APG Yearly Typologies Report 2014

Asia/Pacific Group on Money Laundering

Methods and trends of Money Laundering and Terrorism Financing

Asia/Pacific Group on Money Laundering

Approved and adopted, 17 July 2014

APG Yearly Typologies Report 2014

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

Tel: +61 2 9277 0600
E Mail: mail@apgml.org
Web: www.apgml.org

CONTENTS

INTRODUCTION

Background

1. The Asia/Pacific Group on Money Laundering (APG) is the regional anti-money laundering/combating the financing of terrorism (AML/CFT) regional body for the Asia/Pacific. The APG produces regional typologies reports on money laundering (ML) and terrorist financing (TF) techniques to assist governments and other AML/CFT stakeholders to better understand the nature of existing and emerging ML and TF threats and pursue effective strategies to address those threats. Typologies studies assist APG members to implement effective strategies to investigate and prosecute ML and TF, as well as design and implement effective preventative measures. When a series of ML or TF arrangements are conducted in a similar manner or using the same methods, they are generally classified as a "typology".

2. The Yearly Typologies Report is an important output that is provided under the APG's Strategic Plan and the APG Typologies Working Group Terms of Reference. It 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.) involved in implementing preventative measures including customer due diligence and suspicious transaction reporting.

3. 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 a case study collection 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 2013-2014

4. The APG Typologies Working Group continued its work in 2013-14 under the leadership of India and Fiji as Co-Chairs. In July 2013 the APG Typologies Working Group met to determine the work program for the year, including the conduct of a joint APG and Eurasian Group (EAG) Typologies Workshop in September 2013 hosted by Mongolia in Ulaanbaatar.

5. The case studies featured in this report are only a small slice of the work going on across the Asia/Pacific and other regions to detect and combat ML and TF.

6. The report contains a selection of illustrative cases of various typologies gathered from APG members' reports as well as open sources. 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. Many cases cannot be shared publicly due to their sensitive nature or to ongoing legal processes.

1. WORKSHOPS AND PROJECTS UNDERTAKEN BY APG IN 2013 - 2014

1.1 2013 APG Typologies Workshop and Capacity Building Seminars

7. Each year the APG brings together AML/CFT practitioners from investigation and prosecution agencies, financial intelligence units, regulators, customs authorities and other relevant organisations to consider priority ML and TF risks and vulnerabilities. In recent years APG has taken the opportunity to combine the Typologies Workshop with Capacity Building Seminars to share practitioners' experience on priority topics.

8. The agenda of APG Typologies and Capacity Building Workshops is designed to achieve a number of objectives:

   - Bring together the APG community of practitioners to share experience and foster networks of cooperation;
   - Support research being undertaken by the APG Typologies Working Group;
   - Facilitate APG members to contribute to Financial Action Task Force (FATF)-led typologies studies; and
   - Share best practice and strategies for practical application of AML/CFT measures related to previous typologies studies and other implementation issues.

9. Mongolia hosted the joint APG and EAG Typologies Workshop in Ulaanbaatar from 23 to 27 September 2013, which was attended by more than 210 delegates from 38 APG and EAG members and observers, and 23 private sector organisations. The workshop was jointly chaired by Mr Razim Buksh, Director of Fiji FIU (APG Typologies WG Co-Chair); Mr Balesh Kumar, Special Director, Enforcement Directorate, India (APG Typologies WG Co-Chair); Mr Pavel Livadny, Deputy Head, State Secretary, Financial Intelligence Unit, Russian Federation (EAG Legal Issues WG Co-Chair); Mr Igor Voluevich, Head of Department, Financial Intelligence Unit, Russian Federation (EAG Typologies WG Co-Chair); and Mr Bazarragchaa Tumurbat, Head, Financial Intelligence Unit, Mongolia. The agenda included a range of topics designed to support on-going FATF projects, as well as APG and EAG work.

10. Typologies discussion topics included:

    - The Risk of Terrorist Abuse in the NPO Sector;
    - Illicit Financial Flows and the Use of AML/CFT Tools to Combat Corruption; and
    - ML and TF Risks and Vulnerabilities Associated with Gold Production, Movement, Markets and Trade.

11. The Capacity Building Workshop involved three technical seminars, which covered:

    - Understanding and Managing Risk;
    - Financial Inclusion; and
    - AML/CFT and New Technologies – Understanding Virtual Currencies.

12. The Capacity Building Workshop aimed to expand partnerships between the public and private sectors on AML/CFT typologies and private sector involvement in national risk assessments. It was also an opportunity to strengthen the profile of AML/CFT risk management, enhance industry cooperation on AML and draw on industry experience in the selection and conduct of studies of ML and TF typologies.

13. The outcomes from the APG Typologies and Capacity Building Workshops in Mongolia will play a positive and practical role in improving regional cooperation and countermeasures for AML/CFT across the APG and EAG regions.

1.2 2014 Pacific Typologies Workshop

14. The APG Typologies Workshop on Trans-Pacific Drug Trafficking was held in Auckland, New Zealand, on 29-30 January, hosted by the Government of New Zealand and the Department of Justice. The workshop was a key element of the APG Typologies Working Group project on *ML/TF Risks Associated with Trans-Pacific Drug Trafficking Routes* being led by Tonga and Vanuatu.

15. The meeting was jointly chaired by the project co-leads, Tonga and Vanuatu, and was attended by 48 delegates from 15 APG member and observer jurisdictions and five international and regional organisations. Discussion topics included:

- Sharing regional and global experience of drug trafficking, including the financial investigation issues and challenges.
- Money laundering (ML) and terrorist financing (TF) risks and vulnerabilities associated with trans-Pacific drug trafficking.
- Individual cases, red flag indicators and patterns and trends within (and affecting) the Pacific, including the involvement of organised crime networks.

16. The outcomes from the 2014 Pacific Typologies Workshop will play an important part in enhancing the typologies project over 2014-2015.

1.3 Status of current projects and possible new projects

17. The APG/FATF joint project on *Gold – Money Laundering and Terrorist Financing Risks and Vulnerabilities* is being co-led by India and Australia and is being carried out over the 2013-2015 period. The project team includes representatives from: Argentina, Australia, Bahrain, Bangladesh, Belgium, China, Denmark, Ecuador, Germany, Ghana, Haiti, Hong Kong, India, Iraq, Malaysia, Nepal, Pakistan, Peru, Qatar, Russia, St Kitts-Nevis, Switzerland, Thailand, UAE, USA, Zimbabwe, APG, CFATF, EAG, Egmont Group, ESAAMLG, FATF, GAFISUD, GABAC, GIABA and MENAFATF.

18. The project is examining the characteristics of gold production, movement, trade and markets with a focus on the illicit risks. The aim of the project is to identify the techniques, trends and methods of ML and TF associated with gold; the risks and vulnerabilities, problems and possible solutions for investigations of ML/TF and predicate offences associated with gold; and identify 'red flag' indicators that could assist various stakeholders, including designated non-financial business and professions (DNFBPs), financial institutions and others to capture relevant data and, as appropriate, identify reporting suspicious activity associated with the precious metals market.

19. The APG is also progressing four Pacific-focused typologies projects to be completed over the 2013-2015 period: *ML and Frauds in the Pacific,* being co-led by Fiji and Vanuatu; *Recovering the Proceeds of Corruption in the Pacific,* being co-led by Papua New Guinea and Tonga, in conjunction with the Pacific Islands Law Officers' Network (PILON); *ML/TF risks Associated with Offshore Centres in the Pacific*, being co-led by the Cook Islands and Samoa; and *ML/TF Risks Associated with Trans-Pacific Drug Trafficking Routes,* co-led by Tonga and Vanuatu.

20. Over the past year the APG has contributed to several FATF typologies projects, including one on *Financial Flows linked to illicit production and trafficking of Afghan drugs and associated ML/TF activities* and another on *The Risk of Terrorist Abuse in the Non-Profit Organization*

(NPO) Sector, as well as to other on-going FATF and FATF-style regional body (FSRB) projects.

Private Sector Outreach on Typologies

21. The APG's commitment to engage with the private sector is contained in the *APG Strategic Plan 2012-2016*, as well as in the *2013 Revised Terms of Reference for the APG Typologies Working Group*. The APG recognises the importance of close cooperation with the private sector to assist in identifying and understanding the AML/CFT risks that APG members face, as well as the implementation challenges faced by the private sector in relation to the risk-based approach, strengthening their compliance networks and the impact of new technologies.

22. In July 2013 APG members endorsed revised *Terms of Reference for the Typologies Working Group* which provided for the formation of a private sector contact group. This contact group will, from time to time, involve representatives of financial institutions, DNFBP industry associations, audit firms and payment system operators.

23. The purpose of the private sector contact group is consultative and two-fold: (i) to exchange information on typologies and implementation issues including, *inter alia*, how governments can assist the private sector to assess risk; how the private sector can assist government agencies when conducting national or sectoral risk assessments; what measures can help support strong and professional AML/CFT compliance in the sector; identifying the opportunities and good practice for intra-industry cooperation; how the APG and private sector can constructively engage to strengthen typologies work; and identifying and contributing to priority typologies topics, events and research in order to improve understanding of money laundering and terrorist financing and new developments in the private sector; and (ii) to encourage representatives of the private sector to participate in the yearly Typologies Workshop.

24. The APG continued to pursue dialogue between government and private sector representatives in 2013-2014, building on the contact during the 2012 typologies workshop. During the Joint APG/EAG Typologies and Capacity Building Workshops in Mongolia, sessions were held with the private sector to help set the scene for ongoing cooperation between APG and the private sector on ML and TF risk assessments and responses. Discussions covered the revised FATF Recommendations and requirements with respect to national risk assessments, including the role of the private sector.

25. Several financial sector representatives also shared experience on the private sector approach to risk assessment (including enterprise risk, product risk, country or market risk and customer risk), as well as discussing effective cooperation between the public and private sector in identifying and managing risk. The discussions also covered the need for the public sector agencies to understand and support innovation and new technologies, as well as links to financial inclusion.

26. In support of these discussions, two technical seminars were conducted in association with private sector participants. The *Financial Inclusion – Meeting the Challenges* seminar confirmed that the goals of financial inclusion and risk-sensitive AML/CFT measures are mutually reinforcing. The seminar shared regional experiences in addressing financial exclusion and discussed the use of the FATF/APG/ World Bank Guidance Paper that focuses on facilitating access to formal services for financially excluded and underserved groups[1].

27. The seminar on *AML/CFT and New Technologies – Understanding Virtual Currencies* was a joint seminar with private sector representatives and discussed what virtual currency is and how

[1] *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*, February 2013, available on the APG website at http://www.apgml.org/documents/default.aspx?s=date&c=9

it works. Information was shared on the experience of virtual currency issues across the APG and EAG regions and case studies were presented to assist in identifying the ML/TF risks and vulnerabilities of virtual currencies and what opportunities exist for cooperation between public and private sector entities. The seminar was well attended and identified virtual currencies as a new area requiring further attention. The FATF Research Trends and Methods Working Group is currently carrying out a short-term study on this topic.

2. OVERVIEW OF FATF AND FATF-STYLE REGIONAL BODIES' TYPOLOGY PROJECTS

28. A range of typology studies have been published in 2013 and 2014 by the FATF and several other FSRBs, including:

2.1 FATF Typology Projects

Terrorist Financing in West Africa[2]

29. This report identifies the methods used by terrorists, terrorist groups, and their supporters in the West African region to collect, transfer and utilise funds. The report aims to help policymakers, regulatory and enforcement authorities as well as reporting entities to gain a better understanding of the nature and dynamics of terrorist financing in the West African region.

30. Based on case studies, the research project identified four main categories of typologies of methods and techniques used by West African terrorist and terrorist groups to support terrorist activities:

- Terrorist financing through trade and other lucrative activities;
- Terrorist financing through NGOs, charity organisations, and levies;
- Terrorist financing through smuggling of arms, assets and currencies by cash couriers; and
- Terrorist financing through drug trafficking.

The role of Hawala and other similar service providers in money laundering and terrorist financing [3]

31. This typology report seeks to provide a facts-based review of hawala and other similar service providers (HOSSPs) and the extent of their vulnerability to money laundering and terrorist financing.

32. This typology reviews three major types of HOSSPs:

- Pure traditional (legitimate) ones;
- Hybrid traditional (often unwitting) ones; and
- Criminal (complicit) ones.

33. Distinct ML/TF risks apply to each and there are several reasons why HOSSPs continue to pose a ML and TF vulnerability. These include:

- A lack of supervisory will or resources;
- Settlement across multiple jurisdictions through value or cash outside of the banking system in some cases;
- The use of businesses that are not regulated financial institutions; and
- The use of net settlement and the co-mingling of licit and illicit proceeds.

[2] http://www.fatf-gafi.org/media/fatf/documents/reports/TF-in-West-Africa.pdf
[3] http://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf

34. While the settlement through value or trade that masks the individual fund transfers is a source of vulnerability, the most significant reason for concern is lack of supervisory resources and commitment to effective regulation.

Money laundering and terrorist financing through trade in diamonds[4]

35. This joint FATF and Egmont Group typologies report identifies the ML/TF vulnerabilities and risks of the "diamond pipeline", which covers all sectors in the diamond trade: production, rough diamond sale, cutting and polishing, jewellery manufacturing and jewellery retailers.

36. Some of the risks and vulnerabilities of the diamonds trade, identified in this report are:

- Global nature of trade - The trade in diamonds is transnational and complex, thus convenient for ML/TF transactions that are, in most cases, of international and multi-jurisdictional nature.
- Use of diamonds as currency - Diamonds are difficult to trace and can provide anonymity in transactions.
- Trade Based Money Laundering (TBML) - The specific characteristics of diamonds as a commodity and the significant proportion of transactions related to international trade make the diamonds trade vulnerable to the different laundering techniques of TBML in general and over/under valuation in particular.
- High amounts - The trade in diamonds can reach tens of millions to billions of US dollars. This has bearing on the potential to launder large amounts of money through the diamond trade and also on the level of risks of the diamonds trade.
- Level of awareness - Law enforcement and AML / CFT authorities, including financial intelligence units (FIUs), have limited awareness of potential ML/TF schemes through the trade in diamonds.

37. The report concludes that the diamonds trade is subject to considerable vulnerabilities and risks.

Virtual Currencies: Key Definitions and Potential AML/CFT Risks[5]

38. The FATF conducted research into the characteristics of virtual currencies to make a preliminary assessment of the ML/TF risk associated with this payment method. An important step in assessing the risks and developing an appropriate response is to have a clear understanding of the various types of virtual currencies and how they are controlled and used. This report establishes a conceptual framework of key definitions, which could form the basis for further policy development.

39. The legitimate use of virtual currencies offers many benefits such as increased payment efficiency and lower transaction costs. Virtual currencies facilitate international payments and have the potential to provide payment services to populations that do not have access or limited access to regular banking services.

40. However, other characteristics of virtual currencies, coupled with their global reach, present potential AML/CFT risks, such as:

- the anonymity provided by the trade in virtual currencies on the internet
- the limited identification and verification of participants
- the lack of clarity regarding the responsibility for AML/CFT compliance, supervision and enforcement for these transactions that are segmented across several countries

[4] http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf
[5] http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

- the lack of a central oversight body

41. The report provides law enforcement examples a number of examples of money laundering offences involving virtual currencies to demonstrate how this payment method has already been abused for money laundering purposes.

Risk of Terrorist Abuse in Non-Profit Organisations [6]

42. This typologies report examines in detail, how and where NPOs are at risk of terrorist abuse. The report uses case studies as well as input collected from law enforcement, other government actors and NPOs themselves to increase awareness of the methods and risk of abuse for terrorism of the NPO sector, both domestically and internationally.

43. The report highlights that NPOs are at risk of being abused for terrorism at different levels: from the misappropriation of street-level fundraising to the infiltration of terrorist organisations at the programme delivery level to promote their ideology.

44. Summary of analytical findings:

    1. The NPO sector has interconnected vulnerabilities, and terrorist entities seek to exploit more than one type of vulnerability. In the cases analysed for this project, the diversion of NPO funds by terrorist entities was a dominant method of abuse. However, other types of non-financial abuse such as the abuse of programmes or the support for recruitment appeared regularly as well.

    2. The NPOs most at risk appear to be those engaged in 'service' activities, and who operate in a close proximity to an active terrorist threat. This may refer to an NPO operating in an area of conflict *if* there is an active terrorist threat. However, this may also refer to an NPO that operates domestically, but within a population that is actively targeted by a terrorist movement for support and cover. In both cases the key variable of risk is not geographic, but the proximity to an active threat.

    3. Because of the nature of the threat and the resulting nature of state responses, cases of substantial risk are an important source of information for typologies analysis.

    4. The amalgamation of many types of information held by different actors was an important factor in detecting cases of abuse or identifying substantial risk.

    5. Disruption of abuse, or the mitigation of substantial risk, was dealt with through multiple means including, but not limited to, criminal prosecution. Administrative enforcement, financial penalties, and targeted financial sanctions played important roles in disruption of abuse.

Financial flows linked to the production and trafficking of Afghan opiates[7]

45. This report aims to raise awareness about the financial flows related to the Afghan opiate trade. Afghanistan is the world leader in the production and trafficking of opiates: generating revenues estimated to be as high as USD 70 billion. Despite international efforts, the cultivation of opium poppies in Afghanistan continues, and even increased significantly in southern parts of Afghanistan to reach a record high by 2013.

46. Little information exists about the "business model" of the Afghan opiates trade, but what is known is that globally, only a fraction of drug related funds or assets are confiscated while almost all drug profits are integrated into the world's legitimate financial system.

[6] http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf
[7] http://www.fatf-gafi.org/media/fatf/documents/reports/Financial-flows-linked-to-production-and-trafficking-of-afghan-opiates.pdf

47. This report analyses how the financial transactions related to the Afghan opiates trade are conducted. The report finds that generally, the opiates and the associated financial flows do not follow the same routes. The majority of revenues generated by the trade in Afghan opiates is moved through, and possible stored in, so called "financial centres", usually involving money or value transfer services (MVTS). This report also identifies other methods used by the opiate traffickers to transfer funds and facilitate distribution of the opiates.

48. Another finding is that the Afghan Taliban are heavily involved in the opiates trade, either through trafficking or profiting. The growing trade in opiates will soon be one of their leading sources of income, providing them with the financial means to become a major threat to the national security of Afghanistan and the wider region.

49. This report, and in particular the case studies provided, will assist in the detection of opiate-related financial transactions. It also provides financial centres with information about the factors that make them attractive and vulnerable to financial transactions involving proceeds of drug trade or other crimes.

2.2 EAG - The Eurasian Group

Money Laundering Through the Securities Markets[8]

50. The report notes that the sheer magnitude of transactions in securities markets and the ease of moving funds make these markets an obvious target for laundering illegal funds. Further, the securities market can also be used to generate illegal proceeds through insider trading and market manipulation.

51. **Suspicious Transactions Triggers/Indicators**

A. Customer Identity:

- False identification documents.
- Absence of information or identification documents which could not be verified within a reasonable time-frame.
- Non face to face customers.
- Doubts over the real beneficiary ownership of the account.
- Accounts opened with names very close to other established business entities.
- Suspicious background or links with known criminals.
- Having business contact with high-risk countries and regions in terms of money laundering.
- Large number of accounts having a common account holder, introducer or authorized signatory with no rationale.
- Refusal by the customer to provide the data necessary for customer identification.
- Excessive focus of the customer on issue of confidentiality.
- Transactions carried out which raise suspicion that the customer has acted on behalf of persons on whom transaction prohibition is imposed by the securities regulator.
- Issuance of an instruction to open UIN for legal persons registered in offshore zones and countries not involved in international cooperation in the area of combating money laundering and terrorist financing.

[8] http://www.eurasiangroup.org/files/Typologii%20EAG/WGTYP_2013_4_eng_copy0.pdf

- Location or registration of the customer or one of the participants of the transaction in a country not involved in international cooperation in the area of combating money laundering and terrorist financing.
- Customer requesting to change customer information but providing documents that look like tampered or counterfeited ones.

B. Transactions in customer accounts:

- Use of different accounts by customer alternatively.
- Investment proceeds transferred to a third party.
- Constant transfer of securities and/or cash to the accounts of persons who have no relation with the customer within several intermediary institutions without any reason.
- Transfers involving different depository accounts.
- Unusual activity compared to past transactions.
- Sudden activity in dormant accounts.
- Unexplained transfers between multiple accounts with no rationale.
- Customer trades in securities in large amounts within a short time after opening account and closes the account soon afterwards.
- Account used for circular trading.
- Transactions appear unusual or unjustified in complexity and are different from the accepted practice.
- No economic rationale or bonafide purpose for transactions/trades of substantial amount synchronized/matched without any economic rationale.
- Appears to be a case of insider trading or front running.
- Transactions reflect likely market manipulations for e.g., high delivery turnovers in particular scrips, trading in illiquid securities, concentration of trades on the exchange etc.
- Abrupt termination of account or transaction without any reasonable cause or independent of market conditions.
- Value of transactions just under the reporting threshold amount in an apparent attempt to avoid reporting.
- Large sums being transferred from overseas for making payments.
- Inconsistent with the apparent financial standing/business purpose of the customer.
- Inconsistency in the payment pattern by customer.
- Trades constitute significant proportion of the gross traded volume for the market for the day for the contract.
- Trades resulting in unreasonable gains/loss by giving the impression of not seeking profit, taking no notice of the risks and costs of investments, and carrying out transactions to this effect.
- Transactions of substantial amount through off-market mode in a single scrip/several scrips/off-market transactions invariably preceded/succeeded by on-market transactions.
- Simultaneous orders for purchase and sale of securities and other financial instruments placed by the customer at prices which significantly differ from the current market ones for similar transactions (operations).
- Disregard by the customer of the undoubtedly more favourable terms of service provision, as well as the offer by the customer of an unusually high commission from the one usually charged for such service in the securities market.

- Introduction by the customer of significant, last-minute changes to the previously agreed upon transaction pattern.
- Unwarranted insistence on the part of the customer to speed up the execution of a transaction.
- A customer with no trading or low trading volume requesting large amount of fund to be transferred to another person's account, without obvious transaction end or use.
- Customer frequently entering into long position and short position, both of which are entered into at the same time and almost at the same price for equal or close to equal amounts for the same underlying futures contract, then closing these positions afterwards and acquiring receipts.

C. Funding of transactions:

- Source of funds used in transactions in securities is doubtful.
- Frequent changes in the bank mandate for pay outs.
- Payment through multiple pre-funded instruments having a value that is lower than the reporting threshold.
- Purchase of securities or other capital market instruments having significant value by using cash which is not in accordance with the familiar activities of the customer.
- Frequent cash receipts and payments with amounts close to the large-value transaction threshold for unknown reasons.
- Customer's capital account experiencing frequent receipts and payments while the securities account has been idle for a long time.
- Customer having no or only a small volume of futures trading but receiving funds and making payments in large amounts through capital account.
- Legal persons, other organizations and firms created by self-employed persons frequently and within a short period of time receiving remittances that are obviously unrelated to its range of business, or natural person customers frequently receiving remittances from legal persons and other organizations within a short period of time.

2.3 ESAAMLG – The Eastern and Southern Africa AML Group

***Typologies Report On Money Laundering Through the Real Estate Sector in the ESAAMLG Region*[9]**

52. The study looked at vulnerabilities, methods and/or channels used by criminals in the Real Estate Sector with the intention to assist member countries to put in place measures that can mitigate the ML/FT risks in the sector.

