



**Asia/Pacific Group
on Money Laundering**

ASIA/PACIFIC GROUP ON MONEY
LAUNDERING

APG Yearly Typologies Report 2010

Methods and Trends of Money
Laundering and Terrorist Financing

Adopted by APG Members at the 13th Annual
Meeting

Singapore, 16 July 2010



© 2010 ASIA/PACIFIC GROUP ON MONEY LAUNDERING;

All rights reserved.

No reproduction or translation of this publication may be made without prior written permission. Requests for permission to further disseminate, reproduce or translate all or part of this publication should be obtained from APG Secretariat, Locked Bag A3000, Sydney South, NSW 1232, Australia. (Telephone: +612 9286 4383 Fax: +612 9286 4393 Email: mail@apgml.org)

CONTENTS

INTRODUCTION	2
1. OVERVIEW OF THE 2009 APG TYPOLOGIES WORKSHOP	3
1.1 Human Trafficking and Money Laundering	3
1.2 Money laundering Associated with Large-Scale Trans-National Frauds.....	4
1.3 ML Risks Associated with Carbon Emissions Trading Schemes	5
1.4 ML/TF Vulnerabilities in the Securities Sector – An Update	7
1.4.1 Case Studies – Securities and ML.....	8
1.5 Cash Couriers – Recent Developments.....	10
2. TERRORIST FINANCING TECHNIQUES, METHODS AND TRENDS..	12
2.1 Discussion of TF Typologies at the APG Typologies Workshop	12
2.2 Case Studies and Observations of TF Trends	12
3. CASE STUDIES OF ML AND TF	19
3.1 Casinos & Gambling Activities	19
3.2 Alternative Remittance Services and Underground Banking.....	20
3.3 Real Estate – ML or TF through the Real Estate Sector	21
3.4 ML through Non-Profit Organisations (NPOs).....	22
3.5 Structuring or ‘Smurfing’	23
3.6 Wire Transfers	24
3.7 Use of Shell Companies / Corporations / Trusts	24
3.8 Use of Offshore Companies/ Banks / Trusts (roles of TCSPs)	26
3.9 Use of Nominees, Trusts (onshore), Family Members or Third Parties.....	26
3.10 Use of ‘Gatekeepers’ Professional Services (Lawyers, Accountants, Brokers).....	27
3.11 Use of Stored Value Cards.....	28
3.12 Purchase of Portable Valuable Commodities (Gems, Precious Metals)	28
3.13 Association with Corruption	28
3.14 Use of the Internet and New Payment Technologies	30
3.15 Criminal Knowledge of and Response to Law Enforcement / Regulations	30
4. TRENDS OF MONEY LAUNDERING & TERRORISM FINANCING	31
4.1 Research or Studies Undertaken on ML/TF Methods and Trends.....	31
4.2 Association of Types of ML or TF with Predicate Activities	31
4.3 Emerging Trends; Declining Trends; Continuing Trends	31
4.4 Effects of AML/CFT Counter-Measures	33
5. FUTURE WORK.....	35

INTRODUCTION

Background

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

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

The Yearly Typologies Report includes observations on ML and TF techniques and methods. These observations are intended to assist with identifying instances of suspicious financial activity in the real world. It is hoped that the case studies and 'red flag' indicators included in this report will assist the front-line financial institutions and non-financial businesses and professions (casinos, accountants, lawyers, real estate, etc) which are involved in implementing preventative measures such as customer due diligence and suspicious transaction monitoring.

Each year APG members and observers provide information on ML and TF cases, trends, research, regulatory action and international cooperation. The information collected from APG delegations not only provides the basis for case study collections such as this, but also for selection and design of in-depth studies on particular typology topics. The information also supports the work of the network of typology experts involved in the APG Typologies Working Group.

Typologies in 2009-10

Key typologies information is shared between practitioners during each annual APG Typologies Workshop. In October 2009 that workshop was successfully held in Cambodia (see details below). The APG looks ahead to a successful workshop being staged in Bangladesh in October 2010.

Information gleaned from typologies collection is shaping the ongoing work on in-depth projects within the APG Typologies Working Group. It is anticipated that focused work will be undertaken in the coming year on ML associated with large-scale transnational frauds, as well as TF linked to abuse of non-profit organisations. Summary outcomes of that APG work will be included in next year's typologies report.

The case studies in this report are only a small slice of all the work going on across the Asia/Pacific region to detect and combat ML and TF. The report has attempted to select a number of illustrative cases from this year. It should be noted that some of the cases included took place in previous years, but the summary information has only been released this year. A great number of cases cannot be shared publicly, due to their sensitive nature or ongoing legal processes.

The APG acknowledges and thanks Malaysia and India for their ongoing contributions as APG Typologies Working Group Co-chairs.

July 2010

1. OVERVIEW OF THE 2009 APG TYPOLOGIES WORKSHOP

Introduction

1. Cambodia hosted the 12th APG Typologies Workshop in Siem Reap from 25 – 28 October 2009. It was attended by over 140 participants, representing 30 APG members and 5 international and regional organisations.
2. The 2009 workshop focused on:
 - Vulnerabilities in the Securities Sector;
 - Terrorist Financing trends
 - Abuse of NPOs
 - Kidnap for Ransom
 - Human Trafficking and ML
 - Cash couriers – cases and recent updates on best practice
 - Emerging issues (including ML and large-scale transnational frauds)
3. H.E. Chea Chanto, Governor of National Bank of Cambodia gave the key note address on the first day of the workshop. The workshop Co-chairs were H.E Phan Ho, Secretary General of National Bank of Cambodia and Head of Cambodia FIU, and APG Typologies Working Group Co-chairs Ms Foo Lee Mei, Securities Commission Malaysia and Mr Arun Mathur, Department of Revenue India.
4. Section 1 of this report sets out a number of summary issues arising from the 2009 APG Typologies Workshop.

1.1 Human Trafficking and Money Laundering

5. Australia, Cambodia, Myanmar and Japan provided presentations during the 2009 APG Typologies Workshop on issues relating to ML and human trafficking. Delegates discussed legal frameworks and international cooperation issues arising from the Human Trafficking Protocol and the Smuggling Protocol. Both protocols supplement United Nations Convention against Transnational Organised Crime (UNTOC).
6. Delegates discussed why a country that is not necessarily a source or destination country would take steps to implement the UNTOC protocols. Members discussed the need to include these offences as predicates to ML and the importance in cutting off jurisdictions being used as ‘safe haven’ transit points for both the trafficking/smuggling and the associated ML. Delegates also discussed use of the UNTOC as formal basis for international cooperation.
7. Some indicators of ML associated with human trafficking include use of alternative remittance systems, use of common addresses and disparity of income. Discussions stressed the importance of using the AML regime to:
 1. detect people smuggling and trafficking;
 2. detect organisers of people smuggling and trafficking; and
 3. corroborate evidence of victims of people smuggling and trafficking.

8. During the 2009 Typologies Meeting delegates discussed the need for strengthening informal mechanisms to cooperate at the international level on financial aspects of human trafficking investigations. It was noted that the Bali process provides an excellent framework to give effect to the requirements of Recommendation 40. In this regard the reasons and obligations of all countries to legislate in this area were clarified, irrespective of whether or not that country is a source, transit or destination country.

9. The United Nations Office of Drugs and Crime (UNODC) has recently released a number of significant global studies of human trafficking and people smuggling. Those reports identify a number of significant gaps in information regarding the dynamics of finances associated with human trafficking, including the flows of funds and key money laundering typologies and red flag/indicators for ML.

10. Australia has undertaken to conduct a scoping exercise on human trafficking and ML on behalf of the APG. This included a questionnaire to all APG members. The findings of that initial scoping exercise will be shared with APG members in the coming months.

11. The FATF is undertaking a typologies study on this topic and it is anticipated that APG will seek to contribute to that FATF study in the coming months.

1.2 Money laundering Associated with Large-Scale Trans-National Frauds

12. The APG Typologies Workshop initiated a preliminary discussion on a number of ML typologies associated with large-scale trans-national frauds. It was noted that there was a lack of regional or global typologies on the issue of ML and telemarketing frauds, including boiler room, lottery fraud and heritage fraud.

13. A proposal was made by Hong Kong to undertake an APG project in this area. It was explained that Hong Kong's response has been to dedicated investigative units, recover losses for victims and prosecute ML where possible. Hong Kong's Joint Financial Intelligence Unit acts as a point of contact between banks and foreign FIUs and law enforcement agencies – providing feedback and red flag indicators for the banks.

14. APG mutual evaluations, APG typologies collections and typologies workshops continue to highlight threats from ML associated with large-scale transnational frauds, in particular telemarketing / boiler room / lottery frauds. Jurisdictions which have conducted investigations of these frauds and associated ML highlight the involvement of transnational organised crime groups and highly profitable criminal activity.

15. Laundering of proceeds from boiler room / heritage / lottery frauds is a lucrative, relatively low risk, global criminal activity. Their trans-national nature presents numerous multi-jurisdictional issues for preventative measures, enforcement, prosecution and asset recovery. The failure to rapidly exchange information and the lack of coordinated multi-jurisdictional action to combat and identify the syndicates involved enhances ML vulnerabilities. Increased national and international collaboration is required to combat these offences.

16. Despite the scale of the problem, there remains a lack of recent regional or global ML typologies associated with these large-scale transnational frauds.

17. Telemarketing and related frauds are an example of how transnational organised crime activity has adapted and grown with globalisation. Telemarketing frauds and associated ML have proliferated, utilising an increasingly wide spectrum of modus operandi to present a fraudulent solicitation to a prospective victim.

