given by a Pakistani advocate of an intermediary (Mr. Z) of the son of the convicted narcotics smuggler (Mr.X), demanding GB Pounds 325,000 to be paid to 'Mr. Z', which have been purported to be the investment made by the 'Mr. Z', with 'W Associates'.

*****

Use Of Nominees, Trusts, Family Members Or Third Parties ('onshore')

AUSTRALIA

Third parties used to send bank drafts offshore: A large number of bank drafts valued at between AUD8,000 – 9,000 were purchased in the names of a number of different entities on behalf of the person of interest. More than AUD2.2 million worth of bank drafts were purchased over a 12 month period and it was suspected that these drafts were to be used for a large import of precursor chemicals into Australia. Bank drafts purchased in Australia were being presented at various banks in Greece and deposited into bank accounts of the person of interest.

The bank drafts were purchased below AUD10,000 in order to avoid the reporting threshold and were purchased under false names and made out to false payees. After the drafts were purchased, the purchasers would sign the draft over to the intended payee who was based in Greece. The drafts were then either posted or couriered to Greece and deposited into a Greek account by the intended recipient.

Bank drafts purchased in third party names to evade tax: STRs indicated that the owner of a restaurant was purchasing multiple international bank drafts with cash, in amounts just below the AUD10,000 reporting threshold. The drafts were purchased in the names of family, friends and staff members and signed with different signatures. Investigations identified that the restaurant owner was purchasing USD bank drafts with cash in false names and sending these to relatives overseas.

In order to avoid tax, the owners had been systematically skimming profits from the restaurant and manipulating the cash registers to give incorrect sales readouts. The skimmed funds were then sent to relatives overseas. The money was returned to Australia as "loans" and interest on these "loans" was claimed as tax deductions. As a result of the investigations, the business owners were subject to approximately AUD8.4 million in tax and penalties.

REPUBLIC OF KOREA

Trade based money laundering and use of nominees: *Person A* imported Chinese agricultural products and sold them in the domestic market under the name of *Trade Company B*. He conspired with an employee of a warehouse in the bonded area to exchange high-tariff items with low-tariff items in the warehouse. He gained KRW3.1billion by evading customs duties in 195 such trades, and remitted the price of the import and the illegal proceeds to China in the name of his girlfriend and her daughter.

MALAYSIA

Use of nominees for bank fraud: Mr. Z was a branch manager of a local bank. He manipulates his position as a branch manager to commit criminal breach of trust by liquidating fixed deposit savings of his branch's customers. Mr. Z liquidated approximately RM19 million (USD 5 million) over a period of three years.

Mr. Z transferred the monies to five accounts belonging to five different customers at his branch. Subsequently, RM18million was transferred out of these five accounts to three other major accounts that belong to three different individuals, Mr. L, Mr. N and Mr. T. Investigations also revealed that Mr L, Mr. N and Mr. T were involved in illegal gambling activities (illegal 4 Digits betting). These three individuals claimed that all the monies transferred into their accounts by Mr. Z were payments from Mr. Z for his bets. However, investigation further revealed that the funds were transferred to other accounts in different banks and eventually withdrawn. These three individuals were later found to be collaborating with Mr. Z in his scam.

Mr. Z was arrested and charged for criminal breach of trust while Mr. L, Mr. N and Mr. T were charged for committing money laundering under Section 4 (1) of the AMLA.

HONG KONG, CHINA

During the financial investigation of a pirated optical disc case, a safe deposit box held in the name of Ms X was revealed. Her sister, Ms Y, one of the masterminds of the syndicate, was the authorised person of the safe deposit box. Documents, cash and valuables such as watches, jewellery worth about HKD0.21million were found inside. Investigation revealed that only Ms Y had access to the safe deposit box. It is obvious that Ms Y manipulated her family members to conceal her proceeds and to disguise the real ownership of the valuables and cash.

*****

Use Of "Gatekeepers" Professional Services (lawyers, accountants, brokers etc)

VANUATU

Use of lawyer as professional front: The VFIU is assisting another foreign jurisdiction where funds from a fraud in that country were transferred to a Vanuatu bank account. Enquiries revealed that the bank accounts were opened using a local lawyer as a service provider and the proceeds of the fraudulent activity were deposited with the Vanuatu banking institution masked as "business sales". The offender via his local service provider advised the bank that the funds would be used to pay business related expenditure but instead they were withdrawn in small amounts in several European countries using an international debit card.