53. The following red flags/indicators were identified:

- Large and unexplained transfers or deposits;
- Unusual bank transactions;
- Repeated unexplained transfers or deposits;
- Use of unnecessary 3rd parties during property transactions;
- Use of unusual methods of payment/settlement;
- Complicated proposals where identity of the beneficial owner or source of funds or both is not clear, which gives the impression that they are designed to mislead or the transaction;
- Complicated structures involving multiple jurisdictions for no apparent reason;

[9] http://www.esaamlg.org/userfiles/file/TYPOLOGIES-REPORT-ON-ML-THROUGH-THE-REAL-ESTATE-SECTOR(1).pdf

- Reluctance by any of the parties to a transaction to complete the relevant documents or provide required proof;
- Operating unregistered estate agents;
- Use of cash to facilitate transactions regardless of amount involved;
- Use of Shell companies to buy property;
- Foreign nationals making huge investments directly in real estate using locals;
- Fund structuring;
- Liquidating mortgagees using lump sum payments before time;
- Payments of long leases of say one year by a tenant whose economic background is not sound;
- Transactions by individuals who unexpectedly repay problematic loans or mortgages or who repeatedly pay off large loans or mortgages early, particularly if they do so in cash;
- Transactions involving legal persons which, although incorporated in the country, are mainly owned by foreign nationals who may not be resident for tax purposes;
- Transactions involving legal persons whose addresses are unknown or are merely correspondence addresses (e.g. a shared office or shared business address or telephone), or where the details are believed to be or likely to be false;
- Establishment of legal persons to hold properties with the sole purpose of placing a front man or straw man between the property and the true owner;
- Transactions relating to the same property or rights that follow in rapid succession (e.g. purchase and immediate sale of property), which often entail a significant increase or decrease in the price compared to the initial purchase price;
- Transactions entered into at a value significantly different (much higher or much lower) from the real value of the property or differing remarkably from market values.

2.4 GAFISUD - The Financial Action Taskforce of South America

54. No new reports published in the last year.

2.5 GIABA – The Inter-Governmental Action Group Against Money Laundering in West Africa

***The Nexus between Small Arms and Light Weapons and Money Laundering and Terrorist Financing in West Africa*10**

55. This report presents the key findings of a study commissioned by GIABA to explore the relationship between illicit trade in small arms and light weapons (SALWs), on one hand, and ML and TF, on the other hand, in west Africa.

56. GIABA commissioned this study primarily to provide greater understanding of how illicit SALW trafficking is fuelling and is being sustained by ML/TF in the region. The report shows the typologies and prevalence of illicit SALW trafficking, and reveals the emerging patterns of its relationship to ML/TF in all 15 member States of the Economic Community Of West African States (ECOWAS).

2.6 The Egmont Group

57. See the joint FATF and Egmont typologies report on ***Money laundering and terrorist financing through trade in diamonds*** above.

[10] http://web.giaba.org/media/f/613_519_GIABA%20SALW%20Nexus-final.pdf

2.7 MONEYVAL

Typologies report on the use of online gambling for money laundering and the financing of terrorism purposes[11]

58. The report provides an overview of the online gambling sector in MONEYVAL countries, including the extent and type of gambling offered and the ML/FT risks and vulnerabilities associated with online gambling and the methods of payment used.

59. A list of typologies, red-flag indicators and vulnerabilities is presented, based on the experiences shared by public and private stakeholders with the project team.

60. The report concludes that one of the major vulnerabilities is directly linked to unregulated online gambling. Additionally, given that online gambling, by its nature, is conducted anonymously, the use of false or stolen identities is less likely to be detected. The use of alternative payment systems to credit online gambling accounts systems may also augment the risk of ML/FT. Challenges also arise due to the cross-border nature of online gambling. The regulation and supervision of online gambling remain the strongest mitigating factors to prevent abuse.

The postponement of financial transactions and the monitoring of bank accounts[12]

61. The report examines the experience of competent authorities in participating countries in effectively postponing suspicious financial transactions and monitoring bank accounts. It analyses the use of available procedures and mechanisms and sets out practical problems encountered by relevant authorities in this context. It includes a number of cases, red flags and indicators and formulates recommendations aimed at assisting competent authorities in making a more efficient use of their powers.

62. The report concludes that the monitoring of bank accounts has proved to be an effective tool in tracing criminal assets and that in cases of suspicion of terrorist financing, this is probably one of the most effective investigative instruments. Better knowledge of the methods and practices successfully used in this context by various financial intelligence units and law enforcement agencies and strengthened exchange of experiences and cooperation with the private sector can only lead to more effective financial investigations and successful identification, seizure and subsequent confiscation of proceeds of crime.

2.8 Others

Pirate Trails: Tracking the Illicit Financial Flows from Piracy off the Horn of Africa[13]

63. This study by the International Criminal Police Organization, United Nations Office on Drugs and Crime and World Bank attempts to understand the illicit financial flows from pirate activities off the Horn of Africa. The study focused on: Djibouti, Ethiopia, Kenya, Seychelles, and Somalia.

64. The study (i) analyses how much money is collected in ransom payments; (ii) how and to whom this money - the proceeds of piracy - are distributed; (iii) how these proceeds may be invested.

[11] http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2013)9_Onlinegambling.pdf

[12] http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2013)8_Postponement.pdf

[13] http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTFINANCIALSECTOR/0,,contentMDK:23491862~pagePK:210058~piPK:210062~theSitePK:282885,00.html

Key Findings

Who benefits from the proceeds of piracy?

65. Pirate Financiers stand in the middle of the piracy network. They are "The Money Kingpins", investors and beneficiaries of the piracy business. On average, they collect from 30 to 50% of total ransom, working individually or as a group.

66. Low Level Pirates, "The Foot Soldiers", typically receive a standard fee of US$30,000 to $75,000 per ship, which only amounts to 1% - 2.5% of an average ransom payment.

67. The local community provides goods and services to pirates, including food, repair services and khat which is a legal drug in Somalia.

How are the proceeds of piracy moved, invested, and used?

68. The main reported locations of pirate financiers' assets, suggest that contrary to conventional wisdom, many investments of proceeds of piracy are actually made within Somalia. The proceeds are typically moved by cross – border cash smuggling, trade based money laundering, bank wire transfer and the abuse of Money of Value Transfer Services.

Investments from the proceeds of piracy

69. Pirate financiers invest into a range of sectors, both legitimate business activities (in order to launder money) and criminal activities:

    - some of these proceeds are recycled into financing criminal activities, including further piracy acts, human trafficking, including migrant smuggling, and investing in militias and military capacities on land in Somalia;
    - proceeds from piracy also find their way into the khat trade particularly in Kenya, where the khat trade is not monitored and therefore the most vulnerable to this risk.

How to Break this Cycle?

70. There is need for a strong commitment by countries in the region to work together to:

    - better monitor the financial flows from piracy and share regional financial intelligence;
    - improve cross-border controls, especially border entry - exit points; and
    - improve regional cooperation and international support.

3. TRENDS IN MONEY LAUNDERING & TERRORISM FINANCING

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

AUSTRALIA

71. AUSTRAC (Australia's FIU) produces research on current and emerging money laundering and terrorism financing vulnerabilities to help both industry and government partners detect threats.

72. AUSTRAC's *2013 Typologies and Case Studies Report* examines typologies used to enable and commit transnational crimes and tax evasion which are currently of interest to law enforcement, namely gold bullion, international trade and politically exposed persons (PEPs).

73. All seven typologies and case studies reports (2007 – 2013) are available on the AUSTRAC website, http://www.austrac.gov.au/typologies.html.

74. In addition, AUSTRAC is preparing a national risk assessment on terrorism financing, expected to be completed in 2014. Australia also assisted with the joint FATF/Egmont project on diamonds.

FIJI

75. The Fiji FIU has conducted only basic and informal research on ML/TF methods and trends. The Fiji FIU continues to provide this information through its annual reports. The 2012 Annual Report included case studies from suspicious transaction reports and three major case studies on successfully prosecuted money laundering cases in Fiji. The report also includes emerging, continuing and declining money laundering trends. *Fiji FIU 2012 Annual Report* is available on Fiji FIU's website: www.fijifiu.gov.fj

INDONESIA

76. INTRAC (Indonesia's FIU) conducts ML and TF typology studies which have identified the following:

Corruption

- Use of bank instruments/facilities such as cheques and travel cheques to bribe government officers;
- Use of personal accounts to hold government funds;
- Use of wire transfers to transfer amount of money, followed by cash withdrawal in short period of time (pass by);
- Use of family member or third party bank accounts to receive proceeds of corruption.

Narcotics

- Smuggling narcotics from abroad through couriers and cargo;
- Narcotics trafficking from prison by bribing the prison guards;
- Use of third party bank accounts, but the identity and relationship of the parties is not known;
- Use of cash or wire transfer, followed by cash withdrawal in short period of time (pass-by).

Terrorism

- The most dominant source of funds comes from fai[14] and donations;
- Use of dormant accounts to receive incoming transfer;
- Increased transaction activity after the terrorist act - the funds are used to assist the terrorist syndicate to escape.

NEW ZEALAND

77. The New Zealand FIU produces quarterly typologies reports which can be found at: http://www.police.govt.nz/advice/businesses-and-organisations/fiu/news-and-documents

78. The purpose of the Quarterly Typology Report is to provide an accurate picture of current, emerging and longer term factors impacting on the AML/CFT environment. The Quarterly Typology Report is intended to do the following:

- Examine money laundering and terrorist financing methods used in New Zealand and overseas;
- Provide indicators of money laundering and terrorist financing techniques;
- Highlight emerging trends and topics and share information in relation to AML/CFT and financial crime in general;
- Provide typology case studies;
- Update suspicious transaction reporting and Asset Recovery Unit activity.

79. The FIU is also midway through a new iteration of the National Risk Assessment and expects to conclude the project in late 2014. The Sector Supervisors are also at varying stages of renewing their 2010 Sector Risk Assessments.

3.2 Association of Types of ML or TF with Predicate Activities

HONG KONG, CHINA

63. The most prevalent predicate activities associated with ML are email fraud, telephone deception, auction fraud and online purchasing fraud.

INDONESIA

64. Predicate offences associated with money laundering are corruption, fraud and bribery.

65. Terrorist financing predicate offences are kidnapping, robbery and narcotics.

PAKISTAN

66. After analysis of STRs, there are instances where the reported transactions have links with terrorism/terrorism financing, narcotics, corruption/bribery and unexplained assets, fraudulent activities, counterfeiting and piracy of products, smuggling etc.

THAILAND

67. The most common criminal activity that takes place is drug trafficking, which is one of the main sources of funding for insurgent groups in Southern Thailand.

68. The insurgent groups are also involved in goods smuggling, usually cigarettes, liquor, pirated DVDs, small arms trafficking and human trafficking.

[14] Fai – an Arabic term endorsing robberies in the name of funding jihad

3.3 Emerging Trends; Declining Trends; Continuing Trends

BRUNEI DARUSSALAM

Emerging Trends:

- Trade Based Money Laundering

Declining Trends:

- Laundering of proceeds from tax offences

Continuing Trends:

- Mingling (business investment)

COOK ISLANDS

Emerging Trends:

- Fraud or internet fraud by foreign workers.

FIJI

Emerging Trends:

Currency smuggling (including issues of concealment & security)

69. We have identified a number of cases whereby travellers have failed to declare currency at the border. The "intent" of the traveller carrying the currency is questionable.

Declining Trends:

Use of false identification

70. The Fiji FIU has noted a decrease in the number of cases involving fake identification cards such as passports, Fiji National Provident Fund (FNPF) cards and birth certificates. This is due to some recent measures undertaken by the relevant authorities in Fiji.

HONG KONG, CHINA

Continuing Trends:

Email Scams

71. The trend for email scams continues further to the typologies report last year. Culprits hacked the email account of the customers and suppliers, and then gave false instructions directing the customers to remit the outstanding amount to a new account and the funds were withdrawn by cash or transfer immediately.

INDIA

72. The investigation of money laundering cases under investigation where proceeds of crime have been attached under AML provisions, it is noticed that proceeds of crime are mostly invested in immovable properties, followed by jewellery, vehicles etc.

INDONESIA

Emerging trends:

- The use of credit card for payment.
- Cuckoo smurfing scheme.

Declining trends:

- The use of alternative remittance system.
- The use of 'transfer/overbooking' payment.

Continuing trends:

- The use of 'hard' cash.
- The use of foreign currency.
- The use of false ID.
- The use of third party/ family member bank account.

MACAO, CHINA

73. Throughout the period from January to June 2013, a total of 777 STRs had been received by GIF, with 548 STRs from the gaming sector and 229 STRs from the financial sector (including banking, insurance and financial intermediaries) respectively.

74. Common money laundering methods detected from STRs received are as follows:

    - Chips conversion without gambling activities;
    - Unable to provide ID / important personal information;
    - Suspicious wire transfers;
    - Use of cheques / promissory notes / account transfers etc. to transfer funds;
    - Significant cash deposit with non-verifiable source of funds;
    - Irregular large cash withdrawals;
    - Currency exchanges / cash conversion;
    - Suspected illegal financial business;
    - Suspected PEP related transactions; and
    - Possible match with international watch-list or other black list.

75. From January to June 2013, 89 STRs were disseminated to the Public Prosecutions Office and were consolidated into 10 cases filed for investigation. The cases under investigation were mainly related to fraud, illegal financial activities, commercial crimes and illegal gambling.

76. An emerging trend in ML is that criminals make use of third-party payments and online banking service platforms, which allow criminals to easily transfer money anonymously through the network and leave without trace of record. Other new payment methods commonly used include credit/debit cards, ATM, etc.

77. Commercial type of criminals usually possesses higher education, the modus operandi is more subtle and the proceeds of crime as compared with other types of crime are higher. Criminals generally have careful premeditation and preparation, and make extensive use of modern technology, i.e. computer technology, as it can work without leaving an audit trail, is difficult to detect and is instantaneous. Law enforcement agencies must enhance their studies on high-tech crimes, especially regarding crime characteristics, methods of prevention and investigation skills to collect evidence in order to combat crime effectively.

MALAYSIA

Continuing Trends:

78. Continuing trends indicated by the Suspicious Transaction Reports (STRs) include the following:

Reports on internet/wire transfer scams are increasing, involving cross border transfer of funds:

- Foreigners or individuals associated with foreigners opening accounts in different/multiple banks;
- Multiple inward remittances received from various entities in different countries;
- Funds received were withdrawn in cash and via ATM at various locations immediately upon receipt, leaving low balances;
- Transactions made were not consistent with individual's profile.

Large and rapid movement of funds (transit accounts):

- Large value cheques and cash were deposited into bank account followed by immediate cash withdrawals;
- Funds transferred in and out of an account on the same day or within a relatively short period of time;
- Camouflaging movement of funds to third parties with cash withdrawals.

Unjustified banking transactions:

- Deposits are not justified considering the nature of business or profession;
- Deposits were inconsistent with the volume generated by the business;
- No economic rationale and/or bona fide purposes;
- Deposits were structured below the reporting requirement to avoid detection;
- Deposits at various branches and times for no logical reasons;
- Substantial inter-account transfer between related accounts;
- Multiple cash deposits into an account followed by a large transfer to other third parties account/countries.

NEW ZEALAND

79. Several large scale operations led by the Organised and Financial Crime Agency New Zealand have demonstrated the ongoing ML threat posed by organised criminal groups involved in methamphetamine supply. Financial elements of these recent cases are still under investigation, however, it is clear that multiple laundering methods have been employed including:

- Use of businesses, including traditional cash intensive businesses;
- Extensive control of valuable assets;
- Use of casinos;
- Some use of precious metal bullion.

80. Prosecutions of ML have been predominantly drugs, fraud and tax evasion related.

81. There has been a rapid increase in reporting to the FIU following the commencement of the new AML/CFT regime. One immediate result is greater detection of widespread internet based scams, including use of victims to launder proceeds of crime, predominantly through the remittance sector.

THAILAND

Emerging and continuing trends:

82. Identity theft-related fraud is increasingly a high threat.

83. The insurgent groups continue to use cash couriers to move money because of easy access to air and land borders. Other means to move money is unregulated hawala which is operated through money exchange business.

84. The rampant use of the ATM card is emerging. Insurgent groups recruit students to open bank accounts. ATMs then are used for frequent transactions involving small amounts.

3.4. Effects of AML/CFT Counter-Measures

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

AUSTRALIA

85. In June 2013, the C*rimes Legislation Amendment (Law Enforcement Integrity, Vulnerable Witness Protection and Other Measures) Act 2013 (Cth)* amended the AML/CTF Act to enable more expeditious review of AUSTRAC decisions, harden existing offences, enable AUSTRAC to engage industry secondees, enhance privacy protections, and strengthen financial intelligence by the addition of two new designated agencies under the AML/CTF Act, bringing the total number of partner agencies to 41.
Specifically, the amendments:

- extended existing offences for providing false or misleading information in purported compliance with Australia's AML/CTF regime;
- enhanced protections on AUSTRAC information to ensure regulated businesses are prevented from 'tipping off' a person about whom a suspicious matter report has been raised in a wider range of circumstances;
- ensured that the Australian Commission for Law Enforcement Integrity (ACLEI) is able to more readily access AUSTRAC information to assist with its corruption investigations, in particular by ensuring that ACLEI does not need to rely on authorisation from the AUSTRAC CEO when an investigation involves AUSTRAC;
- achieved more timely and cost effective dispute resolution processes by enabling more expeditious review of AUSTRAC decisions through internal processes;
- strengthened AUSTRAC's analytical capability by enabling it to engage private sector secondees with relevant professional, academic and/or industry experience;
- ensured that AUSTRAC information disclosed by non-designated Australian Government agencies is granted appropriate privacy protections; and
- added the Clean Energy Regulator and the Integrity Commission of Tasmania to the list of designated agencies that are authorised to access AUSTRAC data.

FIJI

86. In September 2012, Fiji issued the *Proceeds of Crime (Amendment) Decree (2012),* which is available for download at the following link: http://www.fijifiu.gov.fj/docs/Decree%2061%20-%20Proceeds%20of%20Crime%20(Amendment)%20Decree.pdf

87. The decree further strengthens Fiji's AML/CFT legal framework. The Decree provides authorities with a mechanism for the forfeiture of "unexplained wealth". The key stakeholders have been creating awareness on the new unexplained wealth provisions and there are plans to set up a taskforce which would handle these cases.

88. Fiji also issued the Proceeds of Crime (Management and Disposal of Property) Regulations, which are available for download at the following link: http://www.fijifiu.gov.fj/docs/LN%2063%20-%20Proceeds%20of%20Crime%20(Management%20&%20Disposal%20of%20Property)%20Regulations.pdf

89. The Regulations contain provisions for the management and control of property that has been restrained by or forfeited to the State. The AML Legal Working Group is developing a manual to support the regulations and there are plans to set up a special unit within the Ministry of Justice to handle the management and disposal of tainted property.

INDONESIA

90. The complexity of the money laundering crime and terrorist financing in Indonesia has been rising significantly. Offenders are now more familiar with using the financial system and disguising their illicit income by using fake ID, and other legal documents that they can obtain from many government institutions. Facing this complexity, in recent years, especially after the enactment of the *Law Number 8 year 2010* (the new money laundering law), the coordination amongst law enforcement is becoming the priority realizing the numerous threats by many crimes in Indonesia. The rule of law in Indonesia is in the process of major reform, and capacity building enhancement amongst law enforcement in Indonesia is becoming a priority.

91. Now many court decisions have been made using the anti-money laundering provision. This differs from earlier years (before 2010) when judges seemed reluctant to use the money laundering law. Now, prosecuting money laundering is a priority, as well as for the terrorist financing when we found the transaction related to the terrorist activity or any name linked to such activity.

MACAO, CHINA

92. The project for revising the AML/CFT Law and Regulation is now at the final stage, and the formal proposal was submitted to the Chief Executive of Macao SAR China in April 2013. It is now under review by the Secretary for Administration and Justice. Following that the legislative process will begin.

93. The private sector consultation period for the R. 3 and SR. III legislation finished on 15 August 2013. The Law Reform and International Law Bureau (DSRJDI) is now at the stage of reviewing comments from the reporting entities and relevant business associations. After the draft is finalized by DSRJDI, the proposal with the final draft of the law will be submitted to the Secretary for Economy and Finance for comments.

94. A special team from relevant government agencies including the Macao, China Customs Service (SA), the Judiciary Police (PJ), the Immigration Department (SM) as well as the legal expert from the Office of the Secretary for Security (GSS) is now carrying out study on setting up a mixed cash declaration/disclosure in Macao, China.

MALAYSIA

Legislative and Regulatory Framework Developments

The Anti-Money Laundering and Anti-Terrorism Financing Act (AMLATFA)

95. The AMLATFA was tabled in Parliament on 4 December 2013 for its first reading. The amendments were to reflect internal standards and domestic requirements and also to enhance investigation powers for law enforcement agencies. The amendments will result in greater clarity on reporting obligations, greater enforcement powers and higher penalties.

Revised AML/CFT Policy

96. Bank Negara Malaysia as has recently revised and issued new AML/CFT policies to its reporting institutions which came into force on 15 September 2013. The revised policies address implementation issues and incorporate the new FATF Recommendations.

Law Enforcement Developments

97. The amendment of the AMLATFA will include provisions on cross border currency declaration and will strengthen the scope of the requirements and enforcement processes for the Royal Malaysian Customs Department.

Policy/Coordination Developments

The National Coordination Committee to Counter Money Laundering (NCC)

98. The terms of reference (TOR) for the NCC was revised and adopted in August 2013 to further strengthen its roles as a decision making and coordinating body for the national AML/CFT. As part of the enhancement, changes were made to cover the following areas:

    (i) counter financing of weapons of mass destruction/proliferation;
    (ii) enhancement in the NCC structure; and
    (iii) improved provisions related to NCC membership and the terms of accountability.

NEW ZEALAND

99. The *AML/CFT Act 2009* came into full force on 1 July 2013 - it is still too early to assess the impact.

100. The *Criminal Proceeds Recovery Act 2009* came into force in December 2009. Since its introduction there has been a year on year growth in the value of annual restraints and forfeitures. In 2012-2013 NZD58.2 million was restrained and NZD14.2 million was forfeited. Based on the estimates of the total value of laundered proceeds in New Zealand in the 2009 MER (<$1billion) and 2010 NRA (around $1.5billion) this would equate to the equivalent of around 3-5% of laundered criminal proceeds restrained. New Zealand Police projects continued growth in the value of criminal assets restrained and forfeited.

101. A Bill will be introduced to the House this year that will introduce, amongst other things:

- amendments to the ML offence;
- international fund transaction and large cash transaction reporting; and
- an identity crime offence.

4. CASE STUDIES OF ML AND TF

4.1 Association with corruption (corruption facilitating ML or TF)

CANADA

102. FINTRAC was acknowledged in 2012 by the Sûreté du Québec (Quebec's police force) for its contribution to Operation Hammer – an investigation into corruption in the construction industry that resulted in numerous charges and helped lead to the creation of the Charbonneau Commission, a commission charged with investigating the above-mentioned corruption charges.