18. A survey by the Crime Prevention Coalition of America found fraudulent telemarketing schemes cost US consumers an estimated \$40 billion each year, while in Hong Kong, 519 cases of lottery and boiler room fraud were reported in 2009 with losses of over US\$13 million. This figure includes cases where the victim actually resided in Hong Kong and also cases where the victim resided in other jurisdictions but where the proceeds were laundered through a number of different jurisdictions, including Hong Kong. The experience of Hong Kong has therefore been that shared with many other jurisdictions, that of a conduit; numerous inward remittances from overseas victims, quickly followed by outward remittances overseas. The businesses and money flows seen in Hong Kong, China have been relatively unsophisticated, although this may not be the case for all jurisdictions.

19. A number of jurisdictions, including Hong Kong and Malaysia, have successfully prosecuted money-laundering offences associated with cross border telemarketing fraud. It is apparent that criminals may take account of AML/CFT controls in various jurisdictions when designing money laundering schemes associated with these frauds.

20. Experience suggests that some financial institutions are successful in identifying accounts used for this type of crime; however, criminals are quick to react and adapt money flows in response to preventative measures. Jurisdictions' experience with this matter is worthy of further examination. APG members discussed a possible in-depth project on these issues and agreed to the preparation of a Project Plan, which will be considered at the Typologies Working Group meeting to be held during the APG's 2010 Annual Meeting in Singapore in July.

1.3 ML Risks Associated with Carbon Emissions Trading Schemes

21. APG delegates to the 2009 Typologies Workshop gave some preliminary consideration to possible vulnerabilities from ML or TF associated with national and international carbon trading schemes. Delegates considered the very rapidly growing size of global carbon trading markets. The world's carbon markets were expected to reach \$122 billion by the end of 2009.

22. One case was presented which involved the United Kingdom. In August 2009, UK Fraud investigators arrested nine people over a suspected £38m carbon credit trading scam. It is thought that the proceeds of this crime were used to finance lavish lifestyles and the purchase of prestige vehicles.

23. Commentators have highlighted vulnerabilities from corruption and bribery at the point of measuring carbon outputs or storage. Delegates also noted vulnerabilities highlighted in recent FATF work on ML vulnerabilities in the securities sector and cross over issues with trading in carbon emissions securities. Delegates to the 2009 APG Typologies Workshop noted that ML vulnerabilities in carbon trading markets may be an area for future study for the APG.

Open Source Report

Norway widens CO2 probe into money laundering

30 March 2010 Reuters News

A Norwegian police investigation into alleged carbon tax evasion is widening its scope into money laundering, with five men charged, Oslo police said on Monday. The Norwegian authorities' investigation is part of a wider probe into tax fraud relating to carbon emissions trading that European police agency Europol said cost treasuries up to 5 billion Euros (\$6.72 billion) in lost revenues.

"We have three arrested and five charged ... Altogether it's six companies (we are investigating)," said police superintendent Boerre Walderhaug, head of the finance and environment unit at Oslo police. He declined to name any of the suspects.

Norwegian investigators previously said that two men had been arrested and around five companies were being probed.

"All five men are charged with both tax fraud and money laundering," Walderhaug told Reuters on Monday. Norwegian tax authorities previously said that the charges were for tax fraud.



Walderhaug declined to say which illegal activity the laundered money was from, but said it amounted to some 260 million Norwegian crowns (\$43.13 million).

Open Source Report


Carbon trading Frauds: A Timeline

30 March 2010 Reuters News

MAR, 2010

-  Spanish police say they have arrested nine people on charges of avoiding 50 million euros (\$67.54 million) in tax linked to trading in carbon credits.
-  Norwegian tax authorities said they will investigate all firms' EU carbon permit transactions in the Nordic country as part of an ongoing probe into VAT fraud.


FEB 26, 2010

-  Norway's tax authority says three people are charged and at least two companies are under investigation in Oslo over alleged carbon tax fraud.


JAN 11, 2010

-  Belgian prosecutors say three Britons and a Dutch man are charged by Belgian authorities with money laundering in an investigation into fraudulent trading in carbon emissions permits.


DEC 10, 2009

-  Fraudulent trading in EU carbon emissions credits in the past 18 months has led to more than 5 billion euros in tax revenue losses for several EU nations, European police agency Europol says in a statement.

SEP 1, 2009

-  A patchwork of unilateral actions by few European Union nations to prevent suspected tax fraud in carbon permit trading could serve only to push the activity into neighboring states.

AUG 19, 2009

-  The British tax office arrests seven people in London in a suspected 38 million pound (\$57.13 million) VAT fraud in the EU carbon allowances market.

1.4 ML/TF Vulnerabilities in the Securities Sector – An Update

24. In 2008-09 the FATF conducted a typologies project on ML and TF risks in the securities sector. As reported in the 2008/09 APG Typologies Report, the APG contributed to the FATF project through case studies and session held in the 2008 APG Typologies Workshop.

25. FATF published the full Securities Vulnerabilities Report in October 2009¹, which is available for download via <http://www.fatf-gafi.org>. The report contains in-depth findings of risks and vulnerabilities as well as illustrative case studies and red-flag indicators of suspicion.

26. During the 2009 APG Typologies workshop the FATF project leader shared a number of key findings on vulnerabilities in the securities sector. These include:

- ✚ **Securities product** – the nature of the securities product itself is an area of vulnerability. For example in the over-the-counter (OTC) options market where OTC contracts can be tailored for a specific investor. Such tailored products can be very complex for the supervisors, FIUs or investigations agencies to appropriately supervise/regulate/investigate.
- ✚ **Markets and other means of access** – Traditional exchanges, OTC, alternative trading platform represent varying degrees of vulnerabilities
- ✚ **Payment methods** – cash, cheques, wire transfers, exchange of securities (e.g. in a takeover situation) present vulnerabilities
- ✚ **Entities involved in securities products** – broker dealers display over-reliance on CDD conducted by other financial institutions (in particular banks), investment adviser and wealth managers.
- ✚ **Clients and accounts type** – trusts, nominee and omnibus accounts present particular vulnerabilities. It may be very difficult to obtain beneficial ownership information especially when business is conducted in a way where such information has not been collected for many years.
- ✚ **Determination of value** – lack of price transparency in some transactions (e.g. off market) creates vulnerabilities.
- ✚ **Rogue employees** – employees who assist customers in AML/CFT poses serious vulnerability in a financial institution.
- ✚ **Terrorist financing** – There is little evidence in securities industry being used to finance terrorism. However, this does not rule out possible use of the sector for terrorist financing.
- ✚ **Predicate offences linked to securities transactions** – this was noted as a particular issue in case studies provided by the APG.

27. In addition to these and other findings, the FATF report summarises the experience reported by APG member countries. The FATF report listed the following common suspicious indicators and methods related to ML and predicate offences involving the securities industry:

- Changing share ownership in order to transfer wealth across borders;
- Redeeming a long-term investment within a short period;
- Opening multiple accounts or nominee accounts;

¹ <http://www.fatf-gafi.org/dataoecd/32/31/43948586.pdf>

- Using brokerage accounts as long term depository accounts for funds;
- Effecting transactions involving nominees or third parties;
- Engaging in market manipulation, e.g. “pump & dump” schemes; and
- Engaging in boiler room operations.

28. APG and the FATF both noted a clear need within the APG for a clearer understanding of the ML/TF risks and vulnerabilities of the securities industry.

1.4.1 Case Studies – Securities and ML

MACAO, CHINA





Case Study – Laundering proceeds of corruption through stock market

29. Mr. D opened an account in XYZ Security Company. He nominated Mr. E as the authorized person of the account, who could act on his behalf to buy/sell shares. The declared relationship between Mr. D and Mr. E was “friends”. Within a month after account opening, Mr. E had placed over 100 orders by trading on one same stock, and the profit obtained was up to \$500,000.

30. After that, Mr. D instructed to transfer all the profits to his own personal bank account. Since the trading amount and pattern were unreasonable compared to his income, XYZ Security Company filed the case to FIU. With information from the bank, it was noted by FIU that the fund was ultimately remitted back to Mr. E, who was later found to be involved in a bribery case.

CANADA

31. Results of a study by FINTRAC identified cases of the securities industry having been used to launder proceeds generated by various crimes including drug trafficking, stock manipulation and fraud. The following typologies were found to be associated with the use of the securities industry for suspected ML:

-  use of front companies;
-  use of professionals to facilitate the introduction of proceeds;
-  use of margin trading accounts; and
-  use of money orders.

Case Study – Suspected laundering of stock manipulation proceeds

32. This scheme involved the manipulation of stocks to make fraudulent profits which were laundered through a number of bank accounts in Central America and the Caribbean, as well as through the purchase of monetary instruments made payable to suspected nominees.

33. STRs from the securities sector and financial institutions led to a case involving eight individuals (an investment adviser and seven business associates) located in Canada and two corporations located in Central America. One of the business associates was under investigation for banking fraud in an Asian country, which cost investors close to CAN\$100 million.

34. The investment advisor appeared to be providing information to the seven individuals as to when to purchase and sell stocks of certain firms:

- ✚ One financial institution reported that the investment advisor was receiving large wire transfers into a business account from a securities dealer. When questioned as to the reason for the transfers, the investment advisor became uncooperative; the financial institution suspected that the individual was dumping a large number of shares purchased earlier from the same securities dealer.

- ✚ STRs from other financial institutions confirmed that the individual was the investment advisor of at least two other members of the group.

35. Another member of the group was found to be associated to two corporations with addresses in two different Central American countries:

- ✚ This individual had signing authority over 24 accounts held by these corporations with the same securities dealer.
- ✚ STR information received from a securities dealer revealed that this individual sold shares of specific companies shortly after purchase.
- ✚ The sales were followed by wire transfers to various bank accounts held by the two corporations and the aforementioned investment advisor at financial institutions in Central America and the Caribbean.

36. The same type of activity appeared to be conducted by all of the individuals associated to this scheme:

- ✚ The purchase of securities (mostly penny stocks that were not regulated, and therefore easy to manipulate) would be quickly followed by a sale, which would then be followed by wire transfers or deposits to bank accounts. Bank drafts would then be purchased, or cheques would be issued and made payable to suspected nominees.