CANADA

Use of lawyer's trust accounts: An individual used a law firm to purchase property through the law firm's trust account using bank drafts purchased overseas from the proceeds of criminal activity. The same law firm was used to set up family trust accounts and various companies.

Use of legal arrangements for real estate: Accountants and legal professionals helped organise several loans and set up the various legal arrangements needed for the purchase of real estate. Non-trading real estate companies were set up and then used to purchase real estate on behalf of the client. To further insulate the client from the laundering scheme, the accountants and legal professionals actively participated in the management of these companies.

Lawyers used to establish offshore companies: A lawyer was employed by an international drug importer to launder the proceeds of his criminal activity. The lawyer established a web of offshore companies in a country with weak corporate regulations on behalf of his client. These companies were then used to hide the movement of the proceeds of crime case. He also cooperated with several other lawyers for the use of their trust accounts to receive cash and transfer funds.

Use of lawyer's trust accounts: On the instruction of his drug-trafficking client, a lawyer deposited money into his trust account and then used this money to make regular mortgage payments from this account for properties owned by the trafficker. The lawyer admitted that he accepted deposits and administered payments, but claimed no knowledge of the origin of the funds.

Collusion between lawyer and mortgage broker to avoid STRs: A common law couple used a variety of methods to launder revenue from cocaine trafficking, including depositing money in financial institutions, buying real estate, and purchasing vehicles. The financial institution staff facilitated numerous transactions and even advised the couple's nominees how to conduct transactions in a way that would ostensibly reduce any suspicion. A mortgage broker and a lawyer helped with the purchase and financing of real property, and an accountant provided advice on investing funds in order to raise as little suspicion as possible. A car was also purchased with cash at a dealership.

Lawyers used as professional launderers: A drug trafficker, who headed an organisation importing narcotics into Canada from Country A, employed a lawyer to launder the proceeds of his operation. To do so, the lawyer established a web of offshore corporate entities incorporated in Country B, where scrutiny of ownership, records and finances is not stringent. A local management company in Country C administered these companies. These entities were used to camouflage the movement of illicit funds, the acquisition of assets and the financing of criminal activities. The main trafficker in this case held 100 percent of the bearer share capital of these offshore entities.

In Canada, a distinct group of persons and companies without any apparent association to the main trafficker transferred large amounts of money to Country C. There, the funds were deposited in, or transited through the trafficker's offshore companies. This same group also transferred large amounts of money to a person in Country D, who was later found to be responsible for drug shipments destined for Canada.

Several other lawyers and their trust accounts were used to receive cash and transfer funds, ostensibly for the benefit of commercial clients in Canada. When law enforcement agencies approached them during the investigation, many of these lawyers cited "privilege" in their refusal to cooperate. Concurrently, the main lawyer in this case established a separate

similar network, which included other lawyers' trust accounts, to purchase assets and place funds in vehicles and instruments designed to mask the beneficial owner's identity.

In 2005, this lawyer and three other accomplices pled guilty to money laundering and to possession of proceeds of crime in Canada and received a combined fine in lieu of forfeiture that totalled approximately $2.7 million.

AUSTRALIA

Gatekeepers / TBML / identity fraud: Mr A was involved in a multi million dollar tax fraud lodging fraudulent Goods and Services Tax (GST) claims. He used stolen and false identities and forged documentation to open and operate bank accounts, obtain credit cards, register companies and open serviced and virtual offices.

Following the GST fraud, Mr A's company's received the proceeds of the fraud and subsequently transferred the funds into other company accounts and various stolen identity accounts. These funds were moved constantly to have the appearance of being legitimate. Mr A also falsified trade documents to launder money between the companies controlled by him.

Mr A also employed international accounting firms using stolen identities and provided forged documentation to help undertake the fraud. He used these gatekeepers to help distance himself from the underlying fraud. Once the proceeds had been layered, Mr A would then withdraw or spend funds via automatic teller machines, business cheques, credit cards, cash cheques, electronic debit system, direct transfers to other parties and cash withdrawals. The cash withdrawals were varied in amounts and were both structured and non-structured.