103. In February 2013, the former head of the McGill University Health Centre (MUHC) was arrested in Panama and charged with defrauding the government, accepting secret commissions, breach of trust, conspiracy, and laundering the proceeds of crime. Investigators sought the assistance of FINTRAC, which uncovered a series of transactions between May 2010 and September 2011 that saw large sums of money deposited into bank accounts held by the individual charged.
104. In April 2013, FINTRAC's contribution to the Unité permanente anticorruption's Project Lauréat was recognized by the Sûreté du Québec. Five people were named in arrest warrants that cited charges relating to fraud, bribery, and money laundering, arising from a contract to build the McGill University Health Centre hospital.

COOK ISLANDS

105. The Police and the FIU are currently under taking an investigation against a Minister of the Crown. The allegations are:

- The Minister was responsible for the Ministry of Marine Resources who is responsible for issuing of fishing licences to both local and foreign fishing vessels. The Minister approved the issuing of an additional licence to a foreign fishing company who also bought a boat from the Minister for the sum of $26,000. The Minister bought the boat from a local owner for $20,000 and on sold it to the foreign fishing company for $26,000. The foreign fishing company subsequently gifted the boat to a fishing association with which the Minister is associated as a member of the association. The Minister has now been relieved of that Portfolio pending the investigation.

- The Minister was responsible for the Ministry of Transport who is responsible for issuing shipping licences for commercial vessels to transport goods into the Cook Islands. Earlier in the year, the Deputy Prime Minister declined an application by a foreign company for a shipping licence with the intent that the licence was to be offered to a local company and operators. However, it was alleged that the Minister without knowledge of Cabinet approved the shipping licence to the foreign company and in return he was gifted $30,000 which he has used as price money on behalf of his business towards the annual constitution day of the Cook Islands being celebrated on his island.

106. The Minister together with a local businessman bought a property on his island for $1,000,000. They borrowed from the bank $700,000, and $250,000 came from a lawyers trust account which originated from overseas. The other $50,000 also came from another lawyers trust account as investment to make up the total of $1,000,000. The matter is still under investigation.

FIJI

107. The Fiji FIU received a request in February 2013 from the anti-corruption commission for financial information on a businessman. The businessman, Person A, operated a hardware business and two stationery supplies shops.

108. There were allegations that Person A was engaged in corrupt conduct, conspired with public officials and manipulated the tender process in order to win bids.

109. It had been established that the goods for which he invoiced and received payments were never supplied.

110. During the analysis, the Fiji FIU established that Person A had transferred money to the bank account of a sister (Person Z) of one of his employees.

111. Upon conducting analysis of Person Z's bank account, it was established that some significant deposits apart from normal salary deposits had been made, which were not commensurate with her salary.

112. Fiji FIU had also established that Person Z maintained a loan account at a credit institution and there was a large one-off loan repayment. The loan was then used to finance the purchase of a second hand vehicle.

HONG KONG, CHINA

113. In 2011, the Hong Kong Police received confidential information that a female serving a sentence in jurisdiction outside Hong Kong (henceforth called "jurisdiction A") controlled several bank accounts and two overseas companies in Hong Kong with a balance of over HK$4.63 million (USD597,281). Enquiries with the law enforcement agency in jurisdiction A confirmed that the female was convicted of corruption and embezzlement offences involving HK$14 million (USD1,806,032) in 2002 and was sentenced to 23 years imprisonment in 2007. Funds in her bank accounts in Hong Kong are believed to be proceeds of a corruption case in jurisdiction A.

INDIA

114. A manager of a Public Sector Bank entered into a criminal conspiracy with other charged persons in the matter of sanction and disbursement of housing loans/ additional housing loans to the persons who were closely related to each other to the tune of INR 27 million (USD462,693).

THE PHILIPPINES

115. The Philippines reported a case study on an elaborate scheme giving rise to the commission of the predicate crimes of corruption, malversation of public funds by PEPS and private persons, plunder and money laundering through the use of fictitious NGOs/NPOs, use of shell companies, purchases of high value goods, use of nominees/trusts/family members, mingling, wire transfers, currency conversion and use of false identification, among others.

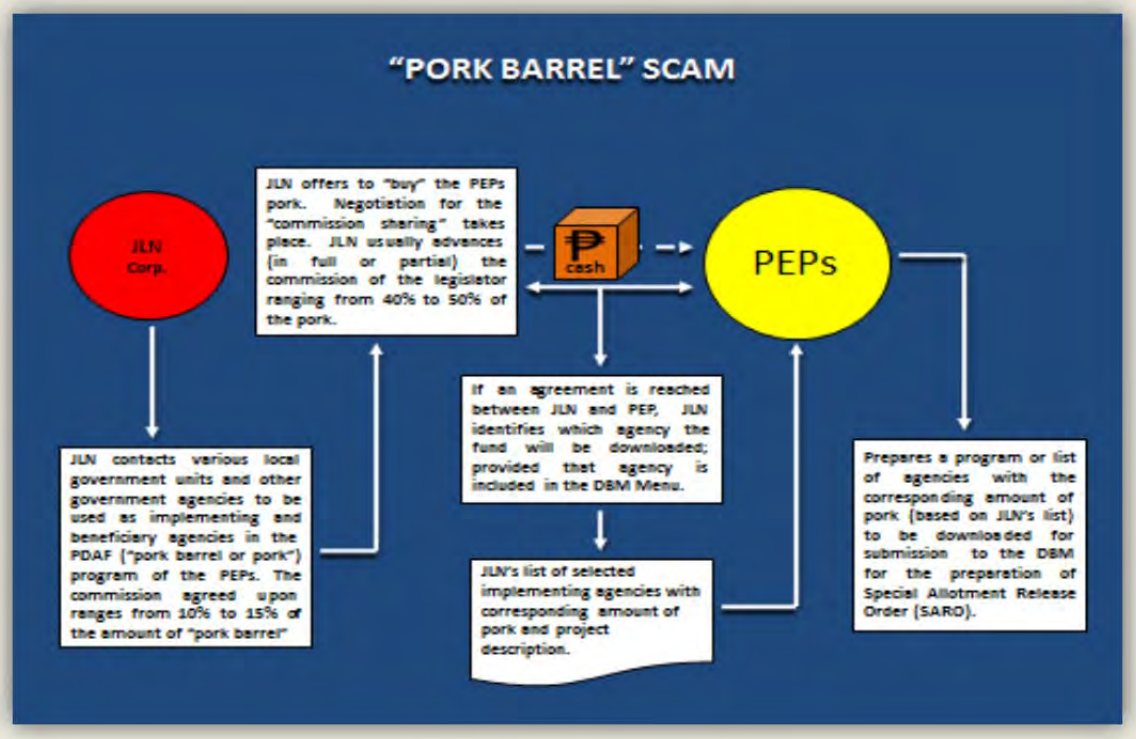
116. In a sworn statement, BKL stated that in the course of his employment with an entity known as JLN Group of Companies, JN, president and COO of said entity who happened to be the affiant's second, instructed him to create Non-Government Organizations (NGOs) or people's organizations to become recipients of government funded projects and to open bank accounts and deposits for and in behalf of these NGOs.

117. According to BKL, JN had instructed him to set up 20 NGOs; and he was also tasked to open bank accounts for each of these NGOs in various banks/banks' branches.

118. BKL further alleged that JN tasked him to set up the fictitious foundations to become recipients of government funded projects. Most of the presidents of these foundations were also employees of JLN Corporation, JN's company. These foundations received the funds otherwise known as "pork barrel or pork" from government agencies. Through an elaborate scheme in collusion with PEPs said "pork" was ultimately remitted to JN. The "pork" remitted by the foundations would

then be deposited into several personal accounts of JN. JN then delivered the 40% to 50% "commission or kickback" to the PEP while the rest would be shared amongst those who participated in the scheme, including PEPs whose approval and signature are necessary for the release of the "pork". JN usually kept 20% to 30% for her service.

119. JN was purportedly able to carry-out her scheme because of her connections with some powerful PEPs through many of these foundations she and her cohorts had fictitiously established. Once she was able to identify a possible "ghost project" for an NGO, the said NGO was utilized as a conduit through which the "pork" was used to fund the scheme to defraud the government and to steal the people's money.



4.2 Laundering proceeds from corruption

BRUNEI DARUSSALAM

Information Received by Anti-Corruption Bureau

120. Information was received by the Anti-Corruption Bureau stating that there were corrupt and fraudulent practices in an oil and gas company (Company X) as follows:

- Submitting false claims on the purchase of chemicals (degreaser);
- Submitting false claims on the purchase of equipment (spill sorbents/pillows).

121. The information also stated that the company involved was 'ABC' Enterprise.

122. Investigations established that 'ABC' Enterprise is a local company owned by one Brunei national and managed by Mr A. Investigation discovered that the local owner was not involved in the daily operation of 'ABC' Enterprise, he was paid BND$3,000 (USD2,434) per month and BND$50,000 (USD40,574) annually by Mr A for being the registered owner. Investigations also revealed that Mr A is a foreign national who is also the owner and the manager of 'ABC' Enterprise.

123. 'ABC' Enterprise's core business centred on common office equipment supplies, stationery items, sport and souvenir items, signs and craft. The company is also responsible for supplying chemicals (Vitrone Degreaser), equipment oil spill kits (GIP), box pallets, carton boxes, drum pallets and other fire safety equipment to Company X and Company Y. Mr A and two of his salesmen Mr B and Mr C, promoted their products to Company X personnel and gave bribes to the Company X and Company Y personnel to increase 'ABC' Enterprise sales and income.

124. Investigation revealed that 'ABC' Enterprise have been active in corrupt activities since 2003 in which, materials such Vitrone degreaser, GIP Emergency oil spill kits, box pallets, carton boxes and other safety equipment were excessively ordered and their physical deliveries to the final recipient are inconclusive.

125. Company X's investigation revealed that 'ABC' has been active in supplying material goods such as Vitrone degreaser. A total of 5,835 drums of 200L Vitrone Degreaser with a value of BND$8,167,875 (USD6,627,993) has been paid from 2003 until 2009. It further revealed that a total of 3,974 drums at a value of BND$5,563,600 (USD4,514,700) were produced during the period of 1 January 2008 till 31 July 2009. About 84% of the purchases, at a value of BND$4,673,200 (USD3,792,166), were made by Company X East Operations (EOP) and Production Operations (POP).

126. It was further revealed that once 'ABC' Enterprise received a Purchase Order from Company X or Company Y, Mr B or Mr C would determine the value of the commission (bribe), a cheque and a payment voucher would be prepared by an Accountant of 'ABC' Enterprise, and signed by Mr A. The cheque would be issued to Mr B or Mr C and the respective person withdraws cash from 'ABC' Enterprise's local bank. They would pass the bribe money (packed in envelope) to the Company X or Company Y personnel who initiated the orders.

Money Laundering Investigation

127. As a result of the substantial amount involved in the predicate offence and the enactment of Criminal Asset Recovery Order, 2012 (CARO) in June 2012, the Anti-Corruption Bureau opened an investigation paper on money laundering offence under Section 3 (1) CARO.

128. Financial investigation of 'ABC' Enterprise revealed that 'ABC' Enterprise had submitted false claims to Company X from March 2007 to June 2009 in supplying Vitrone Degreaser amounting to BND$6,647,450 (USD5,394,213). The payment from Company X was received at 'ABC' Enterprise's account in a local bank.

129. Investigation discovered that funds were withdrawn from 'ABC' Enterprise's account and deposited to several accounts of Mr A's in Brunei Darussalam. It was discovered that in addition to bank transfers, funds were also withdrawn in cash and credit card payments. The total amounts withdrawn from 'ABC' Enterprise's bank account for Mr A are amounting to BND$4,561,451.69 (USD3,701,486).

130. Investigation further revealed that several telegraphic transfer transactions from 'ABC' account were sent to Mr A's account in Singapore amounting to BND$1,456,000 (USD1,181,502).

Charges

131. Charges were laid under Section 6(b) of the Prevention of Corruption Act (Chapter 131) and Section 6(c) of the Prevention of Corruption Act (Chapter 131) and Sections 417, 420 and 477A of the Penal Code (Chapter 22).

Conviction

On 27 November 2013, Mr A entered a formal guilty plea.

INDIA

132. There was a case of misappropriation of government funds against a retired civil servant wherein the amount sanctioned for a public function organized by the State Government was misappropriated through an event management company. The funds allocated by the government were fully withdrawn by the public servant, but only a small portion of it was utilized for the function. Proceeds of corruption were attached under PMLA.

THAILAND

133. A former permanent secretary of the Defence Ministry committed corruption and laundered money through his adopted daughter's account and his associates' accounts aboard. The daughter also withdrew the money to invest in property in the name of her university adviser.

4.3 Abuse of charities for terrorist financing

134. No cases provided.

4.4 Use of offshore banks and international business companies, offshore trusts

CHINESE TAIPEI

135. It was reported by the media that Company X was being cracked down on by Justice owing to health supplements fraud.

136. An employee of Bank B noticed the news and found Company X's certificate of deposit of USD 1 million was withdrawn at the time that alerting the concealing of illegal gains. Thus, Bank B filed a suspicious transaction report (STR) to the Anti-Money Laundering Department (AMLD).

137. Mr. R and his wife J were the president and the general manager of Company X respectively. On behalf of Company X, they contracted some food processing factories to mix budget sugar syrup and artificial pigment into health supplements, and abetted Mr. C, one of employees who had known their intention, to forge the certificates of SGS, the world's leading inspection, verification, testing and certification company, to ensure their products containing no plasticizers, heavy metals and other toxic substances.

138. They sold the health supplements with the price of NTD1,000 (USD 33.3) per bottle through the channels of internet, TV shopping platforms and pharmacies, with the forged certificates presented to the customers as guarantee.

139. Mr. R also claimed all the products were imported from a Nevada Company A in the USA, which actually was only a paper company registered by Mrs. J to pretend the products had been approved by the Food and Drug Administration (FDA) of the USA.

140. The Taipei Field Division joined with the Food and Drug Administration Bureau of the Health Department to crack down Company X in January 2012 and found the amount of illegal profits was over NTD400 million (USD13.3 million).

141. The Taipei Field Division requested the Shihlin Prosecutors Office to issue seizure orders in advance, so that freezing the related banking accounts occurred simultaneously with search and seizure actions, and successfully froze the banking accounts of Company X, Mr. R and Mrs. J amounted over NTD60 million (USD3 million).

142. However, when the prosecutor notified them to be set bail at a large sum of money, Mrs. J defended that all the assets and banking accounts were frozen and they could not afford such huge money for bail. The prosecutor thus decreased the bail to NTD100,000.

143. Unexpectedly, the AMLD received an STR from Bank B next morning to reveal an employee of Company X was withdrawing a USD certificate of deposit amounted to USD 1 million and then timely informed the prosecutor to freeze the proceeds of crime. The frozen crime proceeds amounted to NTD90 million (about USD 30 million). Mr. R and Mrs. J were prosecuted for fraud and the offence of making false mark or indication on merchandise in March 2012.

COOK ISLANDS

144. In January 2013, the CIFIU received a request from a foreign FIU regarding funds relating to an investigation in its country. The investigation related to a hedge fund trader, and two firms involved in a scheme that manipulated several U.S. microcap stocks and generated more than $63 million in illicit proceeds through stock sales, commissions and sales credits.

145. It was alleged that the individuals conducted the scheme through their broker-dealer with the assistance of their close associate, a trader who lives in another jurisdiction. They bought microcap public companies through reverse mergers and manipulated upwards the stock prices of these thinly-traded stocks before selling their shares at inflated prices to eight offshore hedge funds controlled by them. Their manipulation of the stock prices allowed them to materially overstate by at least $440 million the hedge funds' performance and net asset values (NAVs) in a fraudulent practice known as "portfolio pumping."

146. A total of USD6,068,875 was laundered to an offshore trust account in the Cook Islands when it was frozen by the CIFIU. In July 2013, the total amount was repatriated back to the relevant authorities in the requesting country.

INDIA

147. A foreign jurisdiction based company used three front companies based in Mumbai to indulge in money circulation activity in India using multi-level or chain marketing methods and collected money from innocent investors as a registration amount. The amount collected was transferred to overseas account of the accused persons. The quantum of proceeds is around INR 20 billion.

NEW ZEALAND

148. Christopher Chase and Lee Vincent, a New Zealand citizen resident in Thailand, jointly owned a New Zealand 'legal high' business. In addition to selling unrestricted party drugs, the business was used as a front for distribution of illicit drugs. Money generated by both the licit and illicit activity was mingled and the cash generated by these businesses was taken on a regular basis to Vincent's mother's home for temporary storage.

149. The cash was packed into boxes, generally in the form of bundles of $20 and $50 notes. The boxes were then picked up by couriers, who transported the cash to Hong Kong where it was deposited in the bank accounts of three companies beneficially owned by Vincent. Bank statements for these Hong Kong accounts were sent to Vincent's mother's address in New Zealand.

150. The money laundering process was completed by loans made by one of the Hong Kong companies to another New Zealand company. Chase controlled a trust that was a 50 per cent shareholder in the New Zealand company. A small portion of the cash, around $184,000, was retained by Vincent's mother for her own purposes.

151. Court proceedings are ongoing and to date around NZD23 million has been restrained.

152. Methods observed: co-mingling; denomination conversion; cash couriering; shell companies, use of loans.

THAILAND

153. A US court unsealed an indictment charging Mrs. X, the executive of a Thai public enterprise, and her daughter, Y, with one count of conspiracy to launder money, seven counts of money laundering, and one count of aiding and abetting.

154. From 2002-2007, Mr. and Mrs. Z, executives of a film festival management company, who were convicted at trial of nine substantive Foreign Corrupt Practices Act violations, six counts of money laundering, and conspiracy, paid Mrs. X. approximately USD1.8 million in exchange for more than USD 14 million worth of contracts. The payments were made through numerous businesses and U.S. bank accounts to bank accounts in the United Kingdom, the Isle of Jersey, and Singapore held in the name of Y and an unnamed friend. These payments were disguised as "commission" payments in their books and records.

4.5 Use of virtual currencies

USA

OPEN SOURCE NEWS ITEM

Two Charged In BitCoin Money Laundering Scheme

February 6, 2014 4:36 PM

MIAMI (CBS Miami) — Miami Beach Police have arrested two people allegedly involved in a money laundering scheme using BitCoins.

Police arrested Pascal Reid and Michell Abner Espinoza on Thursday on charges of money laundering.

In a release sent Thursday, police said the arrest of Reid and Espinoza may be the first state prosecutions involving the use of BitCoins in money laundering operations.

BitCoins are an electronic currency used for online payments. They eliminate any central financial authority or oversight. Buying BitCoins allows money to be anonymously moved around the world. Improperly used BitCoins can be used for laundering dirty money or for buying and selling illegal goods, such as drugs or stolen credit card information.

According to police, undercover officers and special agents from the Miami Electronic Crimes Task Force (MECTF) posed as Bitcoins buyers and contacted various individuals which had a high volume of BitCoin activity. The agents let them know that they needed to move money to facilitate their criminal activities.

Reid and Espinoza allegedly offered to assist the agents in their transactions, for a fee. According to police it's the classic definition of money laundering.

"All of us in law enforcement know that criminals are always seeking new ways to make their activities profitable," commented State Attorney Katherine Fernandez Rundle. "BitCoins are just a new tool in the cyber criminal's toolkit."

http://miami.cbslocal.com/2014/02/06/two-charged-in-bitcoin-money-laundering-scheme/

4.6 Use professional services (lawyers, notaries, accountants)

CANADA

155. In June 2012, the Toronto Royal Canadian Mounted Police (RCMP) Integrated Proceeds of Crime Unit executed search warrants connected with money laundering of several million dollars of proceeds of crime through a Toronto law office. FINTRAC's assistance throughout the investigation was credited as contributing to the success of the investigation by the RCMP.

SAMOA

156. Mr F, a well-known lawyer, received a bank cheque of USD198,950.00 from Company Y located in Country K. The cheque was for maintenance of wife and children pursuant to a separation agreement done in country K. Mr F claimed to be the lawyer for the wife and children in this case. Mr F presented the cheque to Bank W with instructions to deposit 10% commission (i.e. USD$19,845.00) in his bank account and remit the remaining balance to beneficiaries in country C. Later on, the cheque was returned by the issuing bank as a 'fraudulent cheque'.

4.7 Trade based money laundering and transfer pricing

CHINESE TAIPEI

157. Mr. Chen was a salesperson of Olefin Business Department of Tai-X Company and in charge of sales business of petrochemical products such as Butadiene. From 2009 to November 2011, knowing that the Japanese Wan-Y Company quoted the best price, Mr. Chen sold the product to the Korean company, Chemione that quoted a lower price.

158. Subsequently, Mr. Pu, the person in charge of Chemione, sold the same products to Wan-Y Company at the price it originally quoted. At the same time, Mr. Pu opened several bank accounts in Chinese Taipei and gave the passbook with the ATM cards to Mr. Chen, remitting USD4,861,051 (approximately NTD130,000,000) in total into those accounts as Mr. Chen's commission. Then Mr. Chen withdrew money from the above mentioned accounts to purchase real estate, funds, and insurance. The case was referred to Taipei District Prosecutors Office on February 29, 2012 by the AMLD.

159. Mr. Cai was the actual responsible person for Chinese Taipei Yi-X-Bei-Er Company, and Mr. Lin and Mr. Li were General Manager and Financial Assistant Manager of the Company respectively. During the period from 2002 to 2009, they applied to the Investment Commission, Economic Affairs (EA) for an indirect investment of USD4 million to China Yi-X-Bei- Er Company through American Yi-X-Bei-Er Company without the approval of the Board of Directors.

160. Later on, Mr. Cai, Mr. Lin, and Mr. Li kept remitting USD13.2 million in total from Chinese Taipei Yi-X-Bei-Er Company to China Yi-X-Bei-Er Company which exceeded the USD9.2 million approved by the Investment Commission, EA.

161. In fact, they were aware that China Yi-X-Bei-Er Company had been mismanaged and suffered successive losses in successive years. They partially entered accounting books with the accounting titles "stockholders current account" and "suspense payment", and made financial reports accordingly. Till June 2009, the loss was reported in a Shareholders' Meeting for ratification, and 2008 Financial Reports were revised subsequently; the amount of loss reached NTD250,207,000 (USD8,289,170).

162. Justice referred this case to Taipei District Prosecutors Office on August 24, 2012.

163. XX Zhang was the person responsible for listed companies, Ke-X Company, X-Quan Company, and X-Sheng Company. XX Chen was the Chief Financial Officer of Ke-X Company. XX Zhao was the Secretary of XX Zhang. XX Liu was the deputy head of Solar Power Section of He-X Company that was traded in the over-the-counter market. XX Jiang was the person responsible for Shao-X Company. XX Fan was the person responsible for Yuan-X Company.

164. In order to window-dress the financial reports of Ke-X Company, XX Zhang conspired with XX Liu, XX Zhang, and XX Fan to have phony trades with only cash flows and no material flows for He-X Company, Shao-X Company, Yuan-X Company, and the accused X-Quan Company and X-Sheng Company. The amount of fake deals of X-Quan Company, He-X Company, Shao-X Company, and Ke-X Company in April and May, 2011 was over NTD470,000,000(USD15,666,666).