RED FLAGS associated with this case:

- ✚ Large number of accounts with (a) securities dealer(s)
- ✚ Large number of shares were traded shortly after being purchased
- ✚ Two companies (possibly front ones) were located in a jurisdiction where incorporation is easily obtained, or where business-related claims are difficult to confirm
- ✚ A significant number of wire transfers were made to offshore accounts, particularly following the sale of a substantial amount of shares
- ✚ Monetary instruments were made payable to a number of suspected nominees

Additional red flags possibly related to market manipulation include:

- ✚ Large percentage of securities dealers' commission revenue generated from limited number of clients
- ✚ Securities agent or advisor purchasing or selling stocks outside his or her jurisdiction of registration
- ✚ Financial statements of companies, including balance sheets, income statements, and statements of change in financial position are not publicly available
- ✚ Company's published statements of cash flow indicates the presence of capital, but no cash flow generated by the organization
- ✚ Company's executives reside in jurisdictions without extradition treaties with Canada

- ✚ Securities sales by insiders such as company executives, their relatives etc.
- ✚ Unrealistic increase in share prices without major announcements in terms of future projects, earnings etc.
- ✚ Unrealistic increase in share prices with an announcement that cannot be verified

1.5 Cash Couriers – Recent Developments

APG's Focus on Cash Courier Issues

37. The APG typologies program has included a focus on cash couriers over a number of years. This reflects the very significant challenges faced by many APG members from implementing effective AML/CFT for large-scale cash economies. Many APG members continue to highlight cash smuggling as one of the major typologies for both ML and TF in the region.

Operation Mantis

38. During the 2009 APG Typologies Workshop Canada provided a presentation on some of the lessons learned arising from the Operation Mantis, a G8 initiative to target and disrupt cash couriers. Operation Mantis represents a strong model of international cooperation.

39. Operation Mantis commenced in 2007 as an initiative to support coordinated information sharing to counter cash smuggling used to finance terrorism. Coordinated multi-jurisdictional operations were conducted over several days in April 2009 which resulted in 81 cash seizures totaling more than US\$3.5 million and the detection of another \$4.2 million in undeclared currency at ports of entry around the world. A critical element in the operation's success was the sharing of real-time targeting information and intelligence between law enforcement agencies and FIUs.

40. During the three-day operation authorities examined hundreds of flights at multiple international airports. G-8 members shared real-time information and intelligence in order to target and interdict cash couriers. In addition to intelligence sharing, airport authorities used a variety of cash detection methods to identify cash carried in baggage, on travelers, or in shipments. Detection methods included the use of currency detector dogs, X-ray and gamma-ray equipment, body searches and ion mobility scanners.

41. While the public side of the Operation Mantis focused on seizures and arrests over those three days, law enforcement agencies continue to pursue investigations related to intelligence developed through the operation.

FATF Best Practice Paper on SR IX - Cash Couriers

42. In February 2010 the FATF released its new Best Practices Paper for Special Recommendation IX on cash couriers. In addition to elaborating on best practices for a disclosure or declaration system, the Paper includes practical guidance for identification and targeting of cash couriers and investigation and prosecution following interdiction.

43. The Best Practices Paper includes a collection of red flags/indicators that can be used to detect cash couriers. In many cases more than one red flag/indicator will trigger suspicion.

Open Source Report

26 January 2010 Vancouver Sun

More than \$10 million in cash is being smuggled out of Afghanistan every day, a report by anti-fraud investigators has revealed.

The sum is equivalent to more than \$3.9 billion a year, or more than three times the government's official tax and customs revenue, in a country plagued by corruption. Investigators found the cash leaving Afghanistan is taken out mainly stuffed in suitcases through Kabul airport and most ended up in the United Arab Emirates.

The inquiry, conducted by the Ministry of Finance and organized crime experts from America, found \$202 million in one single 19-day period, mainly through Kabul airport.

2. TERRORIST FINANCING TECHNIQUES, METHODS AND TRENDS

2.1 Discussion of TF Typologies at the APG Typologies Workshop

44. The APG 2009 Typologies Workshop included a number of presentations on legal frameworks and law enforcement responses to the phenomenon of kidnap for ransom. This issue is a particularly serious one for Pakistan and the Philippines as well as Afghanistan and a limited number of other APG members.

45. APG members also discussed typologies of abuse of non-profit organisations (NPOs) and charities for TF. It was stressed that the NPO sector continues to play a vital and highly valuable role in every APG member. The vast majority of NPOs conduct entirely legitimate work for the good of society. Cases of abuse of NPOs represent a very small fraction of all NPO activity.

46. Despite the overall strongly positive role for the NPO sector, APG mutual evaluations, APG typologies collections and typologies workshops continue to highlight vulnerabilities to TF and ML from abuse of NPOs, including charities.

47. Despite the scale of the problem, there remains a lack of recent regional or global typologies on abuse of NPOs for TF. The FATF undertook a typologies study in 2005 on abuse of NPOs for TF, but up to date case studies and trend information from the Asia/Pacific region is lacking.

48. Many jurisdictions may not be fully aware of case studies and existing typologies research on NPOs and best practices identified. Given the continuing vulnerabilities for TF associated with abuse of NPOs, there is a need for up-to-date typologies.

49. A number of jurisdictions, including Canada, Pakistan and Sri Lanka, have investigated TF offences associated with abuse of NPOs. APG members discussed a possible in-depth project on these issues and will discuss a project proposal in July 2010.






50. Eleven APG members provided further detailed terrorist financing trend information and case studies on terrorist financing in the region. A number representative case studies shared by members are summarised below.

2.2 Case Studies and Observations of TF Trends

AFGHANISTAN

51. Open source studies highlight foreign donations and taxes on opium production as key sources of finance for the Taliban in Afghanistan.

52. Afghanistan authorities provided some further detail in relation to the dynamic of kidnap for *ransom* in the country.

-  Kidnappings are relatively common in Afghanistan.
-  Kidnappers are for the most part illiterate.
-  Kidnappers avoid financial institutions for receiving or moving ransom funds.
-  Kidnappers tend to use unregistered hawaladars to transfer funds or store cash on their premises.
-  No suspicious transaction reports (STRs) have been received yet that identify or trace ransom funds.

AUSTRALIA





53. Australia notes that in the previous two years, the most significant TF cases involved funds being raised in the form of donations to NPOs.

54. In such cases a typical scenario sees organisers from overseas arrive in-Australia and attend gatherings in various locations organised by local leaders. The funds raised are given to other local people to wire transfer to nominated accounts overseas.

55. These transfers are spread out over time and are structured in amounts less than the AU\$10,000 reporting threshold. The typology is complicated in that funds are sent to a third party with suspected links to a nominated terrorist organisation, rather than directly to that organisation.

CANADA

56. Canadian authorities highlight general risks of TF from the abuse of NPOs, use of import/export companies (grocery stores, auto dealers) and money service businesses. Details are set out below:

-  Outgoing wire transfers to “locations of concern,” such those in which a particular terrorist organization is known to operate, or financial hubs in South Asia and the Middle East.
-  The purchase and export of cars appeared in some FINTRAC disclosures suspected of being related to terrorist financing. Car purchases were made in Canada, the United States and East Asia. The same entities, and/or their related officers, made payments to import/export or shipping companies, and it is suspected that the vehicles were destined for a Middle Eastern country.
-  The use of money service businesses (MSBs) was a relatively common component of FINTRAC disclosures suspected of being related to terrorist financing. In some cases, the MSBs are suspected of being complicit in terrorist financing activities.
-  Law enforcement and FINTRAC noted the excessive use of money orders in a particular case related to terrorist financing. Over a 5 year period, a large number of money orders were purchased, in cash. These money orders were cashed in a location of concern, and law enforcement suspects that these funds were used to finance the activities of one or more terrorist organizations.

CHINA

57. China notes that terrorist organizations of concern are located outside of China and techniques for TF include the use of remittance through formal channels and through underground banking.

INDIA

58. India highlights three main channels of TF:

- ✚ Use of formal (non-bank) remittance channels through the Money Transfer Service Scheme (MTSS)
- ✚ Use of new payment methods
- ✚ Informal channels of transfer of value.

59. In addition to these methods, India's 2010 Mutual Evaluation Report highlights other TF threat sources for terrorist financing, including:

- ✚ funds/resources from outside India including through foreign NPOs
- ✚ counterfeiting of currency
- ✚ criminal activities including drug trafficking and extortion

INDONESIA

60. Indonesia highlights the following principal methods for terrorist financing in Indonesia:

- ✚ abuse of the financial system (wire transfers)
- ✚ physical movement of cash
- ✚ through the international trade system.
- ✚ abuse of alternative remittance systems (ARS)
- ✚ abuse of charities, or other captive entities to transfer value.

Case Study 1 – related to TF – use of wire transfers

61. A bank filed an STR with the FIU based on suspicion that funds were being sent to a suspected member of a terrorist group. Mr A opened an account in 2007 with an initial deposit of 18 million rupiah (approx USD2000). Transaction records showed a number of incoming funds transfer from other branches varying from hundreds to thousands of rupiah. Fund were withdrawn, usually by ATM.

Case Study 2 – related to TF – use of wire transfers

62. Bank A in Indonesia received information from Bank B in Thailand regarding a common Thai customer ('Mr X') suspected of terrorism activities in Thailand. Bank A revealed that Mr X regularly transferring large amount of money to Ms Y's account (who is also Thailand citizen) located in Thailand.

63. Ms Y then transferred the money into Mr X's account in Thailand. Mr X and Ms Y are suspected of being members of a terrorist group and using the money to fund their activities. Mr X is also a commissioner and share holder in Company ZZZ. Company ZZZ also has an account in Bank A. Company ZZZ's line business is logging with the capacity of export to Thailand and China. Mr X sometimes uses his own personal account for business purposes.