FIJI

Lawyer used to establish an offshore shell company: A case was reported by a solicitor in Fiji where a shelf company from Hong Kong purchased 75% shares of a local company. The company wired funds from Australia as deposits to the solicitor's Trust account without conducting any due diligence. The local shareholders were flown to Australia to secure the deal and all shares purchased were transferred to the remaining local shareholder. A total of FJD1.5 million was sent to the solicitor's account. Investigations by foreign law enforcement authorities reveal the Hong Kong Company to be non-existent. Furthermore, the company has been subject to investigations by other international law enforcement authorities relating to lottery fraud. Investigations are continuing.

JAPAN

Lawyer and false loans and contracts: A lawyer, who received a consultation from criminals to avoid confiscation of the crime proceeds, advised criminals to counterfeit a loan contract to pretend that criminals borrowed money from their acquaintance, and made an illegal procedure for attachment of property (above-mentioned crime proceeds) at Court.

*****

Use Of Foreign Bank Accounts

HONG KONG, CHINA

Use of internet fraud to access third party foreign accounts: This is a variant on the classic 419 West African Frauds. In this instance, victims in South America and Asia received communications advising they were about to receive significant plausible inheritances from overseas. As such, they were induced to release advance fees to facilitate the release of the inheritances. The "advance fee" payments were paid into nominee accounts in Hong Kong, opened by non-residents from South Asia.

The investigation revealed that prior to the fraud the victims had been thoroughly researched by the syndicate. The nominee account holders were arrested upon their return to Hong Kong. A portion of USD4 million in advance fees was recovered and both nominee account holders were subsequently sentenced to terms of imprisonment for their involvement in the scheme.

This highlights the continuing risk of non-resident accounts being used as disbursement accounts for crime proceeds.

REPUBLIC OF KOREA

Foreign shell company accounts: *Person A* set up a shell company in the US to launder money. He also set up many other shell companies in Hong Kong, China, and the US, and established bank accounts under the names of the shell companies. He concealed illegal funds by making several transactions using such accounts until the fund ultimately reached the shell company in the US.

PAKISTAN

Tax evasion and laundering committed offshore: In the bank account of suspect C deposit/receipts of over GBP561,000 were traced out of which over GBP510,000 was remitted from Jurisdiction B. The bank account was found practically operated by a money changer, who was authorised to make transactions on behalf of the suspect C. The cheque book of the account owned by the suspect was kept in possession and used by the money changer.

A bank account owned by suspect D was traced in which deposit/receipts of over GBP445,000 were identified. The sources of these deposits were located in Jurisdiction B and others.

The personal bank account of money changer suspect E was analysed and showed a remittance of over GBP222,000 received from Jurisdiction B, over GBP116,657 was found locally deposited in his personal account. No legitimate reason for transacting the funds into the personal account instead of company accounts could be provided.

A bank account of suspect F was traced in which an amount of over SD1,651,000 was found received from overseas. No legitimate relationship of the account holder with origin, source, reason and utilisation of funds was provided by the suspect.

PHILIPPINES

Gatekeepers/ wire transfers / corruption: Mr. F was a retired public relations expert, hired by Company X, a local construction firm, to secure and ensure its selection by the government agency to undertake a government project to build a transport facility intended to promote tourism. Company X had a foreign company as partner known as Company Z.

As conduits for funds intended to bribe public officials to ensure selection during the bidding process, Mr. F opened several accounts with a bank located in Country A under the account name of two (2) foreign-based shell companies known as Companies 1 and 2, respectively. Mr. F was the designated signatory for the accounts for both companies.

CTR data indicated that the accounts of Company 1 and Company 2 were recipients of $200,000 every month for a period of 10 months, all wire transferred on the 15th of every month, and with a total accumulated amount totalling $2,000,000. CTR data further revealed that the amounts, after being credited to the accounts of either Company 1 or 2, were further wire transferred to accounts with local banks, including accounts owned and maintained by the owners of Company X. Thereafter, the accounts of Company 1 and 2 with the bank in Country A were closed.

Company X was successful in securing the government contract. Investigation revealed that a big portion of the $2,000,000 was utilised to bribe government officials to obtain the contract.

AUSTRALIA

Wire transfers to foreign accounts using "smurfs": A crime group was involved in a cocaine importation from the US using a parcel courier service. Prior to each importation, wire transfers were sent to accounts in the US. These transfers were conducted by individuals who were recruited by the crime group at night clubs to send money on their behalf. The funds were sent to individuals and company accounts held in the US in amounts ranging from AUD6,000 to AUD19,995. The currency of the transactions also alternated between USD and AUD.