165. The amount of fake deals of Yuan-X Company, Ke-X Company, X-Quan Company and X-Sheng Company from January to September 2011 was over NTD650,000,000 (about USD21,666,666).

166. In addition, XX Zhang used the bonded warehouse taken by Ke-X Company in Holland as a trans-shipment warehouse to store solar modules and batteries which had been exported from Chinese Taipei but had not sold yet, that were entered up the financial reports of Ke-X Company with accounts receivable.

167. The amount of counterfeit accounts receivable from 2008 to 2011 was USD9.722211 million. XX Zhang disclosed and announced the fake data on the financial reports of 2008, 2009, 2010, and the upper half of 2011. The AMLD referred the case to Banqiao District Prosecutors Office on February 15, 2012.

INDIA

168. Case study involving trade based money laundering presently under investigation:

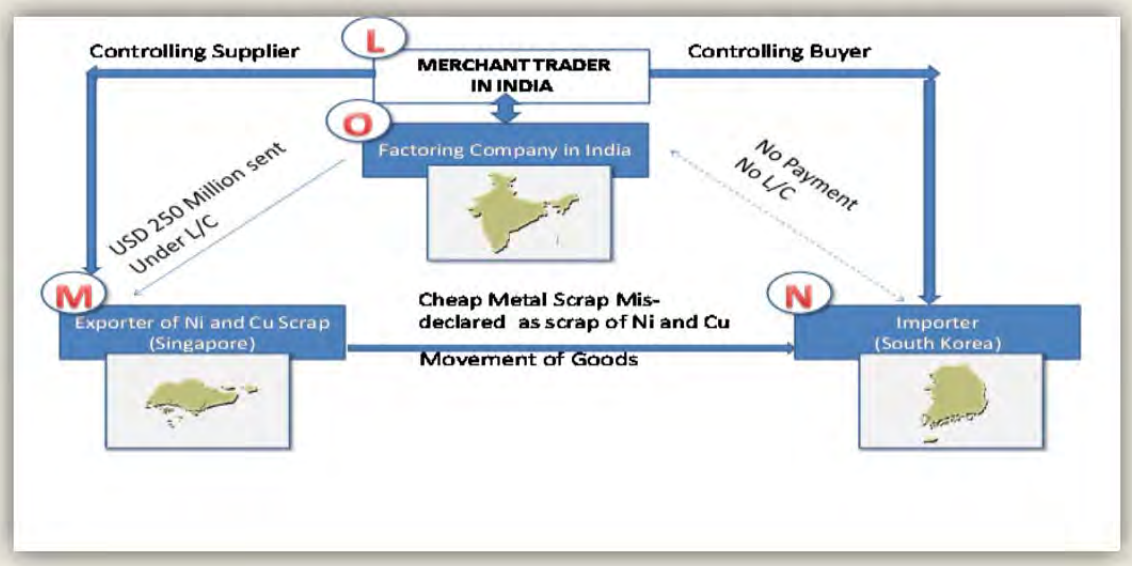
169. Company L located in India entered into a trade arrangement called merchanting trade for "Nickel and Copper Scrap" to be directly shipped from Company M located in Singapore and Company N located in South Korea. Company L was acting as an intermediary to make payments to Company M and receive payments from Company N. To secure payment for Company M, Company L entered into an agreement with Company O in India to get such Letters of Credit issued in favour of Company M (for the import leg of the transaction) against the export payment from company N by obtaining bonds and guarantees furnished by Company L.

170. After the successful completion of the initial rounds of transactions, Company N defaulted on payments to Company L even though the Letters of Credit opened by Company O at the behest of Company L in favour of Company M had already been discounted by Company M. The trade finance arrangement for the import leg of the transaction was completed between Company M & Company O by way of payment to beneficiary (Company M) but for the export leg of the transaction, due to non-acceptance of goods by Company N, no payment was received from Company N to Company O through Company L. Company L was in league with Company M & Company N and caused Company O heavy losses. Predicate offences of cheating and criminal conspiracy were involved and merchanting trade and its finance arrangements were used to launder the criminal proceeds.

171. This case study reveals the misuse of trade and trade finance to generate proceeds of crime and to launder funds. Unlike conventional methods of laundering the money in which generally, the proceeds of crime is structured into the financial system, in this case proceeds of crime were generated through mis-declaration of the goods, forgery of trade documents and the introduction of a third party in a jurisdiction other than the two trading countries. The techniques deployed to

indulge in TBML were mis-declaration of goods and related party transactions which were not independent corporate structures.

172. In this case study, Letters of Credit (trade finance) were arranged only for the import leg of the transaction and not for the export leg. Thus trade finance mechanisms became vulnerable to laundering the criminal proceeds. The lack of proper due diligence by the factoring company in assessing and acknowledging the risks and the lack of duty of care by banks in undertaking the proper scrutiny of the documents facilitated the commission of crime and TBML.



MALAYSIA

173. Methods used:

- Use of nominees, trusts, family members or third parties etc.
- Trade-related ML & TF.

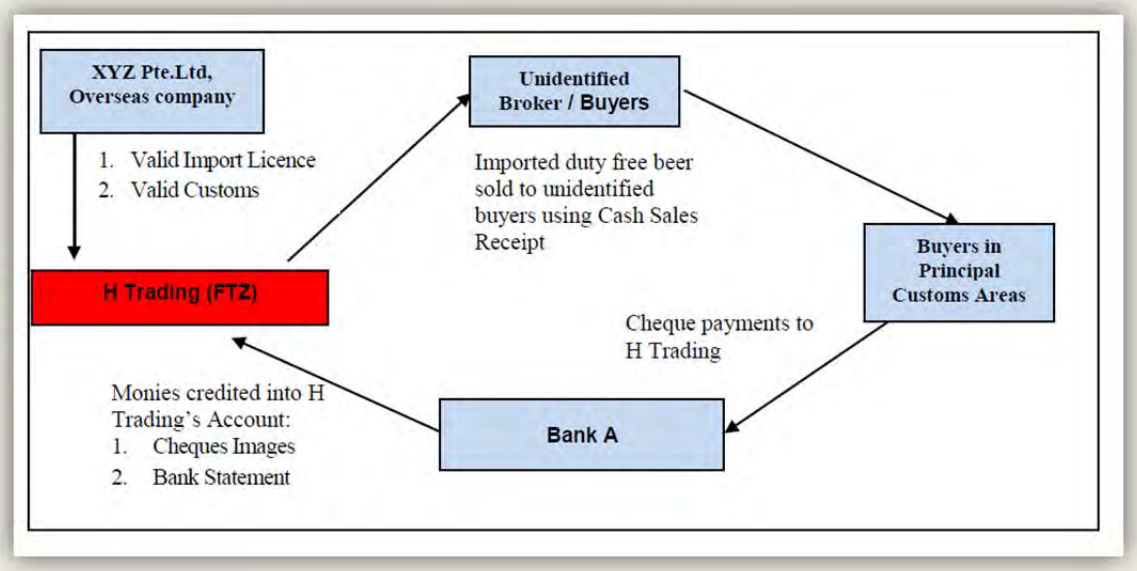
174. H Trading, a company operating in the Free Trade Zone (FTZ), has a valid licence for importation of alcoholic beverages for consumption in the FTZ. These goods were legally imported into the FTZ by H Trading from XYZ Trading Pte. Ltd., an overseas company. The Royal Malaysian Customs Department (RCMD) had noticed red flags in the clear mismatch of the amount of goods imported into the FTZ against the size of the market in the FTZ. H Trading's sales are made wholesale or as retail to persons within the FTZ. The identities of these local purchases were not recorded by H Trading to avoid the discovery of the end-to-end management of the goods disposed by H Trading to persons in the FTZ.

175. Investigation by RCMD revealed that between 2009 and 2011, H Trading received large sums of payments from entities in the Principal Customs Areas (PCA) in Malaysia located outside the FTZ despite the sales being made to persons in the FTZ. The payments by these entities to H Trading were for purchases of alcoholic beverages received by these entities from persons who were not identified.

176. Based on the evidence that (1) H Trading had participated in hiding the supply chain trail of the goods sold through the non-disclosure of the buyer in the FTZ, (2) H Trading received payments from the PCA and not from persons in the FTZ, (3) the lack of evidence from H Trading that goods for which payments were received by H Trading was not supported by evidence of exports from the FTZ and matching imports into Malaysia, and (4) that there was fair evidence that H Trading's import were too huge for the small market in the FTZ, lays strong circumstantial evidence that H Trading had conspired with unknown persons to smuggle out of the FTZ large

quantities of alcoholic beverages without the payment of duties and taxes for goods subsequently imported into the PCA in Malaysia.

177. The RMCD claim RM 91.7 million from H Trading as payment of duties and taxes.



4.8 Underground banking/alternative remittance services/hawala

CHINESE TAIPEI

178. XX Wang hired XX Yang to operate underground banking from January 1 2008 to April 25, 2012. XX Wang borrowed the bank accounts of XX Wu who was his relative, or rented the bank accounts of XX Zhang at the price of NTD3,000 (about USD 100) per month, holding 43 accounts opened by 18 people in total. Meanwhile, he opened accounts in financial institutions in the mainland China.

179. In Chinese Taipei, people had remitted money to the accounts held by XX Wang and subsequently XX Wang notified an associate in China to transferred equivalent value of RMB, to the accounts designated by the remitter. XX Wang charged NTD200 (USD7) for one remittance of RMB. The amount through underground exchange was NTD13,221,853,807 (about USD440,728,460). The case was referred by the AMLD on July 25, 2012 to Tainan District Prosecutors Office.

INDIA

180. Three persons were arrested from a province in India for suspected involvement in hawala transactions. Investigations under the Foreign Exchange Management Act (FEMA), 1999 by Enforcement Directorate, India revealed that the accused persons were receiving and distributing money in India on instructions from people resident outside India.

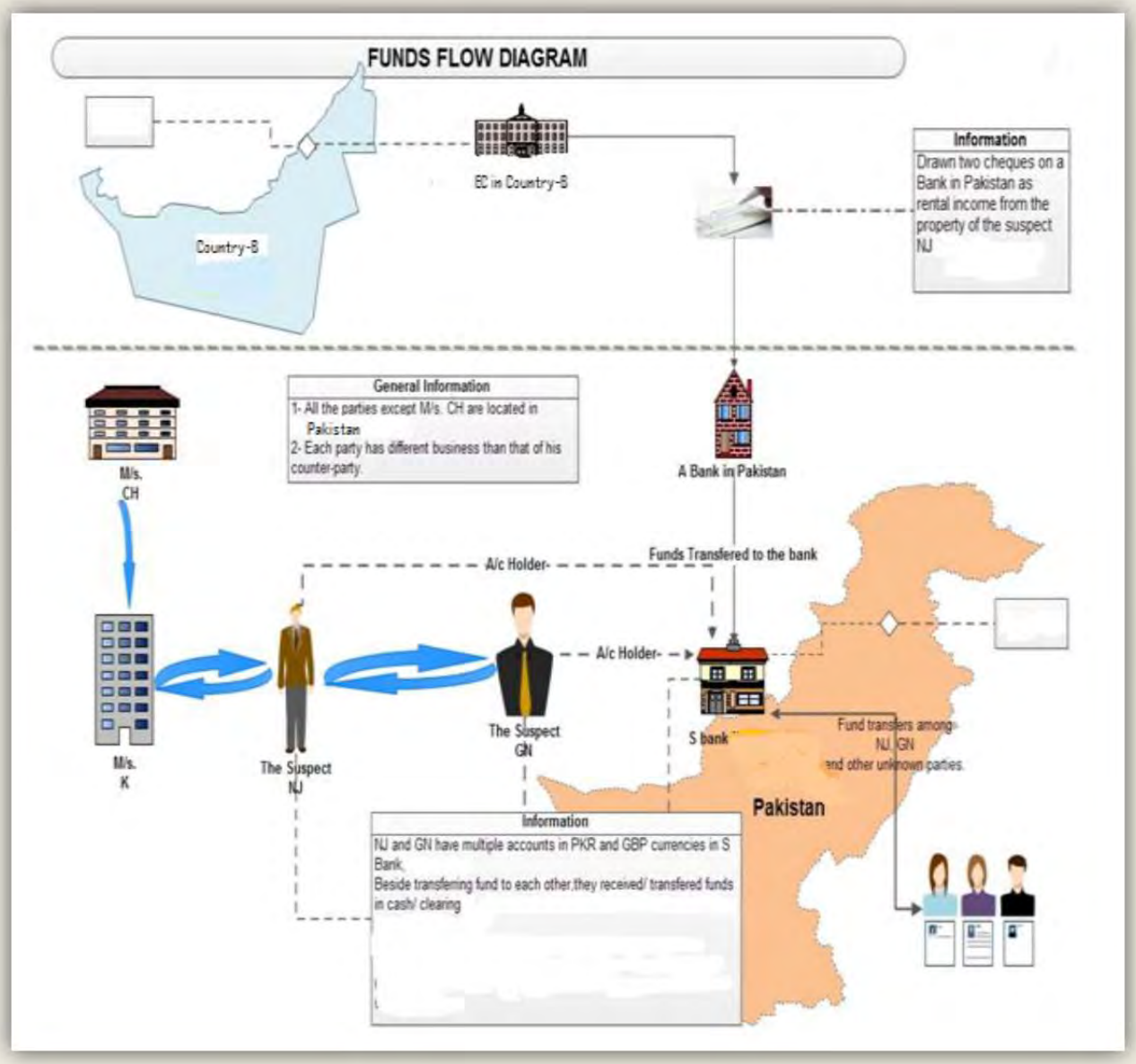
PAKISTAN

181. A high volume of transactions were observed in the account of customer NJ which was inconsistent with his business profile. As per due diligence, NJ owns a coffee shop country-A as a franchise of a well-renowned international coffee serving company and Ms. I.E entity in Pakistan doing investments by purchasing lands in Pakistan.

182. However, no information is available confirming NJ's claim of ownership of the franchise. Further, NJ received two cheques issued by an exchange company in country-B drawn on a bank in Pakistan.

183. On the banks enquiry the customer informed them that the funds were related to rental income from properties in country-B. But the justification does not seem plausible. Further NJ received high volume of funds from customer GN who has a business of fresh juices in one of the cities in Pakistan. Upon inquiry of the bank, customer GN and NJ informed that the funds are the proceeds of their property business in which they both are partners. In this connection, when bank asked for documentary evidences confirming the suspicious funds as property sale proceeds, customers failed to produce them.

184. Furthermore, customer NJ received funds from an entity Ms. K found connected with a country-C based company, namely Ms. CH which is under charge of committing corruption for securing international construction contracts.



185. Modus Operandi:

- NJ and GN held multiple accounts in PKR and GBP currencies in S Bank.

- Besides transferring funds to each other, they received/ transferred funds in cash/ clearing in/ from country-B and multiple individuals/ entities in the same accounts.
- Customer NJ received high volume of funds from unrelated counter-parties in country-B and in Pakistan.
- Customer GN also received funds from unrelated multiple parties and transferred some of the funds to customer NJ declaring the funds as proceeds from sale of properties.
- Customer NJ also received funds from an entity K found connected with a country-C based company Ms. CH which is under charge of committing corruption for securing international construction contracts.
- Most funds transferred were in cash and clearing modes.
- A detailed analysis of all the suspects reveals a nexus which is apparently working for the suspect country-C based company Ms. CH for routing suspicious funds to hide sources of funds earned.
- In conclusion, given the overall findings with reference to unrelated counter-parties, heavy frequent volume of funds, unusual pattern of transactions, and unexplained assets, it appears that entities could be involved in, Hawala/hundi, smuggling or Trade based money laundering activities.

186. The above financial intelligence was referred to LEA for further investigation.

THAILAND

187. A pattern of money laundering used by Thai criminals to launder their ill-gotten gains overseas is through underground banking enterprises (in Chinese Thai "poi-guwan") which are set up as travel agencies or trading firms doing both normal business and underground services. In particular, organized crime groups have a tendency to use money extravagantly, including illegal foreign currency, which is illegally sent out of the country to launder it. The gangs transfer money out of country through poi-guwan. In the poi-guwan system there are no official records of the transaction, so it is impossible to trace.

188. AMLO received information from a Hong Kong narcotics control officer that his office often found several hundred million Baht being transferred to Hong Kong from Thailand. Later, each sum was transferred back to Thailand. An investigation found that the money was not involved with narcotics activities. However, these cases could in fact be money laundering, involving the transfer of money from one account to other country, then back to the same country but with a different account to create a semblance of overseas business, in order to launder money derived from illegal activities.

4.9 Use of the internet (encryption, access to IDs, international banking, etc.)

CHINESE TAIPEI

189. Mr. Li found the loophole of the online game software "Legend of Dragon" that when players are transferring virtual property to other players the game software may be shut down at the same time. The players then can restore the virtual property when they re-logged into the game. The virtual property would recur under the name of the former player in the online game. Mr. Li took advantage of the abovementioned defect to obtain illegal profits by selling the virtual property to other players. The Investigation Bureau, a law enforcement agency in Chinese Taipei, initiated a criminal investigation, and then referred this case to Banqiao District Prosecutors Office on April 17, 2012 for prosecution.

HONG KONG, CHINA

190. In January 2013, an overseas victim's email account was hacked. The culprit gave instructions to the victim's overseas bank and remitted money from victim's account to a bank account of a shell company in Hong Kong. In addition, the culprits also hacked the computers/email accounts

of four business partners of other victims in different jurisdictions and requested those victims to remit money to the above shell company account. The total amount involved was HK$1.5 million.

MACAO, CHINA

191. A company owned by Mr. A and registered in country Y, opened 2 bank accounts in Macao, China, Mr. A stated that the accounts were used for the company's operational payments and receipts.

192. Shortly after the account opening, the accounts began to receive fund remittances from different countries, equivalent to over HKD7 million (USD902,976). Upon the receipt of funds, Mr. A transferred the funds out through the internet banking service to country Y.

193. During the above process of transactions, there were a number of overseas remitters made complaints to their local banks and reported to the police, claiming that their email accounts were being invaded for committing internet fraud, in which the funds were instructed to transfer to the corporate bank accounts of Mr. A in Macao, China. Some victims had reported their loss of approximately HKD 0.7 million (USD90,298).

NEW ZEALAND

Romance Scam to cash muling - use of the internet; use of third parties; structuring; wire transfers; use of false identity

194. A New Zealand woman became ensnared in two related scams that are unfortunately all too common. In the first scam, the woman was victimised in a romance scam after meeting a man living in Nigeria on an online dating site. After a period of online chatting, the scammer convinced the woman to make several wire transactions over a few days to Nigeria, supposedly to pay for airline tickets for the scammer to come to New Zealand.

195. When the scammer did not arrive in New Zealand the woman became suspicious and made a statement to Police that she was the victim of a scam. Contact from the scammer ended for several months leaving the woman several thousand dollars out of pocket as a result of the scam.

196. Months later, the scammer resumed contact with the woman to initiate a second scam that would see the woman became an unwitting accomplice in money laundering. The scammer told the woman that a friend would transfer money from a New Zealand account to the woman's bank account. The woman was to withdraw the money in cash and wire the money to several bank accounts in different South East Asian countries minus the money that the woman had "loaned" the scammer.

197. Unbeknown to the woman, the email address of the other New Zealand account holder had been hacked and fraudulent instructions had been send to the New Zealand bank. The woman's bank became suspicious when its account monitoring detected the money transfers being quickly followed by withdrawals and identified that she was being used as a mule.

198. The woman's bank reported the matter to Police. The subsequent Police enquiry resulted in a formal warning for the woman for the Crimes Act Money Laundering offence.

199. Money Laundering Indicators:

- Deposits quickly followed by cash withdrawal.
- Multiple international wire transfers over a short time period.
- Multiple transactions to structure transaction.

200. Scam Indicators:

- Multiple wire transfers over a matter of days.
- Wire transfers to high risk scam jurisdiction.

PAKISTAN

201. Mr. E and Mr. F, were working as Manager HR and Assistant Manager Accounts, respectively at BME Group of Company in Karachi. They established a fake proprietorship concern and made a fake letterhead. Subsequently, by showing themselves as employees of that entity, they opened accounts at different banks. They enticed people by promising them Spanish visas, conditions of which required the victims to open accounts along with internet banking facility and deposit specific amount of funds for producing bank statement for visa purpose. Once the account was opened by the victims, they somehow managed to get their secret particulars of internet banking facility and used to transfer the funds from the victim's account to their respective accounts.

SAMOA

202. Mr F queried Bank A about funds of USD$800.00 (equivalent to ST$1,839.08) debited from his account without authorisation. Accordingly, the fraudster hacked Mr F's bank account via internet banking, sent instruction to Bank A to remit funds to country C.

203. Company I and Mr L were victims of internet banking scams that involves the same beneficiary, Mr T. These scams were reported by Bank W. Mr T, resided in country A, contacted two different university students, Ms F and Ms M via Facebook asking them for their account numbers. Mr T hacked Company I and Mr L bank accounts and debited ST$1,500 (USD661) from each account. He then credited Ms F and Ms M accounts with ST$1,500 (USD661) each and instructed the students to remit funds to country A.

4.10 Use of new payment methods / systems

204. No cases provided.

4.11 Laundering of proceeds from tax offences

AUSTRALIA

205. A money laundering and taxation investigation commenced into a suspect who, for more than 10 years, declared minimal income to the Australian Taxation Office (ATO) while living a luxurious lifestyle.

206. The criminal investigation into the financial dealings of the suspect revealed that he attempted to disguise from the ATO income he had derived from the trading of shares on the Australian Stock Exchange (ASX).

207. The criminal investigation revealed that the suspect created several offshore companies which, on paper, were owned by 'stichtings' (a foundation in which the identity of the beneficial owner is not publicly available) in the Netherlands.

208. He then sold his ASX shares to the offshore companies at a value well below the true market value in an 'off market' trade. By selling his ASX shares at a discounted price the suspect was able to reduce his tax liabilities in Australia while still maintaining control of the ASX shares.

209. The suspect later arranged for the shares to be sold via his offshore companies at market value. The proceeds of the sales were returned to the suspect in Australia disguised as loans from offshore companies. By disguising the proceeds of the share sales as a loan, the suspect avoided paying tax on the proceeds in Australia. This method of transferring also created distance

between the suspect and the ownership of the shares, while still allowing him to ultimately obtain the benefits from their sale.

210. Analysis of AUSTRAC information identified that, over two years, the suspect arranged 15 international funds transfer instructions (IFTIs) to send funds from offshore companies under his control based in Switzerland to his Australia-based company.

211. AUSTRAC analysed financial transaction reports submitted by reporting entities and identified:

- All incoming international funds transfers were valued between AUD 50,000 (USD46,407) and AUD 1 million (USD928,130), totalling approximately AUD 4.7 million (USD4,362,211).
- All incoming international funds transfers were conducted via major banks and were sent in the names of offshore companies linked to the 'stichtings' in the Netherlands. These companies were under the suspect's ultimate control.

212. The suspect was found guilty of dealing in money valued at over AUD1 million (USD928,130) which was to become an instrument of crime (money laundering) and dishonestly obtaining a gain from a Commonwealth entity (ATO).