64. Bank A in Indonesia received information from Bank B in Thailand regarding a common Thai customer ('Mr X') suspected of terrorism activities in Thailand. Bank A revealed that Mr X regularly transferring large amount of money to Ms Y's account (who is also Thailand citizen) located in Thailand.

65. Ms Y then transferred the money into Mr X's account in Thailand. Mr X and Ms Y are suspected of being members of a terrorist group and using the money to fund their activities. Mr X is also a commissioner and share holder in Company ZZZ. Company ZZZ also has an account in Bank A. Company ZZZ's line business is logging with the capacity of export to Thailand and China. Mr X sometimes uses his own personal account for business purposes.

PHILIPPINES

66. Philippines authorities report that terrorist organizations continue to exploit and rely upon charities as a critical source and means of support as well as common crimes. Sources of funds and methods of terrorist financing by terrorist organisations include:

- ✚ NPOs and charities: terrorist organizations recruit members by providing social, economic and welfare services through charities;
- ✚ kidnapping for ransom;
- ✚ robbery/extortion;
- ✚ marijuana cultivation.

Case Study – Terrorist financing relating to the Rajah Sulaiman Movement (RSM)

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

68. A bank based in the southern Philippines submitted two (2) STRs concerning Mr. MA, one of the detainees, and Ms. ND, one of the wives of Abu "A".

69. Inquiries by law enforcement officers identified account holders who used their accounts to receive and withdraw funds for the organization.

70. The following are the respective profiles of the detainees:

- ✚ Abu "A" was a preacher and broadcaster in Metro Manila and worked for some time as a teacher in Saudi Arabia;
- ✚ Mr. MA is a full-time college student and has no known sources of income. He is an orphan and his uncle, Abu "S" supports his studies;
- ✚ One of the detainees was a nurse who used to work in Saudi Arabia;
- ✚ The group established a media foundation which received funding from foreign and local donors. The foundation served as a front organization of the group. Its new recruits undergo indoctrination in this Madrasa school.

71. Financial structures included:

- ✚ Several inter-branch cash deposits credited to the ATM account held by Mr. MA. These accounts were held by Banks 1 and 2 who had branches in the southern Philippines. The inter-branch deposits were made mostly in different provinces in the Philippines;
- ✚ All withdrawals of Mr. MA were done through ATMs and made almost immediately upon receipt of the fund;
- ✚ The account of Ms. ND was the beneficiary of a large sum of money from a bank in Saudi Arabia. The said fund was withdrawn gradually every week by a male individual believed to be a member of Jemaah Islaamiah (JI) and intended for the JI

training in southern Philippines. The account was however closed by the bank for maintaining “zero” balance.

72. On June 4, 2008, UNSC 1267 Committee approved the inclusion of the terrorist group and 8 of its members in the 1267 Committee’s list of designated entities. On July 9, 2008, the court issued a Freeze Order (valid until July 29, 2008) on the following properties/ bank account:

- ✚ A property located in a province in the northern Philippines with a land area of 70,283 sq.m., with current market value of Php 8,785,375.00
- ✚ Property located in Metro Manila which is 66 sq. m. lot upon which is built a 4-storey building. The lot only is valued at Php 1,237,500.00
- ✚ There is evidence to show the RSM group used the foregoing properties for training its members and other activities related to terrorism.
- ✚ An account in the name of RA with Bank-K and all related web of accounts, wherever these may be found.

73. The above-mentioned Freeze Order has been extended by the court as follow-up investigations are ongoing. A petition for civil forfeiture of the foregoing properties/assets was filed with the court in January 23 2009. Meanwhile, an asset preservation order dated February 13, 2009 was issued by the court to prevent said properties/assets disposition while pending litigation.

PAKISTAN

74. Open source commentaries on financing the Pakistan Taliban highlight principal sources of revenue including funds from foreign militants including Al Qaeda, taxes and protection money from local populations and various criminal activities including kidnap for ransom and robberies.

75. Pakistan authorities note donations and contributions, collection in kind, robberies and kidnapping for ransom as the primary sources of TF in the Federal Administered Tribal Area (FATA) and North-West Frontier Province (NWFP) of Pakistan. Authorities note significant challenges of applying AML/CFT regimes to pursue the proceeds of kidnap for ransom in the tribal areas of Pakistan. Kidnapping for ransom is in many ways a traditional crime in both Pakistan and Afghanistan.

76. Pakistan authorities note a significant increase in the rate of kidnap for ransom (KFR) in FATA and NWFP in recent years. While not all of these cases can be attributed to Pakistan Taliban, their use of this technique to raise funds continues. Between 2007 and 2008 the rate of KFR almost doubled in NWFP. The trend for 2009 was as high as 2008.

77. Serious high-profile cases of kidnapping for ransom include the following:

- Mr. Tariq Aziz, (Pakistan Ambassador) – Feb 2008 in Khyber Agency
- Mr. Abdul Khaliq Farahi, Afghan Ambassador Designate – Sep 2008 in Peshawar
- Mr. Hashmatullah Atherzadeh, Iranian Counselor – Nov 2008 in Peshawar
- Mr. Athunasius, Greek National – Sep 2009 in Kalash Chitral, NWFP
- Mr. Piotr Stanezak, Polish Engineer – Sep 2008 in Attock (Killed in Feb 2009)
- Mr John Solecke, Head of UNHCR, US National –Feb 2009 in Quetta by BLA
- Attempted kidnapping of Miss Lynne Tracy, US Counselor – Aug 2008 in Peshawar

78. Open source data, in particular credible journalistic sources in Pakistan, suggests an upswing in the rates of kidnap-for-ransom in Pakistan. Pakistan police report new schemes targeting wealthy elites and foreign nationals. "Quicknappings" are reported to be increasing in Karachi and other centres. These involve targeted attacks, where high value persons are abducted for several hours while the kidnappers demanded ransom payments from family members.

79. Press reports indicate that police face difficulties in distinguishing between small Taliban-linked groups and purely criminal gangs due to a cross over of tactics. Reports suggest some of the kidnap-for-ransom groups work with the Taliban and surrendering portions of ransom payments in exchange for arms

80. In three cases that had been reported in the press in 2008 and 2009, Karachi police identified Taliban directly involved in the kidnapping for ransom cases². Transporter Shaukat Afridi, film-maker Satish Anand and Aqeel Haji were the victims of Taliban-linked kidnappings. Kidnap-for-ransom groups, specifically those in Karachi, are suspected of having been directly commissioned by the Tehreek-e-Taliban Pakistan (TTP) in South Waziristan to conduct kidnappings in the city and send funds to support TTP.

Case Study – Tracing cell phone records to terrorists' bank accounts

81. A Militant organization planned to carry out multiple attacks against various targets. They established two training centres in a major city for training and logistics support. The organisation managed to open two bank accounts in the names of two different persons. Approximately Rs. four million (US\$47,000) were transferred to these accounts from bank accounts in different parts of the country and Rs. 1.5 million rupees were also transferred to these accounts from a foreign country. During the same period the accused rented four houses in the city to carry out attacks and weapons training. The organisation successfully carried out terrorist attacks on multiple targets causing death of scores of innocent persons and destruction of properties.

82. Investigation of the cell phones of the accused person identified a land line which led to a linked bank account. The account of the accused was identified in the same branch with introduction form and address of next of kin. The Bank account of the second accused was identified during search of the rented house. Six accused have since been arrested and 25 have been declared as proclaimed offenders.

Case Study – Costs of suicide bombings

83. A group of people attempted layered suicidal attacks on the residence of an important person. The group purchased explosive material in Punjab and rented two houses in the adjacent areas where they had planned to carry out terrorist acts. Funds and vehicles were arranged by Arab militants / planners based in northern areas of Pakistan. Approx Rs 2 million (US\$23,000) was utilised during the operations. Thirteen accused have been arrested including an improvised explosive device (IED) specialist. The investigation revealed a nexus between various criminal / militant groups.

² <http://www.dawn.com/wps/wcm/connect/dawn-content-library/dawn/the-newspaper/local/12karachi-change-in-trend-of-kidnappingforransom-cases--bi-02>

SRI LANKA

84. Sri Lankan authorities noted the common use of alternative remittance services to move terrorist fund. Sri Lankan authorities also highlight the abuse, misuse, and direct operation of non-profit organizations. Previous APG typologies reports have provided case studies of the Tamil Rehabilitation Organization (TRO), which was used by the LTTE to collect and channel funds. Charitable organizations registered in various countries have collected and remitted money to the LTTE mainly through the bank accounts of TRO.

Case Study – Funding for bombings

85. Bomb blast suspect “S” received funds and instructions from the UK. Money was transferred from the UK to a local alternative remittance agent “D”, in Colombo. Terrorist suspect S received funds from D, who employs a fleet of youths with motor cycles for disbursement of money. D maintained three accounts in a commercial bank to facilitate his transactions. D received money through; physical cash couriers, netting off arrangements, under/over-invoicing and smuggling of currency/commodities.






THAILAND

86. Thailand indicates that sources of TF were previously from extortion, donations from politicians or foreign donations to educational charities which were diverted for terrorist acts. Recent TF methods involve front businesses, schools used to obtain government subsidies and abuse of local co-operatives and social welfare stores.

87. Thai authorities highlight TF cases where the LTTE used proceeds of fraud for terrorist financing. Forged electronic cards were used to withdraw money from ATMs. Funds obtained through these frauds sent to finance the LTTE in Sri Lanka.

UNITED STATES

88. Law enforcement authorities acknowledge that operatives of terrorist networks are often involved in precursor crimes to facilitate the movement of people, fund operations and procure weapons and explosives. Some of the more common sources from criminal means that we have seen in the U.S. include:

-  Wire transfers;
-  Charities/Non-Profit Organizations;
-  Corporate vehicles/trust and company service providers (TCSPs);
-  Front companies;
-  Money transfer and exchange services.