*****

Use Of Credit Cards, Cheques, Promissory Notes Etc

FIJI

Use of foreign EFTPOS service to remit funds: A restaurant used credit card payment facilities to charge local transactions in foreign currency. The EFTPOS terminal in this restaurant did not belong to either of the credit card acquirers in Fiji. The credit card payments conducted through this restaurant were being channelled directly to a bank account maintained and controlled by the restaurant owners in overseas.

CANADA

Credit card cash advances used to get rid of cash: Credit cards were used to provide cash advances to customers of a strip club for prostitution services. A service charge of 10 per cent was requested for this service. If, for example, a client requested $100, $110 was charged on the credit card and the client received $100 cash. At the end of the month all these cash advances or credit card charges would get deposited electronically into the business bank account of the club. This can be described as an ideal method to get rid of excess cash.

MALAYSIA

Card skimming and cash sales of goods: The suspect, Ms. A, worked as a Sales Representative in a boutique in Kuala Lumpur. She stole pertinent credit card information from customers who made purchases in the boutique, holders of gold and platinum credit cards. Ms. A recorded the credit card number, its expiry date as well as the 3 digits Card Verification Value (CVV) number listed behind the credit card.

Using the credit card information, Ms. A purchased computers and computers components via the internet, impersonating as the actual credit card holders. The computers were subsequently sold at attractive prices to her fellow colleagues and friends. Those who purchased the computers from Ms. A were required to make the payment in cash into Ms A's account via the cash deposit machine.

*****

Purchase Of Portable Or High Value Commodities (Gems, Precious Metals)

CANADA

Use of diamonds as monetary instrument: A money laundering investigation was initiated after the seizure of USD600,000 at an airport during a random search. Subsequent investigation revealed that the subject was operating two money service businesses (MSBs) with jewellery workshops in the back. A search of the MSBs revealed thousands of high-quality diamonds. Information obtained following the seizure revealed a complex international money laundering network involving foreign diamond suppliers. Total payments of USD7.4 million were made to two diamond suppliers, one located in Europe and the other in the Middle East. The seized diamonds were being used as monetary instruments to move currency across international borders.

Drug proceeds used to pay for diamonds: A group was revealed to be involved in money laundering activities and marijuana trafficking. The group was also laundering criminal proceeds from other criminal organisations. A link was established between the group and a diamond supplier in the Middle East. Between July and December 2002, a total of $1.2 million was transferred by wire to the diamond supplier. The diamonds were then sent to the group's contact overseas.

SINGAPORE

High value electronic gadgets: Mr X posted on the internet the sale of electronic gadgets at exceptionally cheap prices. Numerous victims from overseas were cheated of more than SD2 million for the purchase of electronic gadgets. He had also registered a business to add credibility to his schemes. The unsuspecting victims would order the gadgets in bulk and transfer the monies (ranging from SD771 to SD143,779) into the bank account of the business operated by Mr X but the goods were either not delivered or only in part.

Mr X would immediately withdraw the proceeds collected from the victims and would use part of the proceeds to purchase the electronic gadgets at local retailers and shipped them to some of the customers. He made partial refunds to a number of victims and paid off some of his debts, creating a false legitimacy in perpetuating the scheme. He would also spend a portion of the illegal proceeds on himself and this included the acquisition of two vehicles under his name and a third for his wife. A sum of SD25,000 was seized from the sale of the vehicles.

Mr X was eventually charged with a number of charges for fraud and money laundering. The case is was on-going in October 2007 and pending trial.

*****

Association With Corruption
(proceeds & corruption of AML/CFT measures)

INDONESIA

Corruption related to defrauding a housing scheme: In August 2004 Mr. S, a high ranking Indonesian Army officer, opened a time deposit in Bank B in an amount equivalent to USD 11 million. The funds were derived from the Army's Compulsory Housing Contribution (TWP) for soldiers. In October 2004, there was an agreement between the Indonesian Army and Mr. S that he would obtain funds from overseas to build homes for soldiers through a foundation established by Mr S. In order to attract both domestic and foreign assistance, the army provided Rp100billion in a time (fixed) deposit to the foundation. Before the fixed term deposit could reach maturity, Mr. N, Chairman of the foundation withdrew the funds and sent the money to an account held jointly by Mr S and Mr N with Bank M. The funds were then invested elsewhere and used for their personal gain.