213. He was sentenced to eight-and-a-half years' imprisonment.

Offence	Money laundering Tax evasion
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI
Jurisdiction	International – the Netherlands
Designated service	Account and deposit-taking services Securities market/investment services
Indicators	Account activity inconsistent with customer profile Creation of offshore companies Customer declares minimal income, which is inconsistent with the client's luxurious lifestyle Receiving loans from offshore companies Selling shares to offshore company at a reduced value

CANADA

214. Under the directorship of Mr. Y, ABC Corporation, a language instruction company, became a vehicle for tax evasion. ABC had established licensing agreements with contacts in Australia, Malaysia, Chinese Taipei, and the United States. Between 2003 and 2006, ABC underreported income by over $400,000. Mr. Y evaded taxes by creating a scheme involving offshore transactions to and from Belize as well as by creating fraudulent business expenses.

215. In 2003 and 2004, Mr. Y incorporated "University Corporation" and "A-Trust Corporation" in Belize. Each of the corporations had their own Belizean bank account with Mr. Y having sole signing authority. The licensees were directed by Mr. Y to make all further payments owing to ABC to these two corporations. In regards to the fraudulent business expenses, the Canada Revenue Agency (CRA), Canada's federal tax administrator, determined that ABC had claimed,

among other items, advertising and marketing expenses totalling over $300,000. These payments were made to both of the Belizean corporations, serving as a way of moving corporate assets out of Canada and into Country A.

216. The CRA also determined that Mr. Y accessed the foreign funds by utilizing a Visa Travel Money card. Furthermore, he also made telephone and wire transfers from the Belizean bank accounts to Company G & S. As it was later uncovered, these transfers were for the payment of gold and silver which Mr. Y had shipped to him directly. Two of these transactions were fictitiously booked in the corporation as promotional expenses. Eventually, Mr. Y's plan unravelled as CRA investigators built a case founded on indisputable evidence.

217. Overall, between 2003 and 2006, these fraudulent transactions resulted in ABC attempting to evade federal taxes of almost $120,000, while Mr. Y attempted to evaded personal federal taxes of over $180,000. In March 2013, in addition to the taxes owing, Mr. Y and ABC were fined a total of approximately $230,000 by the court, which represents 75% of the taxes evaded. A jail sentence of two years less-a-day, and 120 hours of community service, were also handed down to Mr. Y by the Court. As an additional term of the Conditional Sentence Order, Mr. Y was ordered under house arrest for the first eight months of the Order.

CHINESE TAIPEI

218. X-Yi Huang was the Chairman of Tien-X Company, and signed up contracts to purchase residences and land in Taipei City and New Taipei City with titulars of relatives and friends including X-Sheng Huang during the period from 2003 to 2011.

219. Later on, X-Yi Huang took fake contracts of purchase to go through the procedure of transferring registrations at land administration organizations, and subsequently, he sold the property for a profit of 30%, and paid for individual general income tax at tax collection organizations in the name of the titular.

220. Next, X-Yi Huang entrusted X-Wei Chen and X-Ren Huang of Jun-X Tax and Accounting Service Office to apply to tax collection organizations for profit-making business registration and receiving invoices of real estate sales transactions that are operated individually in the name of X-Hui Huang.

221. They then filled in fake Input/Ouput Documentary Evidence and Account Book of Profit-seeking Enterprise to report and pay for Business Tax and Profit-seeking Enterprise Income Tax at Tax Collection Organizations.

222. The total illegal real estate X-Yi Huang Group obtained were 1,942 articles; the total amount of hidden sales revenue was NTD26,542,655,703(about USD8,847,552), and the total amount of suspicious evasion of Business Tax, Profit-seeking Enterprise Income Tax, and Individual Income Tax was NTD2,063,893,453(about USD68,796,448). The case was referred by the AMLD on June 25, 2012 to Taipei District Prosecutors Office.

FIJI

Case 1

223. The FIU received reports on 3 related companies on the grounds that there were large and unusual cash deposits conducted on the business bank accounts. The nature of business for each company was as follows:

Company A - Restaurant
Company B - Nightclub and restaurant
Company C - Property management/Real Estate

224. All of the businesses were cash intensive businesses. Checks revealed that these companies were registered for tax but were not declaring their revenue earned.

225. Analysis of the business bank accounts revealed a total of FJ$6.5 million (USD3,547,530) being deposited into the 3 business bank accounts.

226. The Fiji FIU disseminated a report to the Fiji Revenue & Customs Authority for tax evasion related activities.

Case 2

227. Person X who is a sole trader operates a construction company as well as another business. Person X has 2 daughters and he acts as the principal trustee to both his daughter's accounts.

228. The Fiji FIU had established that Person X was diverting funds from his construction company to his family member's accounts. The total deposit transactions conducted through his construction company, his daughter's accounts and his personal account in 2011 and 2012 amounted to FJ$3.5 million (USD1,910,209).

229. The Fiji FIU disseminated a report to the Fiji Revenue & Customs Authority for tax evasion related activities.

4.12 Real Estate, including roles of real estate agents

INDIA

230. The case was registered against a Chit Fund Company and its managers wherein the crime proceeds to the tune of INR 30 million (USD512,133) were invested in the purchase of residential property.

NEW ZEALAND

231. Timothy Clifford, a methamphetamine manufacturer and dealer in the Waikato region, used an accountant to receive cash from his drug dealing and convert it into various purchases of farm land over a number of years. He used two of his farm employees to collect and take cash from drug sales to the accountant's office. The accountant had 12 accounts held at different banks in which he would deposit the cash. The accounts were held for his accountancy practice, a gift shop he and his wife owned, his personal accounts and a company account he was nominee director and shareholder of on behalf of Clifford.

232. The accountant went to different branches across the Waikato region and banked the cash into the various accounts. Some excuses he gave about the source of the cash were "it was cash takings from a client who owned a bar" or "it was his cash takings from a stall he operated at a market". The deposited cash would then be electronically transferred to his accountancy practice to be held on behalf of Clifford.

233. With his accumulated wealth, Clifford purchased farm land in the name of his family trust. The trustee of his trust was a corporate trustee company that the accountant was the director and shareholder of. This trust arrangement enabled Clifford to hide the fact he owned the farm land . It was estimated that, over ten years, Clifford had accumulated $4.8 million from his drug offending. He was sentenced to 12 years prison and his farm land (valued at approximately $5million) was forfeited to the crown.

234. Whilst it was clear the accountant had engaged in money laundering, he was used as a witness against Clifford in exchange for immunity from prosecution.

235. Money Laundering Indicators:

- Large cash deposits.
- Use of third parties.
- Use of a professional.
- Co-mingling of criminal proceeds with legitimate business.
- Use of nominee directors/shareholders to hide the ownership of business.
- Purchase of real estate.
- Use of trust to hide the ownership of real estate.

USA

OPEN SOURCE NEWS ITEMS

Real estate agent arrested for money laundering

Posted: Wednesday, July 31, 2013 11:05 pm

Freddy Centeno, of Brownsville, has been arrested following the return of two-count indictment alleging money laundering for a convicted drug trafficker and making false statements to federal agents, United States Attorney Kenneth Magidson announced today. Centeno was taken into custody just a short time ago and he is expected to make his initial appearance before U.S. Magistrate Judge Ronald Morgan.

The sealed indictment was returned July 23, 2013, and unsealed today upon Centeno's arrest. The indictment alleges that Centeno, a licensed real estate agent, helped a narcotics trafficker launder drug profits through the purchase of real estate properties in Brownsville. If convicted, Centeno faces up to 20 years in prison and up to a $500,000 fine.

The arrest comes as a result of the ongoing Organized Crime Drug Enforcement Task Force investigation dubbed Operation Spike Strip. The narcotics trafficking and money-laundering investigation targeted the Armando Arambul drug trafficking organization which operated under the auspices of the Gulf Cartel in Matamoros, Mexico, and throughout the Southern District of Texas.

Arambul and others were responsible for transporting multi-ton quantities of cocaine to Houston and other major U.S. cities and remitted millions of dollars to the Gulf Cartel. Arambul was convicted and is set for sentencing Oct. 21, 2013, at which time he faces up to life in prison.

The investigation was conducted by the Drug Enforcement Administration, Internal Revenue Service-Criminal Investigation, Homeland Security Investigations, FBI, Customs and Border Protection, Border Patrol, Cameron County District Attorney's Office-Narcotics Investigation Division and the U.S. Marshals Service. Assistant United States Attorneys Jesse Salazar is prosecuting the case.

http://www.yourhoustonnews.com/west_university/data/real-estate-agent-arrested-for-money-laundering/article_60203931-4edd-51a0-b54b-413f185c36a3.html

Real Estate Agent Headed to Prison for Money Laundering

Dec 19, 2013

McALLEN, Texas - Freddy Centeno, 52 of Brownsville, has been ordered to prison for money laundering for a convicted drug trafficker, announced United States Attorney Kenneth Magidson. Centeno, a licensed real estate agent, pleaded guilty to a one-count criminal information August 30, 2013.

Today, U.S. District Judge Micaela Alvarez handed Centeno a sentence of 24 months in prison to be immediately followed by a two-year-term of supervised release. In handing down the sentence, Judge Alvarez noted Centeno was responsible for laundering more than $200,000 and further ordered the forfeiture of all real properties.

At the time of his plea, he admitted he helped a narcotics trafficker launder drug profits through the purchase of real properties in Brownsville. Centeno structured financial transactions of residential and commercial properties to conceal the identity and ownership of a narcotics trafficker.

The conviction and sentence comes as a result of the Organized Crime Drug Enforcement Task Force investigation dubbed Operation Spike Strip. The narcotics trafficking and money-laundering investigation targeted the Armando Arambul drug trafficking organization which operated under the auspices of the Gulf Cartel in Matamoros, Mexico, and throughout the Southern District of Texas.

Arambul and others were responsible for transporting multi-ton quantities of cocaine to Houston and other major U.S. cities and remitted millions of dollars to the Gulf Cartel. Arambul was convicted and was previously sentenced to 14 years in prison.

The investigation was conducted by the Drug Enforcement Administration, Internal Revenue Service-Criminal Investigation, Homeland Security Investigations, FBI, Customs and Border Protection, Border Patrol, Cameron County District Attorney's Office-Narcotics Investigation Division and the U.S. Marshals Service. Assistant United States Attorneys Jesse Salazar is prosecuting the case.

http://www.justice.gov/usao/txs/1News/Releases/2013%20December/131219%20-%20Centeno.html

4.13 Gems and Precious Metals

236. No cases provided. (Section 2 provides a reference to the recently published FATF/Egmont typologies report).

http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf

4.14 Association with human trafficking and people smuggling

FIJI

237. A suspicious transaction report was filed to the FIU regarding a 19 year old female student receiving frequent remittances from an individual in Australia.

238. Profiling of the sender in Australia, Person A, revealed that the sender was 39 years old, a banker by profession and had visited Fiji for short periods of time. When he travelled to Fiji, he would stay in high class hotels. We also established that Person A had remitted similar amounts to other beneficiaries in Fiji. The profiles of these other beneficiaries were similar i.e. females, unemployed or students, between the ages of 17 and 23. One of the beneficiaries was recently reported in a domestic trafficking case.

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

FIJI

Case 1

239. An STR was reported on an individual, Person A, who was reportedly employed by a restaurant known for its illegal gambling operations.

240. The commercial bank noted that there were large cash deposits made into his bank account which did not appear to be his salary payments. A 2nd STR was reported on a primary school student, Person B, sharing the same address as Person A. The same commercial bank noted that there were also large cash deposits made into Person B's bank account which were inconsistent with his profile.

241. Analysis of these STRs revealed that Person A and Person B maintained 2 bank accounts each at separate commercial banks. There was a total of FJ$314,000 cash deposits made into their various personal bank accounts. Fiji FIU believed that the personal bank accounts of these two individuals were being used to launder proceeds from illegal gambling operations.

Case 2

242. Person X, a 48 year old widow who is a machinist by profession received a number of deposits (totalling FJ$9,633 – about USD5,257) into her bank account between April and June 2011, which appeared questionable. Fiji FIU later found out that her local mobile number was used in an impersonation scam. The Fiji FIU was able to establish similar deposits made into the bank account of other associates and one of them was also using the same local mobile number of Person X.

243. The whole scheme involved a Person Z who obtains contacts of "victims" from local newspapers. Different individuals claimed that they had received telephone calls from unknown individuals such as Person Z instructing them to deposit money into certain bank accounts for fees such as license fees, application fees for school grants, etc.

244. Person X was charged for money laundering and found guilty. She was ordered by the Court to pay FJ$1,095 (USD598) to the school and was sentenced to one year imprisonment suspended to two years. She was on a bound-over for a period of two years.

MALAYSIA

245. Methods used:
- Use of nominees, trusts, family members or third parties etc.
- Mingling (business investment)

246. Mr. A established 2 companies, Company A and B, through nominee directors and shareholders. Both companies offered similar investment schemes promising guaranteed high returns to the investors. Investors were duped that the funds gathered would be used for investment in projects that will generate high returns and be based on profit sharing basis (the more you invest the more return you will get).

247. Both companies A and B were enticing investors into projects that were either non-existent or were actually owned by other legal entities. Both companies advertised extensively through media, websites, brochures and telemarketers to attract investors.

248. Briefings were always conducted in 5-star hotels and provided potential investors with high value gifts for attending such briefings.

249. To invest, potential investors were required to become a member of a cooperative solely set-up for this purpose.

250. Investors' monies were paid into the companies' accounts, where Mr. A acts as the main signatory for the accounts. Investigation revealed that the return on investment paid to the investors was sourced from the new invested sum, and was only paid for the period of 3 to 6 months before the owner of the schemes disappeared and the scheme collapsed. The bulk of the invested money was utilised for Mr. A's personal benefit and companies' operational expenses.

251. Company A and B together with Mr. A were prosecuted in Court under Section 366(3) of the Companies Act 1965 for fraudulently inducing persons to invest money as well as under Section 4(1) of the Anti-Money Laundering and Terrorism Financing Act 2001 (AMLATFA) for money laundering offence.

NEW ZEALAND

252. Police conducted a financial investigation into a large drug importation and supply ring centred in Lithuania and New Zealand that culminated in multiple convictions for money laundering and drug offences along with restraint of almost three million dollars' worth of property, vehicles, cash and other assets.

253. Concurrent with its drug offending, including multiple importations of ecstasy and LSD, the syndicate involved in the case laundered millions of dollars using intermediaries. The use of intermediaries allowed the central New Zealand-based figure of the drug supply ring, Ronald Brown, to maintain a front of being an unemployment and later sickness beneficiary. The vast majority of transactions identified during the financial investigation involved intermediaries for Brown rather than Brown himself, to deflect any possible scrutiny of Brown's finances.

254. However, even excluding money laundering transactions, Brown's life-style would have appeared suspicious given his declared source of income as being a long term benefit. While on the unemployment benefit, Brown owned several high value vehicles, acquired a bar and later established a company with no identifiable business purpose. Brown's business practices were also unusual, for example business expenses for the bar were paid in cash. Brown was able to use intermediaries in interactions with the financial institutions and dealers which may have otherwise aroused suspicions about his unusual financial profile.

255. Brown used intermediaries to conduct transactions to place the cash proceeds of his drug supply so as to integrate the funds in the form of high value assets. Brown would give cash to one or more intermediaries who would purchase the vehicle from a dealer either using Brown's cash or banking that cash and using a bank cheque. In some instances Brown's company was used as a front by the intermediary. When the vehicle was purchased, it was registered either in a Brown family member's name or in Brown's company's name.

256. Brown also used intermediaries to send proceeds to multiple countries overseas. This was accomplished by intermediaries banking cash and wiring funds or by cash deposits to remitters. In one instance this involved the same individual remitting hundreds of thousands of dollars in multiple transactions over a few months with little explanation. Cash was also carried internationally by Lithuanian cash couriers using false passports.

257. In February 2011, Brown was sentenced to 11 ½ years' imprisonment after admitting importing ecstasy, LSD and methamphetamine, and using a passport in a false name. A number of other individuals involved have also been convicted of drugs and money laundering offences while others are still before the court. The Lithuanian based "mastermind" of the syndicate, Rokas Karpavicius, was also recently convicted and sentenced to six years and three months imprisonment.

258. Methods observed: use of third party intermediaries, use of front companies; wire transfers; cash couriers; cash deposits; purchase of assets (vehicles)

OPEN SOURCE NEWS ITEM

Harry Potter book drug smuggler jailed

Amy Maas

Last updated 09:41 22/11/2013

A Lithuanian man who smuggled LSD into New Zealand in a Harry Potter book and masterminded a sophisticated money laundering scheme has been jailed.

Rokas Karpavicius who was extradited to New Zealand to face the charges, was today sentenced at the High Court in Auckland to six years and three months in prison, with a non-parole period of three years. Karpavicius was found guilty on four charges - one of importing class A controlled drug LSD and three of money laundering - after a jury trial in September.

Justice Graham Lang said the money laundering in which Karpavicius used couriers was closely associated with serious drug offending.

"You were the guiding force and mastermind of the money laundering operation," the judge said. "You were the person who arranged couriers to come to New Zealand and I have no doubt you knew or encouraged them to use false identities."

Karpavicius imported LSD to a syndicate in New Zealand who would then distribute the drugs before syphoning the money from the drugs back out of the country.

Karpavicius' fingerprints were also found on the Harry Potter book containing LSD intercepted by New Zealand Customs in April 2008. The drug was hidden in the spine of the book.

The investigation into the importation of the drugs started in Australia in February 2008 when police there received information about drugs being sent to Australia in large granite statues, the court heard.

Similar statues had been imported into New Zealand on four occasions between March 2006 and December 2007.

New Zealand police then started monitoring conversations between New Zealander Ronald Terrance Brown and his associates, including a man with a strong European accent - Karpavicius. The group used iChat and email to communicate.

Brown has since been convicted in relation to the drugs found in the statues. He was Karpavicius' right-hand man who would pick up and distribute the drugs in New Zealand, the court was told.

In terms of the money laundering, Karpavicius and his associates used electronic transactions and people as cash couriers.

Associates of Karpavicius came to New Zealand on several occasions to syphon as much as $2.2 million out of the country by either changing to money into foreign currency or depositing money into a nominated foreign bank account.

The "human couriers" all used false passports to conceal their identities and one was found by police in an Auckland hotel room with more than €100,000 hidden in a laptop bag. Police, using search warrants, also found a biscuit tin in an ASB vault. In it there were four bundles of $100 notes - a total of $104,000 - and several passports.

http://www.stuff.co.nz/national/crime/9430514/Harry-Potter-book-drug-smuggler-jailed

THAILAND

259. The majority of cases with varying predicate offences involve the use of a nominee. Hiring a stranger to open accounts with ATM cards for illegal use is also a trend.

260. Mr. A was a drug trafficker who set up a methamphetamine-producing factory near the Thai-Myanmar border. His factory had the capacity to produce 10,000 methamphetamine tablets a day. He normally hired hill-tribe people to transport the tablets to his customers, mostly in Bangkok, by using a pick-up truck. One day his hired man was caught at the checkpoint near Phetchaboon province while transporting more than 100,000 methamphetamine tablets, worth more than 10,000,000 Baht (approximately USD250,000). Because his hired man was caught red-handed, he admitted to the police that he was hired by Mr. A to transport these methamphetamine tablets to Mr. A's customers in Bangkok.

261. The police then ran a background check on Mr. A and found that he did not have a credible profession, but owned a big luxurious wooden house and many cars and deposited a lot of money in various local banks. The police also found that Mr. A transferred money many times to Ms. B, his mistress. After the police had probable cause to believe that Mr. A committed a drug trafficking offence and a money laundering offence, and that Ms. B committed a criminal offence of money laundering, the police then asked for the approval of a judge to issue a warrant for the arrest of Mr. A and Ms. B.

262. The police interrogated them both and questioned other witnesses. They also collected all the evidence and forwarded the case to a public prosecutor. The public prosecutor considered the case, and he had probable cause to believe that Mr. A committed a drug trafficking and a money laundering offence, and that Ms. B committed a money laundering offence. A criminal lawsuit was filed, and at the subsequent trial, both Mr. A and Ms. B were found guilty. Mr. A was sentenced to life imprisonment for committing a drug trafficking and a money laundering offence while Ms. B received two years' imprisonment for committing an offence of money laundering.

USA

OPEN SOURCE NEWS ITEMS

Nine face money laundering charges

Posted: Monday, October 28, 2013 10:38 pm

By MARK REAGAN - The Brownsville Herald

Seven Brownsville residents and two Bayview residents are accused of laundering money for the Gulf Cartel in activities alleged to have lasted a little more than four years, authorities announced Monday afternoon.

According to the U.S. Attorney's Office, Southern District of Texas, the nine people arrested Monday opened bank accounts at Bank of America in Brownsville and unidentified people in Florida would allegedly deposit cash in amounts under the $10,000 reporting requirement to those accounts. Then, on the same day, the suspects would withdraw the cash in amounts under $10,000 and cross the cash to Mexico, taking a portion of the money as payment, according to a press release.

According to the USAO, the activities spanned from November 2008 until December 2012.

The 21-count indictment unsealed Monday charges Oscar J. Aguilar, 37, Yurixi Guadalupe Vega-Martinez, 29, Bea Marie Fairbanks, 24, Mayte Ayde Diaz, 39, Lorena M. Moreno-Martinez, 39, Teodosa Gonzalez-Rodriguez, 32, and Yezenia V. Campos-Silva, 31, all of Brownsville, and Yamileth Sinai Carballo, 20, and Miguel Jonathan Pereira, 21, both of Bayview, with violating United States money laundering laws. Jose M. Rivera, 26, of Brownsville, is also charged but is a fugitive with an outstanding warrant for his arrest, documents show.

"Those individuals arrested today (Monday) are members of a money laundering organization that allegedly orchestrated the movement of millions of dollars in illicit proceeds in an attempt to circumvent law enforcement and reap their illicit gains abroad," HSI special agent Janice Ayala said in a press release.

The indictment indicates the money came from illegal narcotic sales belonging to Mexican drug trafficking organizations including the Gulf Cartel, according to the USAO. The indictment also includes a notice of forfeiture against the defendants for nearly $2 million, according to the USAO.

All are charged with one count of conspiracy and one count of operation of an unlicensed money transmitting business, which carries a possible punishment of a maximum five-year prison term with a $250,000 fine on each count. All are also charged with varying counts of structuring withdrawals at a financial institution, which also carries the same five years and $250,000 fine on each charge upon conviction. However, if it is determined the alleged financial scheme involved more than $100,000, then the punishment is up to 10 years in prison with the same $250,000 fine on each count.

Aguilar, Diaz and Moreno-Martinez are additionally charged with conspiracy to commit international money laundering and further face 20 years in federal prison and a $500,000 fine.

The arrests are the result of a year-long investigation by HSI, Financial Crimes Group with the assistance of U.S. Marshal's Service, U..S. Border Patrol, the District Attorney's Office, the Cameron County Sheriff's Office and the Brownsville Police Department.

http://www.brownsvilleherald.com/news/local/article_3062da7c-404b-11e3-b0cd-0019bb30f31a.html

Brownsville Man Pleads Guilty to Money Laundering Conspiracy

May 16, 2014

BROWNSVILLE, Texas – Oscar J. Aguilar, 37, a Mexican citizen legally residing in Brownsville, has entered a guilty plea to conspiring to commit international money laundering, announced United States Attorney Kenneth Magidson along with Janice Ayala, special agent in charge of Homeland Security Investigations (HSI) in San Antonio.