3. CASE STUDIES OF ML AND TF

3.1 Casinos & Gambling Activities

AUSTRALIA

Case Study 1 – Use of ‘cleanskins’ to launder funds through the casino

89. Australia noted a trend of welfare recipients being targeted as money laundering ‘mules’ used to launder proceeds of narcotics through casinos. Welfare recipients are targeted, due to inherent social and financial rewards that come with VIP member status at casinos.

90. This case involved a casino patron with an annual multi-million dollar gambling turnover who incurred net gambling losses in excess of AUD \$1.4 million (approx US\$1.2 million) over 18 months. The patron’s sole source of legitimate income was government welfare payments. Enquiries indicated the likely source of gambling funds was narcotics importation and distribution.

Case Study 2 – Use of online betting to launder funds for organised crime groups

91. An online money laundering syndicate actively sought criminal networks as customers by offering to launder their proceeds of crime. The syndicate used a licensed company as a front to accept racing, sporting and entertainment bets via telephone and the internet. The company accepted payments via charge cards, credit cards and transfers from a related company. To avoid detection by AUSTRAC (the Australian FIU), the related company was based in a Pacific island jurisdiction, and allowed members to transfer funds internationally via the internet or mobile phones.

92. The company’s website contained a step-by-step guide to mobile betting. The guide explained that a link to a mobile betting application could be sent to the customer’s mobile phone by entering the phone number.

93. AUSTRAC analysis identified four persons who made multiple funds transfers from various countries, as well as significant cash deposits and withdrawals.

Case Study 3 – Use of casino accounts to launder fraud proceeds

94. An investigation into a bank employee who gambled millions of dollars from clients’ accounts was initiated as a direct result of STR information. The suspect used his knowledge of the bank’s internal procedures to discreetly transfer funds from customers’ accounts to his own personal account.

95. Over a period of time, these funds were deposited into his casino account in the form of bank cheques made out in his name. The casino lodged STRs in relation to the regular deposit of bank cheques. The same casino had also previously lodged reports when the suspect had placed bets of AUD\$9,000 to avoid the AUD\$10,000 (approx US\$8,500) reporting threshold. As a result of the investigation, the suspect was charged with three counts of money laundering and 37 counts of fraud.

HONG KONG, CHINA

96. Fund flow analysis conducted in Hong Kong into the proceeds of drug trafficking identified five cashier orders, made out from a casino in a neighbouring Jurisdiction B that were later credited into the account of a Hong Kong female Mrs. X. With assistance from Jurisdiction B it was established that Mrs. X had never been to Jurisdiction B when the orders were made out and it was suspected that her bank account had been used to launder the

proceeds of drug trafficking. Mrs. X was subsequently arrested and after investigation, charged and convicted for money laundering.

KOREA

Case Study – Proceeds from illegal bookmaking accounts

97. Suspicious transactions were noted with a pattern of many repeated deposits and withdrawals involving unspecified people concentrated on Fridays, Saturdays and Sundays. Analysis showed a possible connection with horse racing in Korea (races are held every Friday, Saturday and Sunday). The account holders were shown to have bad credit and the accounts were usually closed after 3 months. Investigations led to the arrest of 16 persons including the account holders conducted similar horse racing activity by issuing private horse race tickets worth approximately KRW 318 million (US\$ 260,000).

3.2 Alternative Remittance Services and Underground Banking

AUSTRALIA

Case Study 1 – Co-mingling proceeds of crime with legitimate funds

98. Investigation of a remittance company showed the entity was remitting large amounts of cash in sums of up to AUD\$2 million (approx US\$1.7 million), through the regulated banking system. In the past eight years up to AUD\$100 million had been reported as being remitted offshore. In a recent three-month period, this included AUD\$35 million in cash being deposited by the entity at a major bank for subsequent remittance to beneficiaries in over 40 countries. Intelligence shows proceeds of crime were intermingled with legitimate business and family-related transactions. It was estimated that the criminal component of the proceeds was up to 50% of the total value of sums remitted.

99. It is understood that the funds sent offshore are forwarded through a complex route. A critical factor in the early detection of such matters is to educate frontline bank staff in identifying alternative money remitters, and to recognise 'red flags' such as a sudden and sustained escalation in the value and volume of business activity.

Case Study 2 – Alternative remittance services controlled by organised crime groups

100. An investigation into the operations of a trans-national crime syndicate based in Eastern Europe commenced after AUSTRAC referred a suspicious cross border report to a law enforcement partner agency. Further investigation revealed that the funds were the proceeds of a trans-national organised crime syndicate. The investigation led to the discovery of an Australian drug lab and the seizure of more than 100,000 ecstasy pills.

101. Money launderers had originally used contacts in Eastern Europe to provide underground remittance service for Eastern European residents in Australia wishing to send funds back to their families. Initially alternative remittance was the only option available to remit legitimate money to the region. After official banking channels were established to the region, the underground remittance activity continued, albeit primarily for criminal associates of the money launderers.

102. The money laundering operation was based on the activities of one family, which arranged secret meetings to exchange and collect funds, and used third parties and third-party accounts to remit funds to distance the remitters and the beneficiaries from the transactions. Bank drafts were purchased in the names of 3rd parties and couriered overseas.

Case Study 3 – Complicit money remitters used by organised crime

103. Investigations revealed organised crime syndicates using a network of complicit money remittance dealers in Sydney and Melbourne to launder the proceeds of drug importations. The network of money remitters was controlled by Vietnam-based members of a family based in Australia. The suspects transferred money to syndicates in Cambodia, Hong Kong and other Southeast Asian jurisdictions.

104. The money remitters used various methods to prevent authorities from detecting their activities, including failing to report transactions to AUSTRAC; concealing the identity of their clients and the overseas recipients; using other remitters to reduce the size of the international transfers and conceal the frequency of the international transfers; and paying airline pilots to physically carry large amounts of cash overseas.

105. The proprietors of the money remittance and associated businesses were charged with laundering over AUD\$93 million (approx US\$79 million). One of the airline pilots pleaded guilty to money laundering and was sentenced to four-and-a-half year's imprisonment.

3.3 Real Estate – ML or TF through the Real Estate Sector

HONG KONG, CHINA

Case Study – Laundering proceeds of drugs, including through real estate

106. In 2004 a joint operation between Hong Kong and overseas LEAs resulted in the neutralisation of a methamphetamine-manufacturing centre in an overseas jurisdiction. It was established that significant funds had been remitted from Hong Kong to the overseas jurisdiction where the manufacturing centre was located. Further investigation revealed the wife of the suspected mastermind was in possession of HK\$13 million (US\$1.7 million) in cash and a further HK\$9 million in cash and gems recovered from various safety deposit boxes under her control. After analysis, a total of HK\$32 million (US\$4.1 million) worth of assets, in the form of real estate, cash, funds and gems were restrained.

107. During the trial in early 2009 the judge was satisfied that the wife of the mastermind had reasonable grounds to believe that the funds represented the proceeds of crime. These grounds included her concealment of a large amount of cash at home and her failure to account for the source of her assets, including substantial interests in real estate, while having no discernable income and making no tax returns during the same period. The female was convicted of money laundering and sentenced to 5 years' imprisonment, while her husband remains at large. Another male, who was identified as the remitter of funds, was also convicted and sentenced to a shorter term of imprisonment.

Case Study – Real estate purchase

108. In 2007 Hong Kong Police arrested two males for illegal bookmaking activities; subsequent financial investigation established that one of the males held a number of bank accounts in Hong Kong through which proceeds, in the amount of tens of millions had been laundered over a 7-year period. Investigations identified assets worth HK\$20 million (US\$2.5 million) including cash, funds and 6 properties under the control of the two males. These assets were inconsistent with their legitimate income and lack of tax returns during the same period.

MALAYSIA

Case Study – Investment of proceeds of drug trafficking in real estate, businesses and motor vehicles

109. Malaysia's Narcotics Enforcement Agency seized drugs weighing almost one ton worth about RM254 million (US\$79 million) in street value from a local syndicate. The drugs were seized during transportation from their original source to another place for distribution. The operation resulted in the arrest of two brothers and an associate.

110. Asset investigations identified related assets held by 14 other family members as well as four business entities belonging to the main suspects. Investigation revealed that the syndicate has run trading operations to launder the drugs proceeds. One business venture included rearing ornamental fishes which was used to camouflage the drugs operation as the fish pond was used to hide and store drugs. The drugs proceeds were disguised as business profit and used to buy properties and channelled to other business. In total, the LEA has seized total assets amounting to RM22.4 million (US\$6.46 million) comprising of cash, eight houses and shop lots, sixteen plots of land and seven motor vehicles .

3.4 ML through Non-Profit Organisations (NPOs)

AUSTRALIA

Case Study – laundering proceeds of fraud, including through an NPO

111. Proceeds of fraud were laundered through a complex scheme which included layering through a church-based charity to disguise their illicit origin.

112. Person A was in control of a corporation's financial affairs and abused this position of trust by defrauding the company. He authorised and instructed staff to make electronic funds transfers from the company to his bookmakers' accounts. He instructed the bookmakers to direct excess funds and winnings from their accounts to his account or third party accounts. He instructed bank officers to transfer funds from his accounts internationally.

113. In order to layer and disguise the fraud, Person A instructed his lawyer to contact the beneficiary of the original international transfers to return the payments via wire transfers into the lawyer's trust account. Approximately AUD\$450,000 (US\$385,000) was returned in one international transfer to the lawyer's trust account. The lawyer then transferred AUD\$350,000 (approx US\$300,000) to a church fund in attempt to further hide the assets and was preparing to transfer the funds to an overseas account. Person A accessed these funds through structured withdrawals of AUD\$9,000 each within a nine-day period.