Wire transfers of corruption payments: A private company, A Ltd, submitted a business loan proposal to Bank C. This company was appointed by the head of the Indonesian Coordinating Investment Agencies (BKPM) to conduct this large government project called "The Indonesian Investment Year" (IIY project) totalling Rp33billion (USD3,600,000). Bank C endorsed the loan for the full amount of Rp27billion (USD3,000,000). Part of the disbursement loan, estimated as Rp9,650,000,000, was directly remitted to A Ltd's account. Some of the money, Rp6.7billion (USD75,000), was directly sent into Mr. B's account identified as a BKPM officer. Mr B. overbooked Rp6,400,000 (USD70,000) to the head of BKPM's account namely Mr. T. Based on Mr. T's account record, it was found that a part of the money was cashed and transferred to his account in other two banks as well as used to pay his credit card bill. The funds which initially sent by A Ltd was used entirely for Mr.T's personal gain. Based on the investigation conducted by the Anti-Corruption Commission, it was recognised that A Ltd has a close relationship with Mr. T and was directly appointed by Mr. T to conduct the IIY project without the bidding process. As a result of court proceedings, Mr. T was punished for the corruption crime by 6 years imprisonment.

Use of travellers' cheques for ML: Mr. X, a high ranking officer came to a government bank in order to sell a number of travellers' cheques issued by government bank in total amount of Rp1billion (USD110,000). He also directly deposited some of the money to his saving account and transferred money to his wife's account in another bank. It was suspected that travellers' cheques were related with the bribery activity. It has been alleged that travellers' cheques issued by the government banks in Indonesia are commonly used to conduct bribery.

Investment of state monies into personal account: A provincial government treasurer withdrew Rp12billion (USD1.3 million) from a provincial government account at a local bank. Subsequently, the treasurer directly deposited all of the funds to his saving account at the same bank. As a result, the interest income received from the bank was Rp50million in every month. It was notified that he regularly took this interest income for his personal gain.

Investment of state monies into personal account: In April 2006, a high ranking provincial government officer, Mr.X, withdrew two provincial government's current accounts by using two cheques totally in amount of Rp4billion. He then converted these provincial government funds to become a term deposit under his name at the same bank with the purpose of obtaining the interest income for his personal gain.

HONG KONG, CHINA

Private sector corruption and use of bank and securities account: Mr X and Mr Y were brothers and respectively the Chairman and Executive Director of a listed company in Hong Kong. The company controlled a number of subsidiaries. In early 2001, Mr Y, the Executive Director, signed a 4-year service contract with Mr W on behalf of one of the subsidiaries for the procurement of business from Mainland China. Under the contract, Mr W was entitled to receive commission amounting to 1% of the net procurement amount of the listed company. However, Mr W was in fact employed by the mother of both Mr X and Mr Y.

Between April 2001 and April 2003, two of the subsidiaries paid Mr W about HKD50.5 million by issuing 10 cheques. Nine of which were signed by Mr X and Mr Y while the tenth was signed by Mr Y and a managerial staff. The proceeds were later transferred into bank and securities accounts operated by their mother. Between November 2002 and February 2003, their mother transferred HKD45 million to a company owned by Mr X.

The original allegation was that advantages were offered to the Financial Controller for securing his assistance in enabling these transfers to take place. Both Mr X and Mr Y were convicted after trial of 3 counts of conspiracy to steal and 2 counts of conspiracy to defraud and both were sentenced to six years imprisonment. Their mother absconded and a warrant had been issued for her arrest.

Private sector corruption and use of remittance: Mr A was the Chairman of a listed company and Mr B was the proprietor of a trading company. During the course of the 2000 annual audit, the Financial Controller of the listed company, upon the instruction of Mr A, submitted a false agreement to the auditor of the listed company. Between February and March 2001, Mr A signed a total of seven cheques totalling HKD20.8 million and transferred the same from the listed company's account into the account of Mr B. Subsequently, Mr B returned some of the money to the listed company account while the remainder was remitted to accounts in Macau via four other persons. The original allegation was that Mr A conspired with other members of the listed company to accept advantages from the proprietor of a Cambodian company as a reward for the acquisition of the latter's company.