Aguilar has admitted to recruiting nine others, some of whom were family members, to open bank accounts at Bank of America in Brownsville. Later, co-conspirators in Florida would deposit money from narcotics sales into the accounts. Aguilar's recruits withdrew the money in amounts under the $10,000 reporting requirement and would give that money to Aguilar or other co-conspirators. The recruits were paid for moving the money through their bank accounts. After Aguilar received the money, he facilitated its crossing from Brownsville to Matamoros, Mexico, where it was delivered to the Gulf Cartel.

From September 2008 through November 2012, the conspirators moved approximately $1,893,170 through nine bank accounts, with nearly $1.5 million from September 2011 through November 2012 alone.

"HSI Special Agents often investigate complex financial schemes in order to disrupt and dismantle the ongoing operations of transnational criminal organization," said Ayala. "These investigations deprive the organizations from enjoying the benefits of these illicit proceeds, and prevent them from furthering the efforts of the ongoing criminal enterprise. We will continue to aggressively investigate fraudulent financial schemes that put in jeopardy the integrity of our financial system."

Nine others have been convicted in relation to this case. With the exception of Francisco Jesus Arambul-Cortez, who also pleaded to conspiracy to commit International money laundering, the eight others entered guilty pleas to operating an unlicensed money transmitting business.

Aguilar entered his plea today before U.S. Magistrate Judge Ronald G. Morgan. He will remain in custody pending his sentencing hearing, set for Aug. 18, 2014, before U.S. District Judge Andrew S. Hanen. At that time, he faces up to 20 years in prison and a possible fine of $500,000.

This case was investigated by Homeland Security Investigations and is being prosecuted by Assistant United States Attorneys Karen Betancourt and Joseph Leonard.

http://www.justice.gov/usao/txs/1News/Releases/2014%20May/140516%20-%20Aguilar.html

4.16 Gambling activities (casinos, horse racing, internet gambling etc.)

AUSTRALIA

Case 1

263. AUSTRAC contributed to a joint international investigation sparked by the suspicious behaviour of a prominent Asian businessman. The investigation exposed a multi-million dollar global fraud committed by an Asian finance manager, who was known as a habitual gambler and international casino 'high roller'.

264. Authorities in Asia suspected that the suspect had defrauded a number of international banks. AUSTRAC received an international request for information from counterparts in Asia, seeking assistance with their enquiries with regard to the financial activity of the target while he was in Australia.

265. AUSTRAC data identified that the suspect had conducted significant international funds transfers to Australian casinos, had visited Australia to gamble at the casinos, and had left Australia with substantial amounts of money, presumed to be the proceeds of his gambling. This information proved the initial suspicions of AUSTRAC's Asian counterparts that the suspect had transferred funds to casinos in Australia.

266. The suspect was arrested and subsequently admitted to Asian authorities that he had embezzled approximately AUD78 million (USD72,003,360) from four international banks by forging signatures of executives of his company and opening accounts in the name of his employer.

267. Over a four-year period the suspect transferred approximately AUD190 million (USD175 million) into an Australian casino account via international funds transfer instructions (IFTIs). In addition, the suspect had visited a number of casinos in London, Macau and Malaysia, in some instances placing bets worth up to AUD400,000 (USD369,248).

268. The authorities in Asia requested further assistance from Australian law enforcement to trace additional proceeds of the suspect's fraud. In conjunction with AUSTRAC, Australian law enforcement discovered an additional AUD30 million (USD28 million) in accounts with various Australian casinos, held in the name of the suspect. Of this amount, AUD7 million (USD6.5

million) was restrained by Australian law enforcement under the Proceeds of Crime Act 2002 and a portion of this was repatriated back to the investigating authorities in Asia.

269. The suspect pleaded guilty in Asia to six counts of forgery and eight counts of cheating and was subsequently sentenced to 42 years imprisonment.

Offence	Money laundering Embezzlement
Customer	Individual Business
Industry	Banking (ADIs) Gambling services
Channel	Physical Electronic
Report type	IFTI
Jurisdiction	International – Macau, Malaysia, United Kingdom
Designated service	Account and deposit-taking services Gambling services
Indicators	Correlation between high-volume account activity and gambling activity Opening and use of business accounts to transfer funds to Australian and offshore casinos Recent business transaction activity inconsistent with previous transaction history Sudden increase in high-value activity in a casino account Sudden increase in incoming/outgoing high-value international funds transfers through a casino account

Case 2

270. Suspect A was arrested by law enforcement upon arrival in Australia, where he was found to be in possession of card skimming technology. This included computer disks, a laptop, a card encoder, an ATM feeder 'face unit' and 31 blank ATM cards. The suspect was an international student residing in Australia.

271. Upon his arrest, law enforcement commenced an investigation into his activity and discovered a card skimming syndicate operating in Australia which laundered the proceeds of its crimes through casinos. Analysis of AUSTRAC financial transaction data associated with suspect A identified three additional members of the syndicate and their activities.

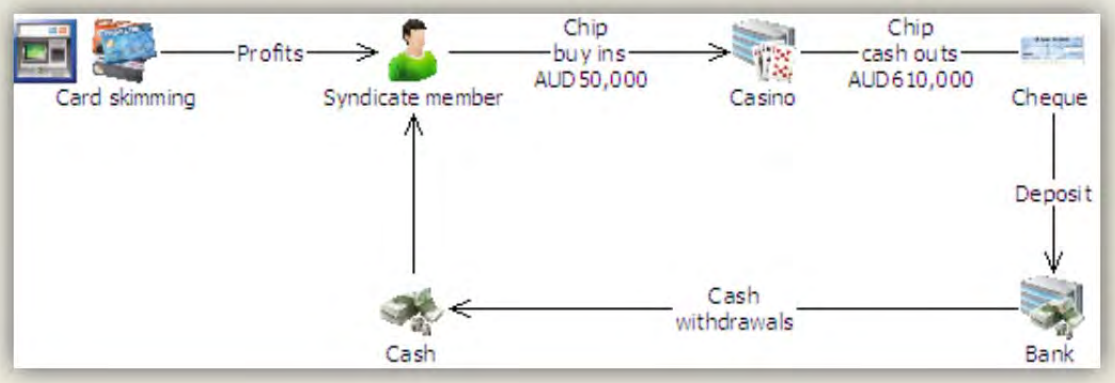
272. Members of the syndicate regularly visited casinos. Over a five-month period, AUSTRAC received threshold transaction reports (TTRs) indicating that suspect A had cashed in more than AUD180,000 (USD166,612) worth of gaming chips at an Australian casino. However, transaction records showed that the suspect had not previously purchased a corresponding amount of gaming chips at the casino. This suggested that the suspect may have purchased the chips directly from another player before cashing them out, while claiming they were actually his 'winnings'.

273. AUSTRAC information was also used to identify the irregular gaming activity of suspect B. Information on AUSTRAC's database indicated that, over a 12-month period, suspect B had purchased AUD50,000 (USD46,156) worth of gaming chips at a casino. However, records indicated that the suspect had cashed out more than AUD610,000 (USD563,103) worth of gaming chips at the casino. Suspect B also made regular cash deposits and withdrawals, often in amounts over the reporting threshold of AUD10,000 (USD9,231), into bank accounts in Australia in the days following the casino transactions.

274. A suspect transaction report (SUSTR) was submitted by an Australian casino, noting that:
- suspect B presented AUD28,000 (USD25,847) worth of casino chips to a cashier to be cashed out, before handing the cash proceeds to another person, believed to be suspect A
- the value of gaming chips cashed out by suspect B did not correspond with the suspect's observed game play at the casino due to the high volumes of winnings compared to funds withdrawn for gambling purposes, nor did it correspond with the expected financial activity of a young university student.

275. A second SUSTR was also submitted by an Australian financial institution detailing suspicious transactions conducted by suspect B. Over a three-month period suspect B deposited more than AUD155,000 (USD143,084) in cash into an account, indicating to bank staff that these funds were casino winnings. The majority of these funds were then withdrawn in cash at the bank and via ATMs at the casino.

276. Suspect A was charged under section 480.6 of the Criminal Code Act 1995 for the importation of a thing to dishonestly obtain or deal in personal information.



Offence	Fraud Money laundering
Customer	Individual
Industry	Banking (ADIs) Gambling services
Channel	Electronic Physical
Report type	SUSTR TTR
Jurisdiction	Domestic
Designated service	Gambling services Account and deposit-taking services

Indicators	Casino chip cash outs do not correspond with observed game play Customer undertakes consistent high-volume gaming chip 'cash outs' which are claimed to be winnings, an activity that appears unlikely with the comparatively low amounts of funds withdrawn by the customer for gaming purposes Funds from casino chip cash outs given to third parties Regular cash deposits into a bank account, followed by cash withdrawals High-volume cash deposits over a short period of time that does not match customer's established financial activity profile Account activity inconsistent with customer profile

MACAO, CHINA

277. Mr. Y was a patron in casino A of country B, having lots of gaming records in terms of frequency and gaming amount in different casinos. He obtained gaming credit from the casino but usually lost in the gaming activities. He sourced his gaming funds for repayment of gaming credit by frequent remittances from his investment firm's account in which he was one of the partners. His firm was located in country C. It came to the attention of the casino that the funds were remitted from the client's account of the investment firm. Out of suspicion, the casino filed an STR.

278. Further analysis found that Mr. Y was in fact embezzling funds from his clients who placed their savings in his firm for investment. Mr. Y was a gambling addict and chose to support his gambling activities by stealing client's funds.

MONGOLIA AND REPUBLIC OF KOREA

OPEN SOURCE NEWS ITEM

South Korean money laundering in Mongolia comes to light

November 13, 2013
Local newspapers have reported that the Economic Crime Combat Division of the Criminal Police Department have brought down a South Korean mafia money laundering operation in Mongolia.

According to a confirmed source, evidence has been found proving the boss of one branch a South Korean mafia Gangpae, or street gang, Ahn Jae Man, was laundering money in Mongolia from extortion, loan sharking and gambling in South Korea.

Ahn Jae Man, the boss of an illegal gambling establishment was sentenced for gambling business and illegal large amounts of money in South Korea. But he transferred the money via the office of "Юилсот" (Youilsot) Company director Lee Jae Gun in order to disguise the money as an investment.

The company used the money to build a hotel named Richfield in Chingeltei District, Ulaanbaatar. The charged Ahn Jae Man was sentenced for illegally obtaining large sums of money reaching 4.5 million US dollars in South Korea.

Now law enforcement officers have collected evidence against the company in Mongolia, "Юилсот" (Youilsot), and Lee Jae Gun the Director, transferred to his boss`s account a large sum of money equal to 11 billion MNT.

Lee Jae Gun, the owner of Richfield hotel in Mongolia was investigated for forcing women into prostitution by Chingeltei District Police in 2011. However prosecutors remitted the case due to lack

of evidence.

Now the State Investigation Department have confiscated the Richfield hotel in Ulaanbaatar Mongolia in connection with the money laundering case.

http://english.news.mn/content/162144.shtml

Authorities stop Richfield Hotel operation due to money laundering case

By M.ZOLJARGAL

Wednesday, November 20th, 2013

A case where a South Korean citizen, Ang Ji Mang allegedly used laundered money from an illegal to gambling house in Korea to build Richfield Hotel in Mongolia was reported by authorities. The hotel's operation has been stopped and suspects are still under investigation, said the police.

The defendant was found guilty by the court for laundering 4.5 million USD from the gambling house. Furthermore, he allegedly transferred his illegal profit to Lee Jae Gung in Mongolia and to build Richfield Hotel near the Bayanburd traffic rotary, according to the police.

Lee Jae Gung was also accused of selling the hotel to a Mongolian citizen on July 2013 fully aware of the illegality of his actions.

http://ubpost.mongolnews.mn/?p=6699

4.17 Purchase of valuable assets (art works, antiquities, race horses, vehicles, etc.)

CHINESE TAIPEI

279. In May 2011, the AMLD received an STR from Bank A indicating that the customer Ms. H usually deposited or withdrew cash at different counters and intentionally structured each transaction within the reporting threshold of CTR which exposed an indicator of money laundering.

280. Mrs. H was the secretary of Mr. L, the president of a listed Company G in Chinese Taipei from May 2003 to June 2011, and was responsible for arranging daily schedule, answering telephone, applying reimbursement of travel and entertainment expenses for the president.

281. According to the internal requirements of Company G, Mrs. H should attach the disbursement vouchers and the reimbursement claim sheets with the signature of the president for accounting and budget cancel after verification. However, the auditors of the Company G neglected to seek the confirmation of the president on expenses that induced the illegal intention of Mrs. H to take the advantages of this loophole.

282. Mrs. H and her husband bought luxury watches, jewelleries, leather goods and expensive household electric appliances at Department Stores and boutiques and paid by credit cards held by Mrs. H and her husband.

283. They required the stores to invoice no more than NTD100,000 (USD3,316) for each transaction to evade auditing. Then, Ms. H attached the invoices to the reimbursement sheets in the name of president L's entertainment fee and paid by Mrs. H and forged president L's signature on them.

284. Mrs. H required the staff of the accounting department to remit the money that she had spent to her banking account with Bank A so that Mrs. H and her husband could pay off the credit card and other personal debts.

285. Mrs. H defrauded the president L's expenses account amounted to NTD1.11 million (USD36,805) in 2007, NTD5.46 million USD181,039) in 2008, NTD13.26 million USD439,667) in 2009, NTD34.44 million (USD1,141,940) in 2010 and NTD29.52 million (USD978,806) from January to May of 2011 respectively.

286. On 5 May of 2011, Company G remitted the reimbursement of NTD3.6 million (USD119,367) to president L's banking account with Bank A instead of Mrs. H's due to mistake. Mrs. H asked the accounting department to remit the abovementioned money back to her banking account and forged president L's signature on the documents that caused the suspicion of the accounting department, and then found the amount of president L's entertainment was incredibly up to NTD29.52 million (USD978,806) from January to May of 2011.

287. There was something fishy about it and the accounting department decided to directly enquire of president L about the expenses abovementioned which disclosed Mrs. H's wrongdoing. After thorough auditing by the accounting department, the total amount of fraud by Mrs. H was up to NTD838 million (USD280 million). Mrs. H and her husband were prosecuted for forgery, embezzlement and fraud in January 2012.

4.18 Investment in capital markets, use of brokers

CANADA

288. In November 2012, the Calgary RCMP Integrated (Capital) Market Enforcement Team laid additional charges on three individuals following their arrest in the same case relating to a Ponzi scheme of over $1 million the year before. In total, 16 charges were laid relating to fraud, theft, money laundering and the possession of proceeds of crime. FINTRAC's collaboration in the case was recognized by the RCMP.

CHINESE TAIPEI

289. On 12 April 2013, 4 suitcases with explosive devices and materials were discovered on a high-speed train and at the entrance of a legislator's office. All four bombs failed to exploded due to either mishandling or design flaws. The Criminal Investigation Bureau (CIB) formed a special investigative team and found out the 4 suitcases containing timer, gasoline, glass bottle with hydrochloric acid and sodium cyanide, which will create a toxic gas when treated with acid.

290. In sight of the enquiry, the CIB quickly discovered the two suspects were Hu, a lawyer, and Chu, a taxi driver long-term being hired by Hu. They fled to Macau after placing the abovementioned bombing devices and two days later, were arrested by mainland China law enforcement agency and deported back to Chinese Taipei on 16 April 2013 according to the framework of the "Cross-strait Joint Fight against Crime and Mutual Legal Assistance Agreement".

291. This was the first time that the law enforcement agencies cross strait had jointly tracked down and arrested the suspects in such an efficient manner and within a short time. Although the two suspects were successfully arrested and taken into custody, they claimed right to silence and refused to state the motive behind bomb.

292. However, the AMLD received a very important STR from Bank A at the time that disclosed some large amounts of money flowed into Hu's banking account for futures investment shortly before they planted the bombing devices.

293. After analysis, the AMLD was alerted the information might be related to motive of the bombing event and immediately disseminated the information to the Prosecutors Office for further investigation.

294. The Prosecutors found the suspect Hu tried to create a large-scale disaster to gain his personal profit from short futures and also achieve the goal of showing his dissatisfaction with society. After planting the bombs, he then went online to place orders for short futures contracts, meaning he expected the market to fall. Had his plot worked he could have made NTD 100 million (USD 33.3 million). His account originally had NTD 15 million (USD497,361), but after taking losses, it only had over NTD 2 million (USD66,315) left.

295. On 6 June 2013, Hu and his accomplice Chu were charged with attempted murder, offences against public safety and other crimes. The prosecutors asked for the most severe punishment for them as they have shown no remorse. From this case, we learn the cooperation between cross strait authorities on combating crimes had significant progress and the FIU of Chinese Taipei also demonstrated its timely functioning to assist prosecutors to crack down this criminal case.

4.19 Mingling (business investment)

BHUTAN

296. STR was reported to the FIU on the misuse of INR (Indian Rupee) facilities. This case deals with the withdrawal of INR over the counter based on production of the import bills and custom declaration forms. The entry number of custom declaration form is given by the customs to organisation, company or businessmen. The number has to be shown to the clearing agent and custom officials during the time of import and gives information about the particular importer. The bank releases INR when this number is shown to them.

297. The case was forwarded to the Foreign Exchange Department of Royal Monetary Authority of Bhutan (RMA) as first line of action since the provisions of INR issues falls under them.

298. To investigate the authenticity of the import documents a team of Foreign Exchange officials from RMA meet with the DRC officials and the officials of the reporting entity. Upon investigation it was found that the entry number the businessman a Non- Bhutanese had used actually belonged to three different companies. The businessman had forged the entry numbers and used it against his business name. It was also found that the businessman has never declared any goods at the checkpoint and had forged the inspectors' signature. Even the business he was running was under fronting and the license of the business belongs to a Bhutanese women.

299. The total amount siphoned off amounts to INR 3,992,565 (USD68,158). Since the license was issued to a Bhutanese citizen, the owner was imposed a penalty of 50 percent of the declared value of Nu 3,992,565, which makes the penalty come to Nu 1,995,282.50 (USD34,059). (Note 1 INR = 1 Nu).

CANADA

300. In May 2013, the RCMP Greater Toronto Area Integrated Proceeds of Crime Unit charged 15 individuals with multiple counts of possession of property obtained by crime, money laundering, obtaining credit through fraud, using forged documents, and committing an indictable offence for the benefit of a criminal organization. The accused are related family members part of a criminal organization involved in operating indoor and outdoor marijuana growing operations.

301. This is the culmination of a three year long financial crime investigation. The current charges allege that members of this organization generated profits in excess of $3.6 million from their illicit activities, which were shared amongst members of this criminal enterprise. Those proceeds were used to purchase 41 properties, three coffee shop franchises, one commercial

fishing vessel and license, and other small businesses, which were used to launder the proceeds of their criminal activities.

INDIA

302. A company obtained a term loan fraudulently from a Public Sector Bank by submitting forged documents with an intention to clear private loans taken out by them on high interest rate. On receipt of the amount from the Bank, they withdrew the amount by submitting forged documents and cleared old debts.

4.20 Use of shell companies/corporations

HONG KONG, CHINA

Case 1

303. Between 2011 and 2012, three foreign passport holders, with the assistance of a Hong Kong based secretarial company, set up shell companies and opened several bank accounts in Hong Kong. The suspects then left Hong Kong and controlled the bank accounts overseas. At least six overseas victims at different jurisdictions were deceived to transfer money totalling HK$17M (USD2.2M) to the bank accounts of these shell companies. Police took swift action to withhold the remaining balances in the bank accounts whilst some of the victims successfully claimed their loss by civil proceedings.

Case 2

304. In June 2013, a foreign passport holder was recruited by two suspects in jurisdiction outside Hong Kong to set up shell companies and open company accounts in Hong Kong. Upon consulting the lawyer, the foreign passport holder made a report in Hong Kong. Investigation revealed that the two suspects set up shell companies and opened company accounts themselves in Hong Kong to launder over HK$80 million (USD10.3 million) between 2012 and 2013. Police later arrested one of the suspects for money-laundering offence while another suspect had left Hong Kong before the case was reported.

Case 3

305. In April 2010, Police received confidential information that a 68-year old female victim had been induced to remit approximately HK$838,000 (USD108,893) to a bank account in Hong Kong. The proceeds were transferred to an account of a local company in which a man later known as the defendant was the sole director and shareholder. Investigation revealed that the defendant had bought the local company at a secretarial company in July 2009 and opened the said account. Although the company did not have any business activities, its account was found to have frequent and significant transactions which had an average daily turnover of HK$100 million (USD12.9 million). Defendant was later arrested and sentenced to 10 years and 6 months imprisonment.

Case 4

306. In December 2011, confidential information suggested that a man (here below called “B”) was believed to have used his corporate bank account to deal with the crime proceeds of about HK$5.3 million (USD683,589) deprived from overseas boiler room fraud, including two remittances amounted to HK$250,000 (USD32,245) from two foreign victims. In January 2013, B was arrested for money laundering who claimed that he came to Hong Kong under the instruction of a causal friend in a jurisdiction outside Hong Kong to open the subject bank account. B denied having any knowledge of the funds in the account. B was subsequently convicted of money laundering after trial and was sentenced to 3.5 years imprisonment.

Case 5

307. An overseas victim was deceived in a boiler room fraud scam and had remitted about HK$12 million (USD1.5 million) into three corporate bank accounts in Hong Kong. A man (called "C") was the sole authorized signatory of the subject bank accounts and was arrested in December 2012. C claimed that he was recruited by two persons in a jurisdiction outside Hong Kong to set up shell companies and to open the subject bank accounts in Hong Kong but he had no knowledge about the funds deposited into these bank accounts. C later pleaded guilty to four counts of money laundering and was sentenced to 3 years 4 months imprisonment.

INDIA

308. The person charged floated nearly 327 shell companies with relatives and trusted employees and used these companies to obscure the source of funds and the persons controlling the funds. The quantum of proceeds in this case is around INR 21 billion (USD360 million). The accused person laundered the proceeds into movable and immovable properties.

MACAO, CHINA

309. A local steel trading entrepreneur 'A' had set up a number of companies in Macao, China in the past few years; some of these companies had real on-going trading business in place. The entrepreneur conspired with two foreigners to open 2 other shell companies in Macao, China, these 2 shell companies acted as suppliers and issued sale invoices to A, claiming that the sale of iron and steel was purchased by A. Then A used those fake invoices to apply for a number of bank loans consistently for years. Banks which granted the loans would have the funds deposited into the bank accounts of the shell companies. Police later found out that those funds were in return transferred back to the accounts of the entrepreneur A.

310. The fraud funds obtained were partly used to repay loans in order to continue borrowing from banks, partly were transferred to overseas capital market for speculative investments and partly were invested in real estate. The maximum funds during the same period of time were more than HKD 50 million (USD6.4 million).

311. The suspect had used false invoices for loan financing nearly 230 times and total funds granted were HKD 300 million (USD38.7 million). Judiciary Police detained three suspects.