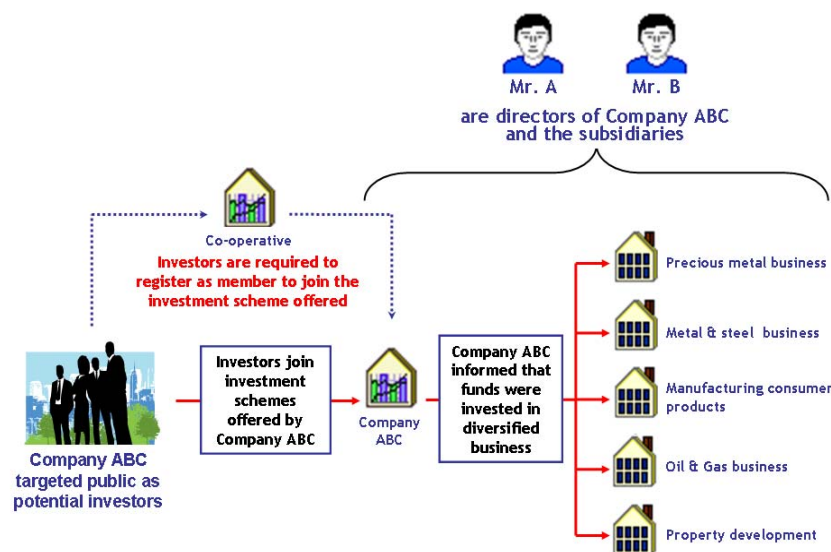
MALAYSIA

Case Study – laundering proceeds of illegal deposit taking through a cooperative

114. Company ABC offered investment schemes promising high and guaranteed returns to investors without regulatory approval. Company ABC claimed to invest funds in diversified businesses to ensure high returns. However, all the companies involved were actually subsidiaries to Company ABC that share the same directors, Mr. A and Mr. B. Investigation revealed that the subsidiaries were either dormant or had minimal business activities.

115. Mr. A and Mr. B subsequently established a co-operative to avoid the regulatory authority's intervention in their illegal deposit taking activities. Potential investors were enrolled as a member of the co-operative as a pre-requisite to join the investment schemes.

Under the Co-operative Act 1993, a co-operative is allowed to collect deposits from its members.



116. Company ABC maintained accounts with Bank X and Bank Y. Both Bank X and Bank Y were suspicious of the transaction patterns where the accounts received multiple cash deposits (in round figures) from unknown third parties. Bank X and Bank Y, which suspected that Company ABC could be receiving funds from investors, submitted STRs to the FIU on suspicion of Company ABC's involvement in illegal deposit taking activities. The analysis of the STRs' information also confirmed Company ABC's involvement in taking deposits illegally from the public and that it had frequently received funds from a neighbouring country as well, indicating the possibility that the illegal investment scheme had been expanded into the neighbouring country to recruit more investors to participate in the investment scheme.

117. Company ABC, Mr. A and Mr. B were prosecuted in court under Section 25(1) of the Banking and Financial Institutions Act 1989 for taking deposit from the public without license as well as Section 4(1) of the Anti-Money Laundering and Terrorism Financing Act 2001 for money laundering.

3.5 Structuring or 'Smurfing'

HONG KONG, CHINA

118. A Hong Kong male operated an illegal soccer and horse racing bookmaking operation. The total value of betting records seized and downloaded from computers at the scene amounted to HK\$2.4 million (US\$300,000). Financial investigations commenced in 2008 identified proceeds of approximately HK\$17 million (approx US\$2.1 million) had been structured and laundered through a number of different bank accounts. The male was convicted for both bookmaking and money laundering in June 2009. Confiscation is now being pursued in respect of assets worth HK\$5 million (approx US\$700,000) in the form of cash, property and funds.

3.6 Wire Transfers

JAPAN

Case Study – Proceeds by “Furikome” fraud

119. A money launderer provided a crime group which committed “furikome” fraud with a bank account with the function of mobile banking. This enabled customers to conduct bank transactions via mobile phone in order to acquire the money deposited by the fraud victims. The launderer was then able to acquire the deposited funds and transfer them to another false bank account. Investigations resulted in prosecution for concealing crime proceeds 88 times worth over 30 million yen (approx US\$320,000) from August 2004 to April 2008.

3.7 Use of Shell Companies / Corporations / Trusts

CANADA

120. Three typologies were found to be associated with the use of investment companies and trusts for suspected money laundering and terrorist financing purposes:

- 1) multi-jurisdictional structures of corporate entities and trusts;
- 2) involvement of non-financial intermediaries/professionals; and
- 3) use of nominees (individuals and businesses, including shell companies).

Case Study – Organised crime group adopting complex ML schemes

121. Information from law enforcement indicated that a large number of individuals and businesses, located in the greater Montreal area and with links to organized crime, were under investigation for money laundering.

122. Illicit revenues were invested through complex schemes in various businesses (including investment companies) that generated further profits. This was done with the assistance of nominees (family members and other associates) and through the use of trust accounts set up by lawyers and/or notaries, referred to as lawyers’ trust accounts.

Case Study – Laundering criminal proceeds through the use of investment companies and trusts

123. Many separately incorporated businesses were found to be located at the same address and their owners or directors were suspected to be nominees, sometimes with no apparent links to the organized crime group. Most of the companies were located in Canada but many financial transactions were conducted with offshore companies (Company A and Company B), some of them suspected of having been created for the sole purpose of concealing the criminal origins and ownership of the funds. As published on their Web sites, these two companies were reported to offer financial and investment services, which included the use of trusts, therefore allowing the clients to keep their own identity and that of beneficiaries completely confidential.

124. Highlights of the case:

- EFTs were ordered by or for the benefit of Company A, located in the Caribbean, and individuals and businesses from Europe, Asia, and the United States. Furthermore, EFTs were ordered by or for the benefit of Company A and investment/securities companies, as well as trust accounts (including lawyers’ trust accounts) located in Canada, some of them held by Company B. Company A also ordered EFTs to the benefit of a lawyer’s trust account held in the United States.

- Company C and its Director, Individual 1, both under investigation and suspected of being nominees for the organized crime group, were found to be associated with another three investment companies (including Company D) and two other individuals (Individual 2 and Individual 3). All entities were associated with the same specific address in Canada and were linked through their positions within each organization.
- Company C offered financial services and ordered EFTs to the benefit of Individual 4, a lawyer residing in the United States. Individual 4 and Individual 1 had the same last name and were suspected of being relatives. Company C also ordered EFTs to the benefit of real estate companies located in the United States.
- According to publicly available information, Individual 2 held the position of Director for both Companies C and D. In addition, Individual 3, a relative of Individual 2, was reported to be a major shareholder of Company D. A number of EFTs ordered by or for the benefit of Company D to an account in the United States held by Individual 3, as well as to another personal account in Canada also held by Individual 3.
- Individual 5, a notary, was also under investigation and suspected of facilitating the laundering of illicit funds through a trust account and a personal account. Individual 5 transferred funds from a personal account in Europe to the lawyers' trust account in Canada. Individual 5 was also the beneficiary of EFTs ordered by individuals and businesses mainly located in Europe and the United States.

125. Nominees and trust accounts set up by lawyers and/or notaries were used in abundance in this case. Some of the companies, located in various jurisdictions, were suspected of being shell companies and used solely for laundering funds generated by the organized crime group.

Red flags/indicators associated with this case:

- Frequent movement of funds between same trust accounts and bank accounts held by businesses located in various jurisdictions and with accounts in different financial institutions also located in various jurisdictions;
- Multiple and frequent transfers of funds between accounts held by businesses located at the same address and/or owned by the same individuals

HONG KONG, CHINA

Case Study – laundering proceeds from large-scale transnational frauds

126. Following receipt of information from a European jurisdiction, an investigation was undertaken into a suspected 'Boiler Room' fraud in which two Hong Kong-based company bank accounts were apparently used as temporary depositories for the proceeds of the fraud.

127. Investigations revealed a large number of overseas victims had been persuaded through high-pressure sales tactics to trade in worthless shares of various companies and were requested to transfer money to two company accounts in Hong Kong.

128. Analysis of the accounts showed that a total of nearly HK\$350 million (US\$45 million) had been deposited into one company account from June 2005 to when it closed in August 2006. A total of around HK\$200 million (US\$25 million) was deposited into the second account from September 2005 to when it closed in February 2007. A non-Hong Kong male resident was found to have established and opened a total of six companies (two incorporated in Hong Kong, the others in the BVI) and 13 accounts in seven different banks.

129. Five persons were arrested overseas in connection with the case and more than 1,000 complaints were received. The male operating these repository accounts was subsequently arrested in Hong Kong and later convicted of multiple counts of money laundering and was sentenced to a lengthy term of imprisonment.

3.8 Use of Offshore Companies/ Banks / Trusts (roles of TCSPs)

AUSTRALIA

Case Study – Use of trust and company service providers

130. Members of an organised crime syndicate acquired a number of companies registered in Belize through a Hong Kong-based trust and company service provider. These Belize offshore companies issued bearer share certificates with beneficial owners remaining anonymous. The Belize registered companies were acquired through a Hong Kong-based trust and company service provider. Offshore bank accounts denominated in Euros and United States dollars were established and substantial amounts of money were transferred in and out of those accounts. Funds were telegraphically transferred internationally and approaches were made to international banks to obtain loans. These transactions occurred outside the Australian financial system.

3.9 Use of Nominees, Trusts (onshore), Family Members or Third Parties

HONG KONG, CHINA

131. In 2006 Hong Kong commenced a joint investigation with neighbouring Jurisdiction A targeting the manufacturing and cross-border trafficking of dangerous drugs. Following raids and arrests in Jurisdiction A, follow-up financial investigation in Hong Kong identified family members, including the wife of the mastermind, as having received and laundered the proceeds through Hong Kong bank accounts. In the prosecution of the wife for ML evidence showed that HK\$4.2 million (US\$530,000) had passed through the wife's account between 2005-2007 that was inconsistent with her salaried employment as a schoolteacher and her tax returns. The wife was convicted and sentenced to 2 ¼ years imprisonment.