Mr A was convicted after trial of seven counts of theft, four counts of furnishing false information, one count of publishing a false statement, one count of making a false instrument, four counts of using a false instrument and one count of making a false statement to an auditor. He was sentenced to six years imprisonment. Mr B was convicted after trial of two counts of dealing with property known or believed to represent the proceeds of an indictable offence. He was sentenced to 3 years imprisonment.

Corruption funds remitted to a 3rd jurisdiction by underground banking: Information from an STR revealed that a PEP from a jurisdiction X had an investment account at a local bank. The account's balance was well in excess of what could be expected from the PEP's identified legitimate salary. Enquiries showed that the PEP came to Hong Kong on a number of occasions for very short lengths of time; during these visits he deposited large sums of cash into the account. The account also showed payments from what are believed to be unregistered remittance agents.

The PEP was subsequently arrested for corruption in the Jurisdiction X. Using Hong Kong's "Absconder Proceedings" legislation the funds in the PEP's bank account in Hong Kong (some USD8 Million) were then made subject of a restraint order.

REPUBLIC OF KOREA

Co-mingling corrupt proceeds with business funds: *Congressman A* of *Region B* promised several persons who wanted to run in mayoral elections in the region to help them get nomination from *Party C*. The congressman received KRW500million of illegal political funds from them. He used the name of a third party to remit KRW200million (about USD211,000) of the illegal fund to an account under the name of *Person D*, owner of a restaurant near the capitol building. He tried to disguise the illegal political funds as legal incomes of the restaurant owned by *Person D*. *Person E*, the congressman's secretary, and *Person D* visited a bank near the National Assembly building and withdrew all the KRW200million in cash in two transactions. On the same day, they deposited the money in another bank account under the name of *Person D*. *Person E* then withdrew KRW200million in cash in five transactions.

MALAYSIA

Wire transferring corruption proceeds: Mr. A, a diplomat attached with a foreign embassy in Malaysia, had a bank account that received regular cash deposits from various parties, subsequently followed by large cash withdrawals. The pattern of transactions was unusual for someone working in an embassy and who has a fixed salary income. Mr A also made various telegraphic transfers to his son studying in Europe.

The investigation conducted by the Anti-Corruption Body of the home country revealed that Mr. A was involved in charging illegal fees to passport applicants during his tenure. Mr A was charged for graft where he was found guilty and sentenced to 29 months imprisonment.

PAKISTAN

Laundering proceeds of corruption through real estate, etc: Mr. AB, who was from a poor family, joined a public sector department in a clerical position. During his appointments as support staff with senior officers of the department, he exercised undue influence and received illegal gratification. A complaint was received in the National Accountability Bureau about his corrupt practices. Investigations revealed that during his 16 years of service, Mr. AB accumulated assets in the form of real estate, bank accounts and savings certificates in public limited companies from the proceeds of corruption. He used the names of his family members to acquire assets. These assets were beyond his known sources of income.

CHINESE TAIPEI

Corruption, real estate, nominees: A1 was a prosecutor for the district prosecutor's office, and was connected with A2. In Feb, 2005, Company B1, for which A2 is the principal, was involved in litigation with Company B2 for NTD 43.5 million under a sales contract. A2 attempted to force B2 through filing lawsuit. The criminal plaint originally intended against the principal of Company B2 was transferred to the prosecutor's office where A1 served and A1 was put in charge of the case. A1 immediately commanded the police to initiate investigation. The police applied for a search warrant, but were refused. A1 signed a warrant for arrest of the principal of company B2. A1 ordered the police to seize important documents of B2, including computers, without a search warrant. A1 allowed A2 to download computer data from the seized computers. A2 then transferred the title for a house to A1's father-in-law designated by A1, at a price totalling NTD9,831,401 after evaluation, but A1 only paid NTD 6,000,000. A1 obtained illegal profit of at least NTD 4,441,401. A1 was subsequently prosecuted for the crime of breach of duty and of receiving illegal benefit and money laundering.

JAPAN

Use of nominees to receive bribes: A local government official, at a business of recommending bidders of city order constructions, made a construction company put bribe into the bank account under a fictitious name controlled by him.