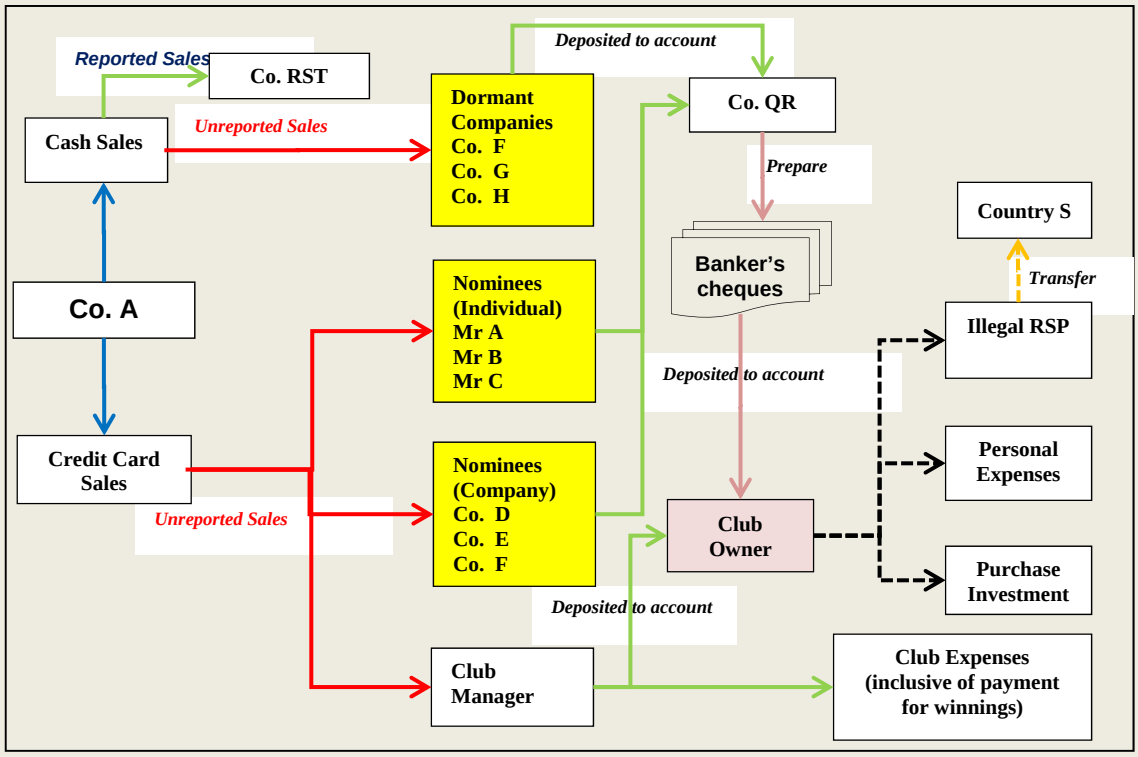
MALAYSIA

Methods used:

- Use of shell companies/corporations.
- Use of nominees, trusts, family members or third parties etc.
- Purchase of valuable assets.
- Alternative remittance services.

312. Company A conducted legal business and received payments from sales through 2 methods i.e. cash and credit card sales. To avoid paying the right amount of tax, Company A deposited sales by credit card into various nominees' bank accounts using either individuals (with relationship with Company A) or dormant companies. All these monies were transferred to an account belonging to Company B, another dormant company before the money was later transferred to personal account of Mr. Z, the owner of Company A. The money was used for Mr. Z's personal expenditure including buying shares and also transfer overseas using illegal remittance service providers.

313. Investigation established more than RM700 millions had not been reported and the Inland Revenue Board (IRB) managed to trace transactions involving more than RM400 millions (USD124.7 million) and recovered the tax amount due to the government.



NEW ZEALAND

New Zealand Shell Company Implicated in Suspected Attempted Sanctions Violation - use of false ide ntity; use of shell companies; real estate; use of shares

314. A New Zealand registered company approached an overseas-based law-firm's client seeking to buy a hotel in a third country. The law firm became suspicious about the transaction when it discovered that the owners of the New Zealand company did not have legal representation for the sale despite the size of the transaction which was in the tens of millions of dollars.

315. Know your customer and customer due diligence processes raised a number of additional concerns relating to individuals involved in the transactions. Firstly, the Iranian owners of the New Zealand company had passports issued by a State known to sell passports. In addition, the law firm could not find any indication that the owners had any real connection to New Zealand or the country where their passports were issued.

316. The transaction was to involve two New Zealand Companies. The company making the purchase and a second company that was to loan money to the first. However, the law firm could not establish the relationship between the two companies. In addition, the law firm could not establish what either company actually did or how the capital involved in the loan had been made.

317. The transaction for the New Zealand company to purchase of the hotel also raised the law firm's suspicions as the purchase was to be funded through an unusually complicated transaction structure which the law firm could not account for. The New Zealand company was proposing to raise funding by selling shares and through a loan from the second New Zealand company. Finally, a bank cheque drawing on Bank Melli (the Iranian national bank) was presented to pay for the purchase.

318. Based on these red flags, the law firm and the client became suspicious that the transaction was an attempt to circumvent sanctions against Iran. Based on the evaluation of the high risk of sanctions evasion, the client decided not to proceed with the transaction.

319. It seems likely that the Iranian nationals obtained passports from the offshore State and set up a New Zealand shell company and structured the complicated transaction to obscure the Iranian origin of funds that they were attempting to move from Iran.

4.21 Financing the proliferation of weapons of mass destruction (WMD)

320. No cases received.

4.22 Association with illegal logging

INDONESIA

Adelin Lis case

321. Adelin was charged with corruption and illegal logging activities in Mandailing Natal regency, North Sumatra, that were estimated to have cost the state more than Rp 400 trillion (USD3.65 billion). Prosecutors had demanded a 10-year prison sentence plus a Rp 1 billion (USD86,900) fine.

322. Court Decision on Adelin Case State Court of Medan freed Adelin Lis from any charges managed by State Prosecutor.

323. Supreme Court sentenced Adelin Lis for 10 years in prison and fine of Rp.1 billion or 6 months imprisonment. The court also sentenced Adelin Lis for returning State Loss in the amount of Rp 119.8 billion and USD2.938.556,24.

324. State prosecutors appealed the decision to the Supreme Court. However, while the court was about to hear the appeal, Adelin disappeared following his release from the state penitentiary.

325. The police have named Adelin a suspect and fugitive in connection with a money laundering case. They have also asked the prosecutor's office to extend Adelin's travel ban and worked with the North Sumatra provincial prosecutor's office to prevent him from escaping the country.

326. Police are also looking for Adelin's older brother, Adenan Lis, who has been on the police's wanted list since February last year, along with Korean national Lee Suk Man. The men headed the PT Inanta Timber and PT Keang Nam Development companies, respectively, under the auspices of PT Mujur Timber.

4.23 Currency exchanges/cash conversion

AUSTRALIA

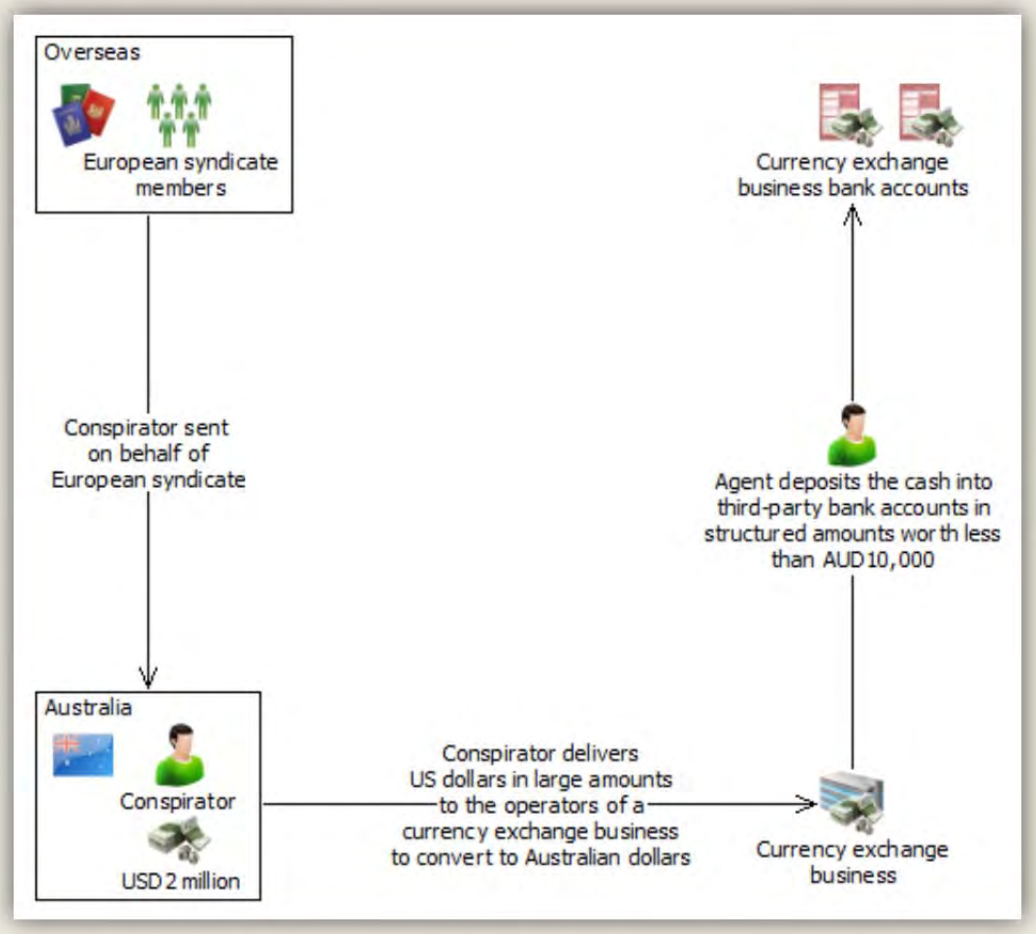
327. A multi-million dollar money laundering syndicate was dismantled following a 12-month joint agency investigation. The investigation uncovered a currency exchange business being used to launder the proceeds of crime for a European drug syndicate.

328. Law enforcement officers suspected that the currency exchange business had laundered more than AUD2 million (USD1.8 million) for the drug syndicate. During the law enforcement investigation, financial transaction activity recorded on AUSTRAC's database helped unravel the money laundering process used by the syndicate.

329. A suspect representing the European drug syndicate arrived in Australia to transfer back to Europe the illicit cash proceeds generated by a drug importation. The following steps outline the method used to launder the funds:
    - When the suspect arrived in Australia, European syndicate members informed him that the illicit cash was located in a safe in an apartment. The suspect followed instructions and took possession of more than USD2 million cash.

- Over a 10-day period the suspect delivered the US dollars, in large amounts, to the operators of the currency exchange business.
- The operators of the currency exchange accepted the US dollars and instructed an agent, on their behalf, to deposit the cash into third-party bank accounts in structured amounts worth less than AUD10,000. The agent undertook hundreds of cash deposits, often depositing cash into the same account and on the same day, but at different bank branches. The deposits of US dollars were all in amounts worth less than AUD10,000 to avoid triggering threshold transaction reporting requirements.

330. The activities of the currency exchange business came to AUSTRAC's attention after it was the subject of a number of suspect transaction reports (SUSTRs) submitted by industry. The SUSTRs detailed the suspicious transactions undertaken by the operators of the currency exchange, including:
    - structuring of foreign currency exchange transactions and travellers cheques.
    - always exchanging the same two currencies: United States Dollar and Hong Kong Dollar.



331. AUSTRAC prepared a financial intelligence assessment on the exchange business's suspicious activity and disseminated it to a law enforcement agency.

332. The suspect representing the European drug syndicate was arrested in possession of more than 28 kilograms of illicit drugs with an estimated value of AUD8 million (USD7.4 million).

333. Law enforcement officers seized a further AUD47,500 (USD43,908) cash and restrained approximately AUD247,000 (USD228,332) in assets related to the currency exchange operators.

334. The two operators of the money exchange business were charged, under section 11.5 of the Criminal Code Act 1995, on two counts of conspiracy to commit an offence (money laundering) against Commonwealth law. They were convicted and sentenced to seven years imprisonment on each count.

Offence	Money laundering
Customer	Business Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	SUSTR
Jurisdiction	Domestic International - Europe
Designated service	Account and deposit-taking services Remittance services (foreign exchange)
Indicators	Structuring of cash transactions by currency exchange business to avoid reporting requirements Multiple structured cash deposits using a foreign currency Multiple same-day cash deposits into same accounts at different branches Multiple structured transactions to purchase foreign currency and/or travellers cheques

JAPAN

335. Concealment of criminal proceeds related to a murder-robbery case abroad

336. In July 2012, a Japanese man "X", living with a Japanese woman "Y" in Macao S.A.R., intentionally and with premeditation stabbed Y to death with a knife in a room of their apartment house to rob Y of her HKD 1,400,000 in cash.

337. Repeatedly exchanging HKD which he robbed her of for JPY, in August 2012 X asked his acquaintance "Z" to exchange HKD 140,000 for JPY, upon X's return to Japan.

338. Not knowing the fact that the HKD 140,000 was a part of the money which X had robbed from Y, Z exchanged HKD 140,000 for about JPY 1,100,000 at a financial institution in Japan under Z's own name and handed the exchanged money to X.

339. As mentioned above, X, for the purpose of laundering HKD 140,000 which was a part of the cash X stole from Y, pretended that Z owned the HKD 140,000, by having Z exchange HKD 140,000 for JPY under Z's own name.

340. Police therefore arrested X in September 2013 for violating the Act on Punishment of Organized Crimes (disguise of facts with respect to disposition of criminal proceeds).

4.24 Currency smuggling (including issues of concealment and security)

COOK ISLANDS

341. In March 2013, a foreign national arrived into the Cook Islands with a total cash of AUD$18,900 (USD17,407) and USD$3,800 and failed to declare upon his arrival. The following day the subject walked into one of the local banks to exchange the money into New Zealand dollars. A

report was made to CIFIU and the matter was investigated. As a result the subject was sternly warned.

FIJI

Case 1

342. A Chinese national, Person X was charged for one count of failing to declare currency of FJ$52,987 (USD28,949). It was noted that the total possession of currency comprised of 6 different currencies including AUD, USD, HKD, SGD, BAHT and RMB.

343. Person X was interrogated by Customs Officials and arrested. Person X was produced at the Nadi Magistrates Court and he pleaded guilty. The accused was fined FJ$2,000 (USD1,093) in default of six months imprisonment. The money was released to the accused.

Case 2

344. A local couple, Person A & Person B were charged for one count of failing to declare currency of USD5,890, AU$165(USD153), NZ$620 (USD531) and FJ$97 (USD53).

345. Person A, the wife was in possession of the currency and was produced at the Nadi Magistrates Court and she pleaded guilty. The accused was fined FJ$100 (USD50) in default of 10 days imprisonment. The money was released to the accused.

4.25 Use of credit cards, cheques, promissory notes, etc.

PAKISTAN

346. “Mr. A” approached the “Bank W” to open a sole proprietorship account by the name of “M/s. SAF”, having the business of vehicle tracking systems. However, “Bank W” refused to open the account on the back of dubious particulars provided by Mr. A for opening the account and reported STR to FMU. Forged cheques were used for fraudulent activities.

347. Upon probing the online SECP database, it was revealed that M/s. SAF is a Private Limited Company. The risk screening watch list depicts positive hit of “Mr. A”, having same parentage, was involved in a terrorism case. Based on the facts, the financial intelligence was shared with LEA for further investigation.

348. In response, LEA approached the management of “M/s. SAF (Pvt.) Ltd” for the verification of “Mr. A” and found that “Mr. A” has never been employed/worked on behalf of Company.

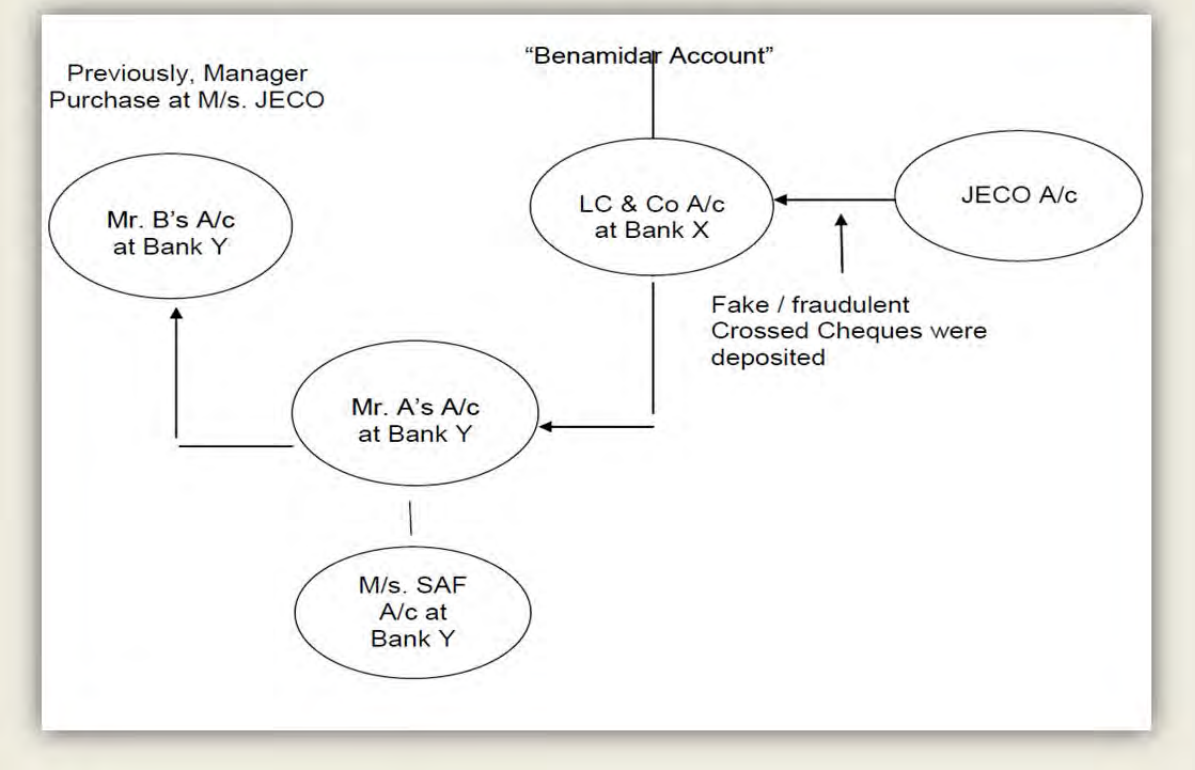
349. The enquiry conducted by LEA further revealed that “Mr. A” appeared in Red Book is not the same person who was involved in terrorism. Nevertheless, LEA conducted physical verification of provided contact particulars of “Mr. A”, which transpired his couple of accounts at “Bank Y” with the titles of “Mr. A” and “M/s. SAF”.

350. The details of account title “Mr. A” suggested high turnover, which was not commensurate with the declared CDD profile of “Mr. A”. The transactions trail of account title “Mr. A” suggested that funds were received from “M/s. LC & Co”, a proprietorship concern associated with civil work and general order supplier, having account at “Bank X”.

351. Moreover, the account title “LC & Co” was found as “Benamidar” owing to different beneficial owner. Upon receipt, “Mr. A” transferred the funds to “Mr. B’s account” at the same bank i.e. “Bank Y”. “Mr. B” previously served as Manager / In-charge Purchase at “M/s. JECO Limited”.

352. In view of aforementioned transaction trail, further enquiry into the account title “LC & Co” at “Bank X” was conducted by LEA to identify the source of funds. The said enquiry revealed that

forged cheques were deposited in the account title "LC & Co" by the concerned staff (including Mr. B) of "M/s. JECO Limited" to conceal the misappropriations by falsifying the books of account. These funds were then routed through "Mr. A"s account" to "Mr. B's account" at the same bank i.e. "Bank Y".



THE PHILIPPINES

Case 1

353. HSS was arrested in a buy-bust operation conducted by LEA.

354. Financial investigation revealed that HSS worked as a cook at a local restaurant in Binondo, Manila. She had a number of active bank accounts with transactions involving significant amounts. Her transactions were not commensurate with her source of income.

355. One of her bank accounts showed a purchase of a manager's cheque worth PHP3 million (USD68,812) paid to MS Inc., a well-known department store, for the purchase of several MS Gift Cheques. She used these cheques to launder part of the illegal drug proceeds by:
- exchanging these cheques (at a discounted value) to cash i.e., approaching MS Store patrons who would agree to exchange their cash to cheques; and
- purchasing goods such as jewellery, perfumes, clothing, and appliances at MS Store, then selling these items to innocent parties in legitimate transactions, thereby, converting the otherwise illegal drug proceeds into clean funds.

Case 2

356. Suspicious Transactions Reports were received from different commercial banks about fraudulent negotiations of spurious and altered cheques.

357. These cheques were deposited with rural banks. Since rural banks do not have clearing facilities, such banks deposit the same with commercial banks, which in turn present the same for clearing with the issuing banks. Upon verification by the issuing bank with the drawer, it was discovered these cheques were either spurious or altered.

358. In the case of altered cheques, it was found that the same have either been lost or stolen and thereafter altered with respect to the amount, payee, and serial numbers, among others. Interestingly, some of these altered cheques were dishonoured immediately after they were presented to the issuing bank either because the alterations are glaring or the altered amount exceeded the outstanding balance of the account. However, there were incidences where the cheques passed through clearing and the culprits were able to withdraw the amounts of the cheques.

359. Further investigations conducted revealed that since these cheques are crossed, the persons responsible for the counterfeiting and alterations, or their cohorts, opened accounts with rural banks. They then deposited the cheques to these accounts, taking chances that the same would pass the clearing and amounts thereof would be credited to their accounts for withdrawal. During the account opening, these persons presented identification documents which upon verification turned out to be fictitious.

360. However, the identification documents bore pictures of the account owners which were authentic as per information from the rural banks, and which lead to the identification and arrest of the persons, who turned out to be spouses, responsible for the counterfeiting of the spurious and altered cheque.

4.26 Structuring (smurfing)

AUSTRALIA

Case 1

361. AUSTRAC disseminated a suspect transaction report (SUSTR) to a law enforcement partner agency, which sparked an investigation into a widespread money laundering syndicate.

362. Investigations revealed that the syndicate, which operated in multiple states across Australia, was using a money laundering technique known as 'cuckoo smurfing'.

363. The criminal syndicate misused the bank account of a legitimate Australia-based export company in its money laundering scheme. The scheme also exploited legitimate international funds transfers made by a customer of the export company, who was based in Pakistan.

364. The Pakistan-based customer sent funds, via a remittance business in Pakistan, to the Australia-based export company. The funds transfers were payments for legitimate invoices owing to the Australian company.

365. However, investigations revealed that the Pakistani remitter used to remit the funds had connections with money laundering crime syndicates in Australia.