JAPAN

132. In a “Furikome” fraud, a member of the Boryokudan organised crime group concealed criminal proceeds by having the victim deposit money into an account under the name of another person but actually managed by the member of the Boryokudan. Funds were used for unpaid credit settlements, payments for renewal/withdrawal of member registration of an obscene website, repayment of a loan by relatives of the victim to the “black market finance” to purchase stock.

KOREA

Case Study – use of family members to launder proceeds of fraud

133. An STR was submitted on the ground that Person A withdrew a total of KRW 400 million (US\$300,000) twice from two branches of the same bank which was deposited in the name of Person A on the same day Person A opened an account at K bank.

134. The results of analysis showed that Person A is on trial after being arrested for embezzlement and the source of the funds is likely to be criminal proceeds obtained from embezzlement. The withdrawal was conducted to conceal the criminal proceeds, which was determined to be a money laundering activity and which was disseminated to the Public Prosecutors' Office. The older brother and Persons B and C, younger brothers, of Person A received respectively KRW 40 million and KRW 440 million with the knowledge that the money was acquired by embezzlement.

3.10 Use of ‘Gatekeepers’ Professional Services (Lawyers, Accountants, Brokers)

AUSTRALIA

Case Study – Allegation of role of trust and company service providers

135. A Sydney accountant was charged with 34 offences after she allegedly incorporated businesses in Vanuatu to help clients evade tax by laundering funds through a AUD\$10 million (US\$8 million) offshore tax evasion scheme. Authorities allege that the accountant promoted and implemented the scheme on behalf of her Australian-based clients, and have investigated businesses in Vanuatu as part of their ongoing probe.

136. The scheme allegedly involved the use of companies in Vanuatu, which were owned by the directors of Australian-based companies, to issue false invoices to the companies for services that were never actually provided. The companies then claimed tax deductions for the false expenses, while the funds held offshore were laundered back to the individuals in Australia to avoid being disclosed as income in tax returns.

137. To date, the investigation has traced AUD\$5.2 million allegedly laundered through the tax evasion scheme.

HONG KONG, CHINA

138. Hong Kong authorities note that it is common for syndicates to recruit third parties to open accounts to dissipate the proceeds of criminality. At the more sophisticated end of the spectrum, accounts opened by company secretarial firms are designed to cloak transactions and ultimate beneficiaries. The case is a useful test case whereby it was the first conviction of the operator of a company secretarial firm for money laundering and serves a useful warning to those business sectors that provide services and advice that may ultimately facilitate money laundering.

Case Study – Company secretaries setting up companies involved in advance fee frauds

139. In 2005 two overseas victims remitted sums of money amounting to ‘advance fee fraud’ to bank accounts operated by two Hong Kong companies, which had been set up in Hong Kong by a Hong Kong female, the director of a company secretarial firm. Further investigation revealed that the director and the sole bank account signatory for these companies was this female’s father. Between August 2005 and January 2006, 127 remittances totalling HK\$ 43.2 million (US\$5.5 million) were deposited into these accounts and then quickly remitted out, mostly to a neighbouring jurisdiction.

140. During the investigation, the female denied any offence, stating that a third person had hired her to set up the companies and open the bank accounts for receiving funds from allegedly legitimate overseas business clients. The female argued that she was merely providing legitimate company secretarial service, for a fee, and that all remittances were made according to instructions from a third person. Her father admitted signing as the director of the suspect companies but denied actual ‘dealing’ with the funds as both denied knowledge of either the source or ultimate beneficiary of the funds. In June 2009, both the female and her father were convicted of money laundering.

INDONESIA

Case Study – Using lawyer’s account to transfer illicit funds to third parties

141. Mr. A is a lawyer who opened a bank account which received remitted funds from Mr. B of US\$50,000. Investigations revealed that Mr B is a drug dealer sending money using his lawyer’s account. The transaction was described as “lawyer payment” based on information from the sender Bank. After receiving funds from Mr. B, Mr. A directly withdrew some of the funds and transferred the rest of the money to third parties (Mr. C and Mr. D). Mr. D also transferred some of fund that he received from Mr. B to Mr. C.

3.11 Use of Stored Value Cards

AUSTRALIA

Case Study – Laundering through stored value cards and structured wire transfers

142. FIU information assisted authorities investigating a man allegedly operating an illegal early release superannuation scheme. Information showed that the operator of the scheme had transferred the proceeds of the scheme overseas in structured amounts to avoid the AUD\$10,000 reporting threshold. He had also used cash to add more than AUD\$98,000 (approx US\$80,000) onto a stored value card.

143. The operator of the scheme was charged under the Superannuation Industry (Supervision) Act 1993, restricted from leaving Australia and prevented from providing any further financial services or disposing of any assets.

3.12 Purchase of Portable Valuable Commodities (Gems, Precious Metals)

CHINESE TAIPEI

Case Study – Purchase of gold bullion from proceeds of fraud

144. Mr C withdrew cash from his account at Bank A in the sum of \$43 million and \$4.9 million in two days. An investigation found that Mr C used a forged land ownership certificate to sell a piece of land to Developer A and received three cheques of Bank A in the sum of \$5.5 million, \$60 million and \$80 million respectively. Mr C deposited those cheques in an account at Bank A opened on the same day. Besides making cash withdrawals, Mr C wired \$100 million into his account at Bank B and used the money to buy 110 kg in gold bullion.

3.13 Association with Corruption

AUSTRALIA

Case Study – Using account to administer illicit business

145. The main suspect in this case wanted to establish a profitable company but did not want to be legally associated with the company due to a professional conflict of interest. An associate of the main suspect, a certified accountant with no criminal history, became the legal and apparent senior staff member of the company, while the main suspect actually directed and managed the company, albeit without any legal standing to do so.

146. The accountant administered both real and false invoices to create the illusion that funds moving through the company were from legitimate commercial activity. He also drew up cash cheques and cashed these on a weekly or fortnightly basis. Frequently, these cash withdrawals from company accounts were for amounts greater than the AUD\$10,000 transaction reporting threshold. Bank staff did not become suspicious of these regular withdrawals due to the apparently legitimate nature of the transactions. The accountant then gave this cash to the main suspect, allowing the main suspect to receive profits while remaining at arm's length from the official business of the company.

147. The main suspect attempted to launder the cash proceeds through direct deposits into a mortgage account, deposits into his mother's account, and the private cash purchase of a vehicle. He also attempted to launder cash through accounts and through a mortgage for real estate which was in his father-in-law's name, but which was in fact operated by him. The main suspect paid for improvements to this property with cash. Both the main suspect and his wife also gambled significant sums of money.

148. The company later became the focus of a corruption investigation which uncovered the illicit activities of the main suspect. The investigation further revealed that the company accountant was also a registered tax agent, a financial planner and a finance broker. In addition to the false invoicing and cash withdrawals he undertook for the welding company, he also supplied false documentation to clients wishing to misrepresent their financial status.

KOREA

Case Study – Laundering proceeds of corruption through purchase of certificates of deposit

149. Person A asked Person C to change a bank cheque (totalling KRW 300 million – US\$240,000) that he received as illegal political funds from Person B into 15 certificates of deposits (each worth KRW 20 million). On the next day Person A concealed and disguised the property by putting those certificates of deposits in a safe at X Bank where an acquaintance of Person A is a staff member.

CHINESE TAIPEI

Case Study – Laundering of corruption proceeds through complex bank transactions

150. Bank's customer XX's account balance was usually low. After \$8,320,000 was wired into XX's account from Bank A, XX came to the bank, saying that he would like to withdraw \$8,000,000 in cash. The bank teller advised him to wire transfer the money, but he insisted on withdrawing the money in cash. Because the bank did not have that much cash they asked XX to come back the next day.

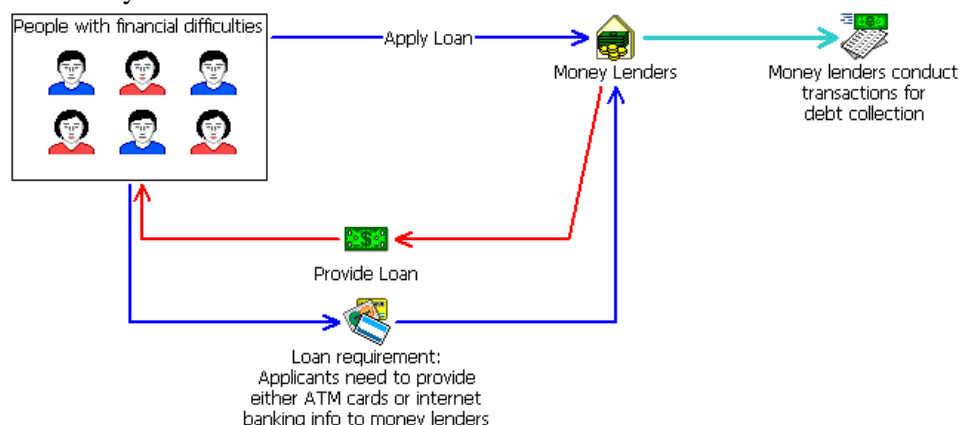
151. Investigation by the FIU found out that the members of local government borrowed the licenses of Construction Company B and several other construction firms to bid for projects with the local government authority. YY would leak the price ceiling in advance so that the award price ended up being exactly identical to the set ceiling. After the work was completed, the contractor deducted its costs and transferred the profit from an account at Bank A into the account of a third party at the same bank, from which the money was wired into the account of YY's half brother XX at Bank B. XX then withdrew the money in cash and gave it to YY.