MACAO, CHINA

Use of net banking and casino chips to launder corruption funds: A civil servant, Mr. F opened an account and received multiple lots of cash totalling USD350k in two years' time. He made use of internet transfers to move funds in and out of the account, further receiving USD251k. He also performed conversion of cash chips into cash without gaming activity. Mr. F is the sole owner of three investment companies. Records of Company Registry indicated that one of the companies was involved in company service. It was suspected that Mr. F's activities were in serious conflict of interest with his civil service and that he could be using banking and casino facilities to conceal the origin of his proceeds, which were not commensurate with his income as a civil servant.

BANGLADESH

Use of foreign nominee accounts: Mr. 'N' is a Bangladeshi politically exposed person (PEPs). He opened two accounts in Bank 'X'. One is for him and one by his wife's name. His wife is also a renowned professional. He had recently awarded a construction bid to company 'Z' for approximately Tk.1000million. In exchange he received Tk20million and the money was deposited in his wife's account. The money was deposited from several business persons who are involved in construction business. After layering the bribed money he placed all the money in a foreign bank in two accounts. The accounts are held by his two daughters who have resided in England for last three years.

*****

Use Of The Internet And New Payment Technologies (encryption, payment systems etc)

CHINESE TAIPEI

Online auctions fraud and 3rd party accounts: Mr. A, familiar with the operation of online auction website, connected to the eBay website and after several trials got the correct account name and password of a highly praised eBay website member, Mr. X. Then he stole Mr. X's membership by modifying this victim's account password and contact phone number so as to prevent X from accessing his own website.

Mr. A then started selling several false valuable commodity merchandises on the internet, he invited a great deal of public bidding with lowest price, then after accepting all the bidder, he asked bidders to remit the money to a designated third party account he controlled.

Internet/phone scam and use of alternative remittance: A gang purchased large amounts of third-party accounts and phone cards, and issued advertising inserts attracting employees with promises of an "easy job, high salary". They colluded with accomplices in China Continent to hire staff to answer phones from interested parties asking for the job. When the job seekers made their calls, they were forced to remit certain amount of "security" to some designated account to ensure their job seeking sincerity.

Once the victims remitted their "security", the money was transferred by online banking service to another account which the gang controlled so as not to risk sending someone to the bank to withdraw money.

It is estimated the deceived victims number approximately 2000 people, and that the proceeds were shared with the gang in China Continent by underground banking. The members of the gang were arrested after a long period of detection.

*****

Identity Fraud - Use Of False Identification

INDONESIA

Use of false ID to open accounts: A suspect sent news to a victim via Short Messaging System (SMS) that they had won a specific prize, such as a car or a certain amount of money. If the receiver responds to the message, he will be asked to transfer money as delivery cost and prize tax. These fees should be transferred in advance to SMS's sender account. The prize will never be delivered and investigators found that a suspect had used what later turned out to be a false ID card to open a bank account. Generally, a suspect cashed the money through ATM. In Indonesia, it was identified that a suspect is involved in embezzlement cases using a false ID in opening an account at the bank.

REPUBLIC OF KOREA

Forged documents used to take over a bank account: *Person A* plotted to swindle a huge amount of money from *Person B's* bank account. He forged *Person B's* ID card and reported loss of bankbook to the bank and requested reissue of a bankbook and change of password. *Person A* also applied for internet banking service. On the next day, *Person A* withdrew KRW 1.5 billion from the account and transferred it to an account under the name of a third party that he managed. On the following day, he remitted the money into his own account in multiple transactions through the internet banking.

PHILIPPINES

A complex array of accounts in false names: An STR led to the discovery and apprehension of a syndicate headed by a husband and wife team who had used false identification documents to open accounts in different branches of various banks located in several provinces.

Mr. Z, the mastermind of this fraudulent activity, was using several aliases to open several bank accounts by initially depositing USD100.00 bills and dollar-denominated cheques which were payable to the persons whose real names the perpetrator usurped through the use of fraudulent or fake identification documents. The same was true of his spouse, Mrs. Z, who also used fake IDs in depositing foreign cheques to her own newly-opened account. These cheques were reported by the real payees as missing or stolen in transit.

In all, the husband and wife team were able to open twelve (12) different accounts under different aliases in various amounts ranging from USD100 (P5,000.00) to USD28,000 (P1,500,000.00).