3.14 Use of the Internet and New Payment Technologies

MALAYSIA

Case Study – Misuse of internet banking facilities

152. The borrowers are required to surrender either their ATM cards or disclose their internet banking accounts information when they take loans from money lenders to be used as collateral. The money lenders then gain full control of their borrowers' accounts and conduct the loan repayment transactions themselves. The purpose of this modus operandi is to ensure that the money lenders receive their loan repayments on time. For internet banking transactions, the same mobile numbers will be used for the online internet banking transactions authorisation code (TAC). The mobile numbers provided are suspected to be belonging to the money lenders or their runners or debt collectors who control the accounts.



153. The STRs received also identified instances whereby unscrupulous credit card merchants are providing money lending services to their customers. The merchants allow their customers to charge their credit cards purportedly for buying goods at their outlets. However, the customers are actually taking cash from the merchants instead of buying any goods when they charged their credit cards at the business premise. The merchants will then be paid by the bank on the credit card charges made by the customers. Ultimately, the credit card merchants are facilitating the customers to acquire cash loans using their credit card facilities from the banking institutions.

3.15 Criminal Knowledge of and Response to Law Enforcement / Regulations

AUSTRALIA

Case Study – Using currency exchange to launder

154. Investigators identified that a cash dealer, who was not compliant with AUSTRAC obligations, was laundering proceeds for a drug trafficking target. The remitter was accepting large cash deposits in excess of the AUD\$10,000 threshold and exchanging the cash for American Express traveller's cheques in amounts over AUD\$10,000.

155. The traveller's cheques were initially issued without being signed. Carbon copies of the sales receipts for the traveller's cheques were completed using false names and non-existent addresses. Documents obtained from subsequent search warrants revealed that the cash remitter had received several large cash deposits.

4. TRENDS OF MONEY LAUNDERING & TERRORISM FINANCING

4.1 Research or Studies Undertaken on ML/TF Methods and Trends

AUSTRALIA

Money Laundering and terrorism financing trends report

156. AUSTRAC publishes an annual Typologies and Case Studies Report, which includes terrorism financing typologies and indicators – see <http://www.austrac.gov.au/typologies.html>

157. AUSTRAC is finalising research reports on money laundering methodologies involving the use of solicitors and accountants and through the gold bullion / jewellery and motor vehicle dealer industries. Research is also being undertaken to compare the various money laundering methodologies and preferences for disposal of the proceeds of crime being employed by members of Asian organised crime groups across Australia. Plans are in place to extend this area of research to other organised crime groups including outlaw motor cycle gangs, Eastern European groups and Middle Eastern groups.

4.2. Association of Types of ML or TF with Predicate Activities

CHINA

158. The predicate activities of corruption are mainly associated with money laundering through the formal banking system, underground banking, cash transaction and real estate sector.

159. The predicate activities of smuggling are mainly associated with money laundering methods through false trading and underground money shops.

160. The predicate activities of drug trafficking are highly associated with cash transactions.

161. The predicate activities of financial fraud and violation of financial management order are highly associated with the counterfeiting, use of sophisticated or forged financial instruments and use of mass transaction accounts.

4.3 Emerging Trends; Declining Trends; Continuing Trends

AUSTRALIA

162. Analysis of case studies received from law enforcement agencies indicates that criminals continue to move and stockpile large amounts of cash outside of the formal banking system. Large amounts of cash have been carried out by couriers to return to principals of organised crime groups based overseas and/or to pay for commodities in which they are dealing. Cash is also used to invest in various types of assets including motor vehicles, real estate and jewellery.

163. Alternate remittance dealers continue to be utilised by criminals to assist in moving the proceeds of their illegal activity. Alternate remittance dealers offer a cheap, fast and efficient method of moving proceeds offshore. The criminals feel comfortable dealing with

members of their own community and feel they have a reduced risk of a STR being submitted on their activity.

164. Transnational crime: Many crime syndicates now operate across international borders, posing a direct threat to Australia. The case studies in this report show how Australia, no longer sheltered by its geographical remoteness, is being targeted by crime syndicates from many parts of the world, and how the criminal profits made in Australia are then moved overseas.

INDONESIA

165. Indonesian authorities note that corruption as a predicate offence is becoming increasingly significant compared to frauds. Money laundering from the proceeds of corruption occurs particularly through the misuse of state budget/district budgets by treasurers or government institutions.

166. An emerging trend in Indonesia is the proceeds of drug trafficking laundered through alternative remittance systems.

HONG KONG, CHINA

167. The primary sources of laundered funds in Hong Kong, China continues to be illegal gambling, frauds and financial crimes, loan sharking and vice. Cross-border telemarketing fraud is becoming a significant source of laundered funds; often victims are domiciled overseas and Hong Kong bank accounts are used to launder the proceeds. Investigation of these cases continues to present a challenge to the police due to the fact that the crime is often multi-jurisdictional and proceeds are quickly transferred out of Hong Kong.

JAPAN

168. The most common predicate offences leading to money laundering in Japan are “black market finance”, followed by fraud such as “Furikome” fraud. The third most common predicate offences related to distribution of obscene objects, followed by opening a gambling place for profit and habitual gambling.

169. Japanese authorities noted a slight rise in the number of number of ML cases which involved “Boryokudan” organized crime groups. Such cases accounted for 36.4% of all money laundering cases in 2008.

PAKISTAN

170. Pakistan authorities note that in cases of corruption-related money laundering, the use of real estate and foreign bank accounts has been prominent. Use of Offshore banks / companies and cash couriers has also been detected.

171. In narcotics related money laundering, use of real estate (residential houses, plots, commercial plazas/ shops, agricultural land etc) and third party accounts is typically utilised.

THAILAND

172. Authorities in Thailand note a continuing trend in relation to drugs dealers hiring persons to open a bank account for a modes fee, then take over the ATM card and deposit book.

VIETNAM

173. Authorities in Vietnam note the following patterns of suspicious transaction reports are:

- ✚ Transferring money obtained by fraud or swindling in foreign countries to bank accounts opened in Vietnam for subsequent withdrawal;
- ✚ Cheating, amending or falsifying the contents of documents, address of the account's owner in order to transfer money into the account and withdraw thereafter;
- ✚ Deceiving people to pay charges for receiving award prizes into bank accounts in Vietnam by promising that they have won a prize in a lucky program;
- ✚ Transferring money by using credit or commercial contracts.

4.4. Effects of AML/CFT Counter-Measures

AUSTRALIA

Threshold Transaction Reports – Gambling Services

174. Previously, a risk existed where individuals could have funds sent to them from overseas to an Australian casino without them being identified as the beneficiary. Individuals could access the funds and only be reported when they cashed out gaming chips. Recent legislative change has seen the introduction of a new report type, Threshold Transaction Reports – Gambling Services (TTR-GS), which seeks to capture all value transfers linked to gaming services.

175. One case involved an Australian-based casino receiving over AUD\$3 million (US\$X) from overseas. The beneficiary of the funds was recorded as the casino, whereas the actual beneficiary was a casino patron. The casino had given the patron a facility to directly credit the casino bank account with fund transfers that the patron was able to access to either buy chips or use as spending money. Only when the patron cashed out chips were Significant Betting Transaction Reports (SBTRs) lodged with AUSTRAC.

176. With the move from the reporting type SBTRs to Threshold Transaction Reports – Gambling Services (TTR-GS), the casino now reports every cash transaction over the threshold linked to a gaming service. Now, each time a patron accesses funds deposited into the casino bank account to buy chips or withdraw cash, a TTR-GS is lodged with AUSTRAC.

MACAO, CHINA

CFT Measures

177. Macao, China considers risks of terrorist financing as extremely low in Macao but requires financial institutions to establish monitoring systems to detect and report TF-related STRs. Macao, China reports two typical cases of financial institutions monitoring and reporting potential TF-related STRs:

Case Study 1 – identifying possible proliferation financing using sanctions list and STR

178. A Bank has established a business relationship with customer A for several years and the transactions were mainly trade finance related. Recently the customer obtained a supplier in Country B which is under UN Resolution restrictions in relation to proliferation financing.

179. The customer approached the bank and requested to carry out a remittance transaction for settlement of trading business with a company located in Country B. The bank refused to carry out the transaction and reported the case to the FIU. After analysis, the trading transactions were found to be normal and outside the scope of the UN Security Council Resolution restriction. Feedback to the bank was made accordingly.

Case Study 2 - identifying possible TF using sanctions list and STR

180. A customer approached a bank and requested to carry out a TT to an individual in Country A. The IT monitoring system of the bank detected that the name of the beneficiary appeared in the sanction list of a UN Security Council Resolution.

181. However, due to the fact that no identification information was provided in the UN sanction list, the bank could not verify whether the beneficiary was the person concerned. Therefore, the bank refused to carry out the transaction and reported the case to the FIU. After analysis and follow up with relevant government agencies, it was verified that the beneficiary was not the person under sanction. Feedback to the bank was made accordingly.

5. FUTURE WORK

182. In 2010-11 the APG Typologies program will continue to support the Typologies Working Group, a regional typologies workshop, in-depth studies of priority typologies topics input to the typologies work of the FATF and other AML/CFT bodies.

183. During the 2010 APG Annual Meeting the APG Typologies Working Group considered and adopted proposals for in-depth work on ML associated with large-scale transnational frauds, as well as a project on TF vulnerabilities from non-profit organisations. APG delegates will also discuss ways in which the APG's experience of ML and human trafficking can be further researched, including by contributing to an ongoing project within the FATF Typologies Working Group.

184. The 2010 APG Typologies Workshop will be hosted by Bangladesh in October 2010. This important regional meeting in Dhaka will be an excellent opportunity for APG members and observers to discuss priority issues, as well as a chance to interact directly with the private sector on typologies issues. As in previous years, cross over issues between AML/CFT and anti-corruption will be a standing item on the typologies agenda.

185. Finally, the APG will continue its ongoing program of case study and other data collection relevant to developing effective typologies of ML and TF and to better understanding the nature of the criminal environment.