Alerted by reports filed by the real payees of the missing or stolen cheques, one of the banks was able to identify one of the cheques deposited by Mr. Z as one of those declared missing or stolen. Subsequently, other cheques reported as missing or stolen were identified as the same cheques deposited to the accounts of either Mr. Z or Mrs. Z with other branches of the same bank. Accounts were opened by Mr. and Mrs. Z using different identification documents.

Finally, one of the branch managers of the bank identified Mr. Z to be the same Mr. AMC who was attempting to open an account with his branch using fraudulent identification documents. The branch manager allowed the account opening then filed an STR. Thereafter, the law enforcement authorities were alerted, and an entrapment operation was set-up. When Mr. Z *aka* Mr. AMC returned to withdraw the proceeds, he was arrested together with his wife and their cohorts.

NEW ZEALAND

False accounts linked to welfare fraud: An Auckland man created 123 false identities which he used to obtain welfare benefits from the Government. As a result, he defrauded the Government of over NZD3.2 million dollars. The proceeds were used to purchase shares in international companies, gold bullion, cash, luxury items and the installation of a NZD50,000 garden in the property he rented.

A search of the address located NZD200,000 cash in his house, gold bars hidden under the shower tray in his bathroom and further gold bars were found in his house. NZD750,000 was also located buried in his backyard.

*****

Use Of Life Insurance Products

INDONESIA

Structuring life insurance transactions to launder proceeds of corruption: During various periods in 2005/2006 Mrs A bought more than 20 investment-related life insurance policies with insurance premium value mostly of over USD40,000 each in cash, purchased using multiple intermediaries in different areas. The life insurance company sent an STR to PPATK in respect of the large cash transactions moving through the company accounts. Transaction history showed that to pay for the policies Mrs. A used cash withdrawn from her savings account in AAA Bank, CCC Bank and ZZZ Bank and a joint account with her husband Mr B in JJJ Bank.

The source of funds in the JJJ Bank account had been transferred in from several parties accounts during 2005 totalling about USD620,000 and from Mrs. A's account in CCC Bank within 2005 for a total amount more than USD250,000. There were also several amounts deposited in cash by others parties between 2005 estimated at over USD120,000.

As Mr. B was a high ranking police officer of Republic of Indonesia (a PEP) the STR referral was submitted to law enforcement agency for action and identification of possible corruption and money laundering activities.

Children of a PEP investing in life insurance: From March – July 2004 there were several additional premium payments ('top ups') to a life insurance policy for a total amount more than USD500,000 funded from a man's account in HEALTH Bank ltd.

In June 2006 that person's older sister bought a single premium of investment related life insurance product estimated USD200,000. She terminated this insurance policy by July 2006 due to urgently needed for funding a real estate investment. She then established and registered company named "CV GOOD" in September 2006 with capital of approx. USD50,000 to engage in the mining business, with herself assigned as owner/director. The life insurance company disclosed the early termination insurance policy to PPATK.
The woman then bought another life insurance policy in October 2006 with CV GOOD acting as policyholder.

An exchange of information with Indonesia Corruption Eradication Commission resulted that people were the children of a former high government official of Republic of Indonesia. The father was under investigation in corrupting National State Budget year 2002-2004.

Corruption and life insurance: The ABC life insurance company submitted an STR to PPATK regarding several transactions involving family members. A woman invested her money in life insurance investment related products in mid-2005 with large insurance premium values, funded from her savings account in DDDbank Ltd where a deposit had previously been made of $1,600,000, derived from redemption of Jane's mutual fund in two different managed investments totalling about $1,750,000 – these funds originated from terminating a term deposit held with EEEbank Ltd on behalf of one of the woman's sons. Part of the proceeds was moved to the Son A's account in EEEbank Ltd who had also purchased a life insurance, investment-related policy which he terminated only two months later, transferring the proceeds to Son B's saving account in FFFbank Ltd.

There was a deposit in Son B's account deriving from terminating his mother's insurance policies for around $1,000,000 in June 2006. Son B invested large amounts in real estate and luxurious cars. Son B had also made a large payment to a life insurance company to fund a policy on behalf of his father who was a high government official of Republic of Indonesia. There were several additional premium (top-ups) paid to the father's policy from his wife and sons' various accounts.

The source of the funds in the father's bank account was from several massive amount of cash deposit from other parties which were unknown. In addition, the father deposited and withdrew in cash in regular basis roughly at over $10,000.