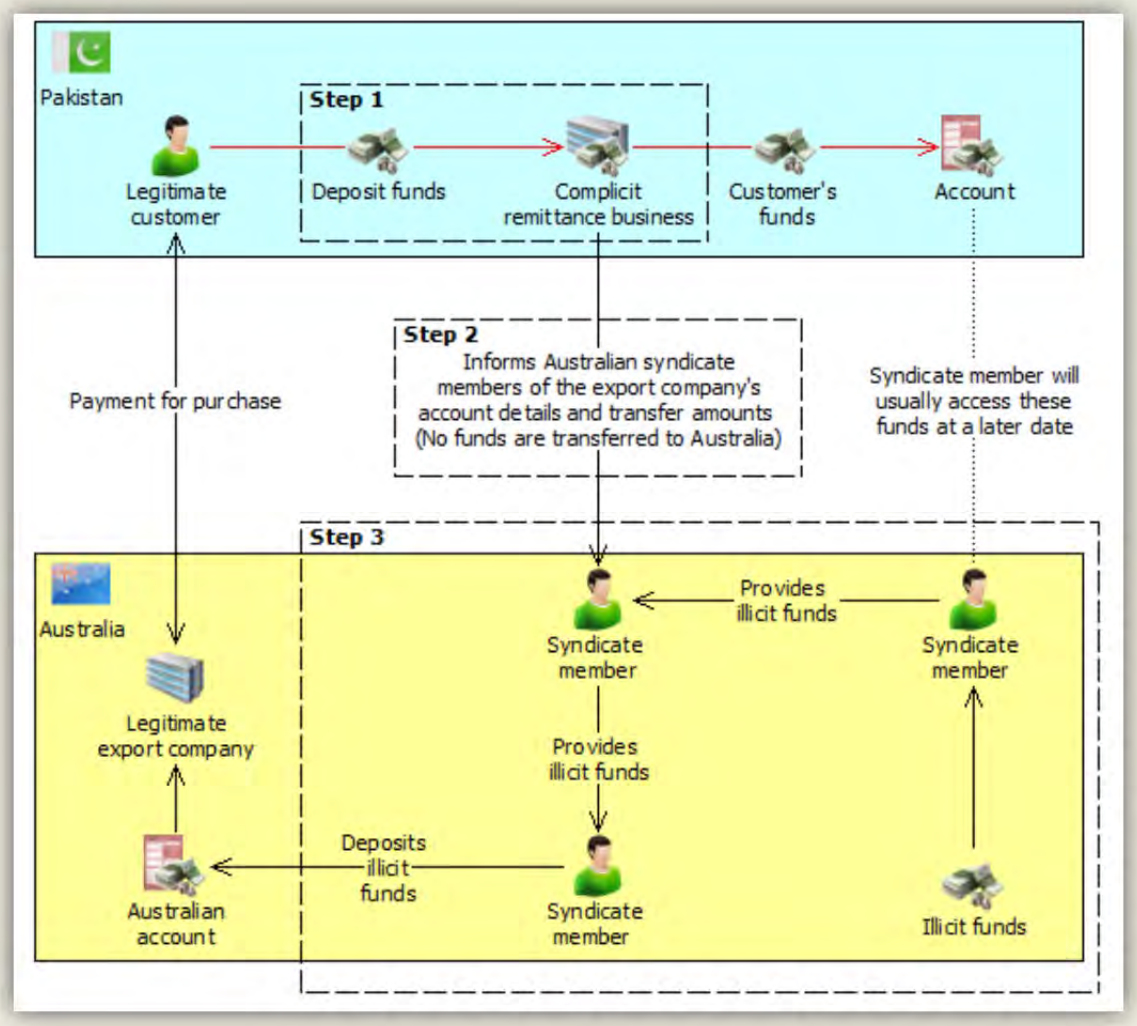
366. The following steps outline how the illicit funds were laundered:
- The Pakistan-based customer of the export company attempted to send funds via a Pakistani remittance business to the export company's Australian bank account, for the payment of legitimate invoices.
- The Pakistani remitter informed the money laundering syndicate in Australia of the export company's bank account details and the amounts required to be deposited into the company's account in Australia.
- Australian syndicate members made a number of cash deposits into the Australian account of the export company equal in value to the expected payments from Pakistan. The cash deposits were often made in structured amounts, intended to fall below the AUD10,000 cash transaction reporting threshold. These funds were the proceeds of illicit activities undertaken in Australia.

- Meanwhile, the remitter in Pakistan transferred the funds provided by the customer in Pakistan into another account in Pakistan, to be later accessed by a member of the syndicate.

367. Over a 15-month period, 13 SUSTRs were reported to AUSTRAC by major banks, identifying multiple structured cash deposits made by third parties into the export company's Australian bank account.

368. During this period approximately ten syndicate members conducted 217 cash deposits totalling AUD2.1 million (USD1.9 million) into the Australian bank account of the export company. A total of 196 of these cash deposits were structured deposits, totalling AUD1.6 million (USD1.5 million). The structured deposits were primarily conducted in amounts between AUD8,000 and AUD9,500 at multiple bank branches throughout Sydney and Melbourne.

369. The syndicate members were careful to provide the bare minimum of personal information when undertaking the cash deposits. Nevertheless, 18 bank deposit receipts examined by law enforcement revealed identifying characteristics such as phone numbers. This information led to the identification of some of the depositors.



Offence	Money laundering
Customer	Business
Industry	Banking (ADIs)
Channel	Physical
Report type	SUSTR
Jurisdiction	Domestic International - Pakistan
Designated service	Account and deposit-taking services
Indicators	Multiple third-party cash deposits into the same account conducted on the same day Third-party cash deposits conducted at multiple branches in the same city Third-party customer undertaking transaction provides the bare minimum of information to reporting entity about the transaction Structuring of cash deposits

Case 2

370. A suspect transaction report (SUSTR) triggered AUSTRAC's automated monitoring system, revealing a syndicate using a technique known as 'cuckoo smurfing' to launder funds, suspected to be the proceeds of illicit drug sales.

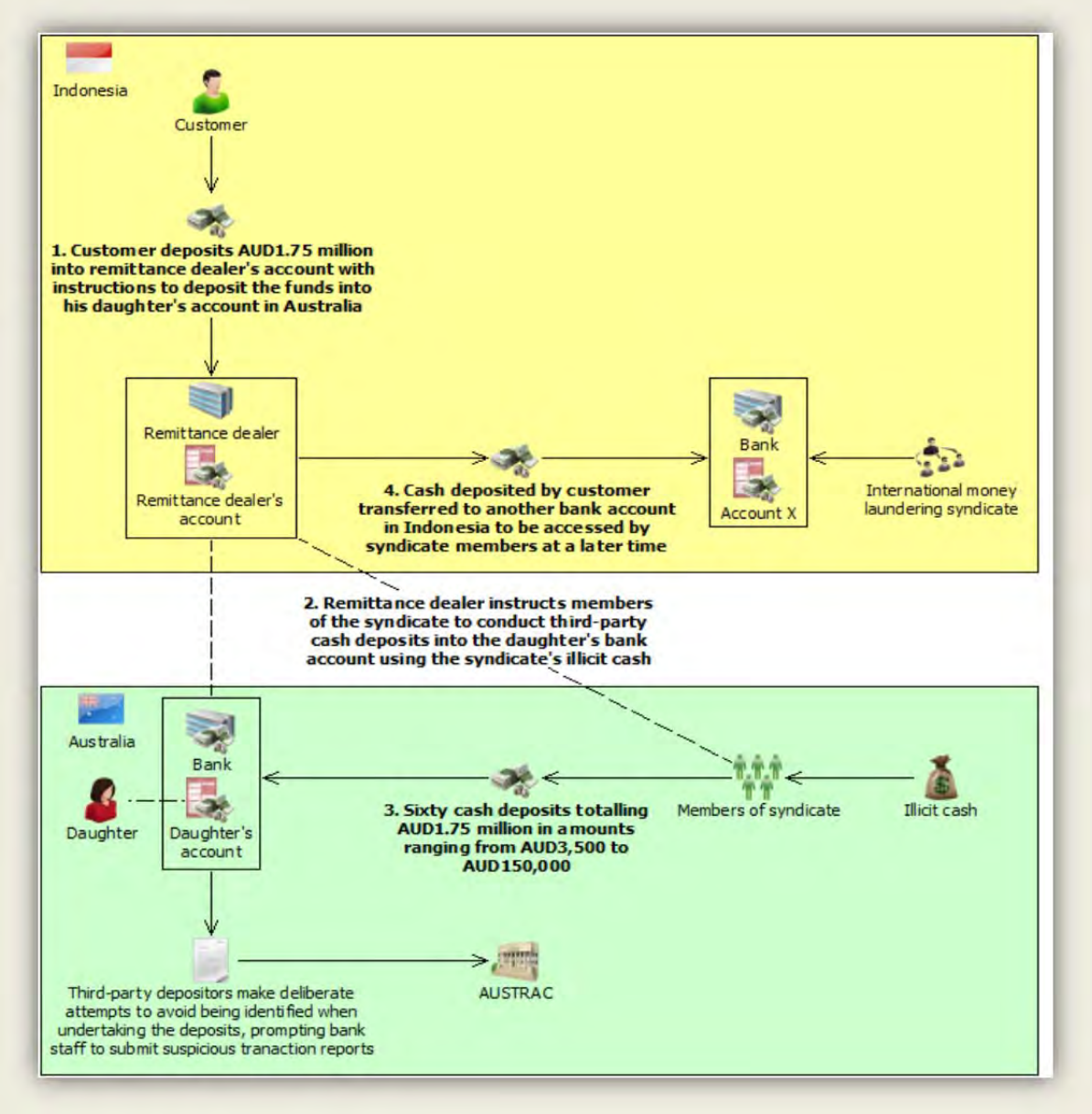
371. The SUSTR was submitted after a legitimate customer in Indonesia attempted to transfer AUD1.75 million (USD1.62 million) to his daughter, who was studying in Australia. However, the funds were unlawfully diverted by an Indonesian remittance dealer, who was connected with an international money laundering syndicate operating in Australia.

372. The money laundering methodology operated as follows:
- The customer in Indonesia deposited cash into the remittance dealer's bank account in Indonesia.
- He provided the remittance dealer with his daughter's Australian bank account details and instructed that the deposited funds be transferred to his daughter.
- Rather than transfer the funds to Australia, the Indonesian remittance dealer informed members of the syndicate in Australia of the daughter's bank account details. The syndicate members in Australia used this information to make a number of 'third-party' cash deposits into the account. The syndicate members made multiple cash deposits at bank branches throughout New South Wales and Victoria. Often these deposits were made on the same day, prompting bank staff to suspect that the cash deposits may have been for illicit purposes.
- Over a six-week period, the daughter's Australian bank account received 60 cash deposits totalling AUD1.75 million (USD1.62 million). The cash deposits ranged from AUD3,500 to AUD150,000.
- The cash the customer had originally deposited into the remitter's bank account in Indonesia was transferred to another bank account (Account X) to be accessed by the syndicate members at a later time.
- This completed the 'cuckoo smurfing' operation. With the assistance of the complicit remittance dealer, the syndicate had introduced illicit cash into the Australian banking system via the bank account of the unsuspecting customer in Australia. This left the syndicate free to access the 'clean' money, which the Indonesian remitter had transferred into Account X, without attracting the attention of authorities.

373. The third-party depositors made deliberate attempts to avoid being identified when undertaking the deposits, prompting bank staff in Australia to report the transactions to AUSTRAC as suspicious. In particular, four SUSTRs submitted to AUSTRAC detailed how:
- the third-party depositors attempted to avoid being identified by not wanting to provide their names and details on deposit slips and by writing telephone/fax numbers in an illegible manner
- the third-party depositors only used their given names on deposit slips.

374. Authorities also identified that one of the third-party depositors was involved with a drug syndicate.

Offence	Money laundering
Customer	Business Individual
Industry	Remittance services Banking (ADIs)
Channel	Physical
Report type	IFTI SCTR SUSTR
Jurisdiction	Domestic International – Indonesia
Designated service	Account and deposit-taking services
Indicators	High levels of cash deposits far in excess of expected legitimate banking activity of the account holder Multiple cash deposits, at multiple bank branches, often on the same day Third-party cash deposits made at branches distant from the branch at which the account is held Third-party cash deposits made by unidentifiable persons Third-party deposits made by evasive customers with incomplete identification



COOK ISLANDS

375. The CIFIU referred another structuring case to the Police to investigate. The subject involved is an Aircraft Engineer and he transfers funds of $9,999 once a month from his work income into his trust account in his home country. The matter is still under investigation.

INDIA

376. The case was registered for the predicate offence under the Prevention of Corruption Act against a highly placed official of Government Undertaking for possessing disproportionate assets worth INR 4.5 million (USD77,189). The proceeds of crime were deposited in the name of 49 fictitious depositors indicating the accused as nominee in all the deposits by using all possible means to avoid KYC/reporting norms. A loan amount of INR 1.7 million (USD29,160) was taken against the above fictitious deposits to purchase a flat in the name of his son, which was later sold for INR 6.2 million (USD106,350). The sale proceeds were placed into fixed deposits in the name of his son.

PAKISTAN

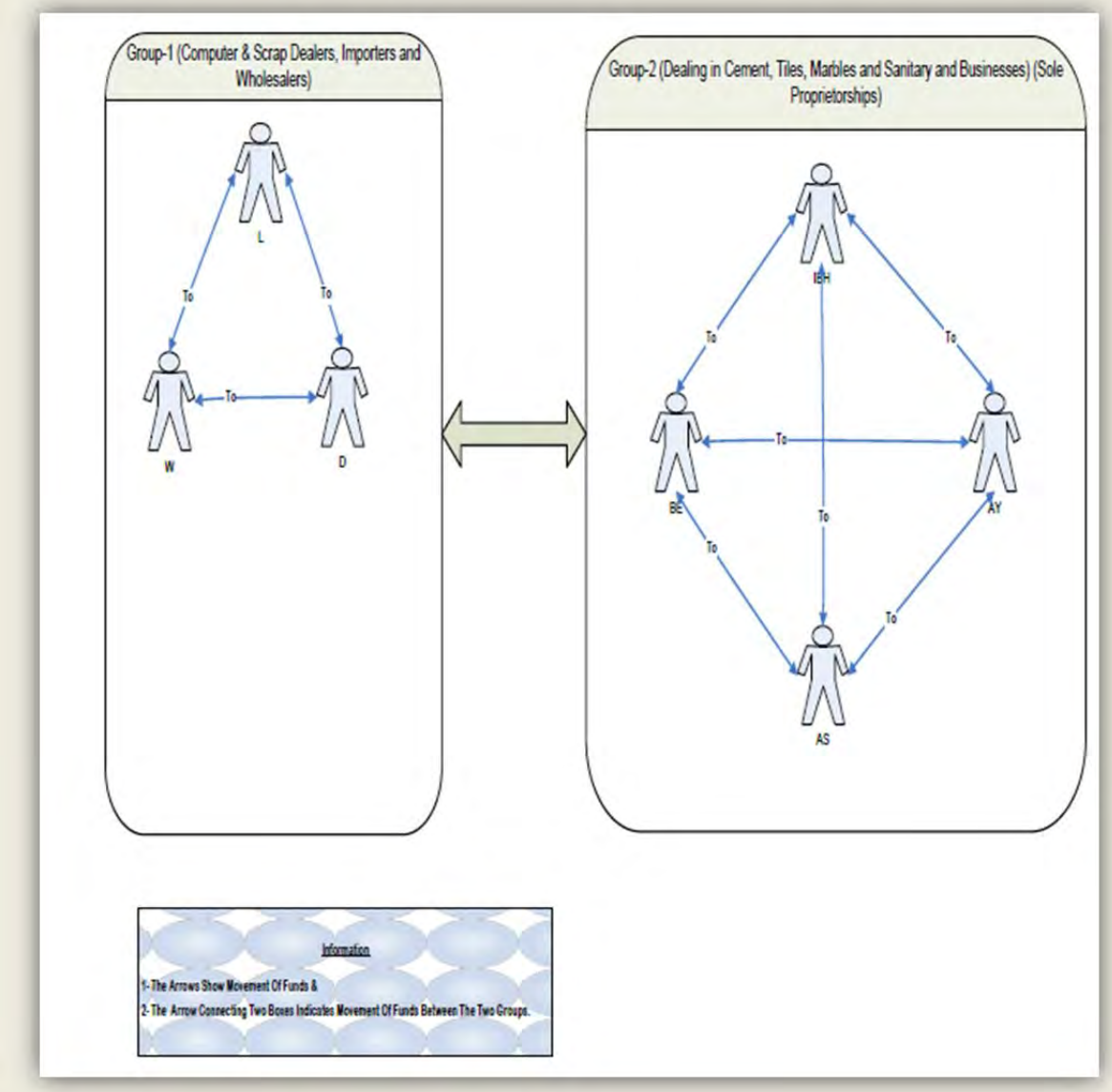
377. Account information of customer L was requested by a Law Enforcement Agency from bank for his alleged involvement in fraudulent trading activities. The bank, besides giving information to LEA, also reported STR to FMU.

378. The suspect L had a network in terms of exchange of funds with other six customers namely W, D, AY, AS, BE and IBH against whom suspicions were also raised by the bank.

379. It was found that the suspects L, W, & D deal in the business of import and wholesale of computers and scrap. Whereas suspects AY, AS, BE and IBH are close relatives of each other and deal in wholesale business of cement, sand, tiles and other sanitary products.

380. The suspects L, W, & D opened accounts on the same date and in the same branch "M" of the bank "MM". All the suspects are introducers of each other and live around in the same locality wherein mostly low income profile people live.

381. The suspects AY, AS, BE and IBH opened accounts either on the same date or in the consecutive month. Interestingly, the bank and branch of the all the suspects is the same as that of the suspects L, W, & D, i.e. the branch "M" of the bank "MM".



382. A detailed analysis of the transactions revealed that there were actually two groups who are connected with each other. Group-1 comprises the suspects L, W, & D whereas Group-2 comprises the suspects AY, AS, BE and IBH.

383. Group-1 transferred millions of rupees on a daily basis among them via cash and transfer mode. The pattern of transactions suggested immediate deposits and withdrawal of the funds and transfer of funds to other suspects in either the same Group-1 or in Group-2. Further, the same type of pattern of transactions was observed in Group-2. It appears that both groups were trying to create a complex network of movements of funds in order to hide source of funds.

384. In conclusion, as the suspect L is allegedly involved in fraudulent import activities, the noted suspicious funds appear to be earned through fraudulent import activities and, therefore, all the suspects in Group-1 and Group-2 probably tried to integrate the suspicious funds in legal economy by creating complex movement of funds through banking channels.

385. The intelligence has been disseminated to LEA for necessary action.

4.27 Wire transfers/Use of foreign bank accounts

FIJI

386. An STR was reported on a university student, Person A, who received two large telegraphic transfers totalling FJ$76,624 (USD41,863), from unrelated individuals/entities in Australia to her personal bank account.

- The 1st telegraphic transfer of FJ$4,495 (USD2,456) was remitted into Person A's account from one Person B in Australia. On the same day, Person A withdrew the exact amount and two days later, remitted FJ$3,880 (USD2,120) to one Person C in South Africa.
- The 2nd telegraphic transfer of FJ$72,128 (USD39,406) was remitted into Person A's account from a Company D in Australia. On the same day, Person A withdrew FJ$10,000 (USD5,463) cash and transferred FJ$40,000 (USD21,854) to her mother's bank account. Person A continued to remit funds to Person C in South Africa. Investigations revealed that the funds were sent from Company D's bank account without proper authorization.
- A 3rd telegraphic transfer of USD8,750 was about to be remitted from Person E in Spain to Person A's bank account. However this remittance was stopped because the local commercial bank received a message that the sending customer's email was hacked and funds were sent without proper authorization.

387. Investigations revealed that Person A was communicating with an individual via Facebook to whom she provided her account details.

HONG KONG, CHINA

388. In early November 2012, a victim in a jurisdiction outside Hong Kong received a phone call from a group of people who alleged themselves to be police in that jurisdiction. The suspects accused the victim of being involved in a deception case and instructed to transfer money to a bank account in Hong Kong, claiming that the money would be under Police's supervision.

389. The victim complied and made a wire transfer of approximately HK$390,000 (USD50,302) to a bank account in Hong Kong which was subsequently withdrawn by cash. The victim eventually realized that she was deceived and a report was made to the police. The account holder was found to have left Hong Kong after withdrawing the crime proceeds from the account and had not returned since then.

4.28 Commodity exchanges (barter – e.g. reinvestment in illicit drugs)

390. No cases received.

4.29 Use of false identification

391. No cases received.

4.30 Others

CANADA and USA

OPEN SOURCE NEWS ITEMS

Department of Justice
Office of Public Affairs

FOR IMMEDIATE RELEASE Thursday, December 19, 2013

Canadian Citizen Arrested for Money Laundering in Connection with Illegal Importation and Trafficking of Narwhal Tusks

A Canadian man was arrested today in St. John, New Brunswick, Canada, on an extradition warrant requested by the United States for money laundering crimes related to the illegal importation and illegal trafficking of narwhal tusks, announced Robert G. Dreher, Acting Assistant Attorney General for the Environment and Natural Resources Division.

On Nov. 14, 2012, a federal grand jury sitting in Bangor, Maine, returned an indictment that was partially unsealed today upon the arrest of Gregory R. Logan of Grand Prairie, Alberta, Canada. The indictment also names Jay G. Conrad of Lakeland, Tenn., and Andrew L. Zarauskas of Union, N.J. Logan was arrested on charges in the indictment for money laundering conspiracy and substantive money laundering violations. The indictment also charges Conrad and Zarauskas with conspiracy to smuggle narwhal tusks, money laundering conspiracy, smuggling narwhal tusks and money laundering violations. According to the indictment, Logan illegally laundered the money earned from his illegal imports and sales of narwhal tusks in the United States. It further charges that Conrad and Zarauskas bought the narwhal tusks from Logan, knowing the tusks had been illegally imported into the United States, and sold or attempted to sell the tusks after their illegal importation.

The arrest of Logan on an extradition warrant in Canada begins the extradition process to the U.S. The extradition process is governed by a 1971 extradition treaty between the U.S. and Canada.

The charges contained in the indictment are merely accusations and the defendants are presumed innocent unless and until proven guilty in a court of law. If convicted of these charges, the defendants each face up to twenty years in prison on each of the most serious charges, as well as fines up to $250,000.

The case was investigated by agents from National Oceanic and Atmospheric Administration Office of Law Enforcement and the U.S. Fish and Wildlife Service Office of Law Enforcement. The case is being prosecuted by Trial Attorney Todd S. Mikolop of the Justice Department's Environmental Crimes Section, with assistance from the Justice Department's Office of International Affairs.

http://www.justice.gov/opa/pr/2013/December/13-enrd-1341.html

Former Mountie Gregory Logan, who ran narwhal tusk-smuggling ring, facing up to 20 years in U.S. prison

Tristin Hopper | December 19, 2013 | Last Updated: Dec 19 9:46 PM ET

Gregory Logan, an Alberta ex-Mountie who for 10 years orchestrated the most pervasive narwhal tusk-smuggling ring of modern times, is now set to face U.S. prosecutors only two months after a New Brunswick court handed him Canada's largest-ever wildlife penalty.

On Thursday, acting on an international warrant, police arrested the 50-something Grande Prairie man in Saint John, N.B. He is awaiting extradition to the United States on money-laundering charges.

"If convicted of these charges," noted a Thursday statement by the U.S. Department of Justice, Logan could "face up to 20 years in prison … as well as fines up to $250,000."

For more than 10 years, Logan used New Brunswick as a base to smuggle as many as 250 narwhal tusks past a sleepy border station in Bangor, Maine.

Although the tusks, which are really an elongated tooth, are legal in Canada under strict conditions, the importation of narwhal products into the United States has been banned since 1972.

As revealed by Operation Longtooth, a two-and-a-half year Environment Canada probe first spurred by a 2009 tipoff from U.S. authorities, Logan's method of smuggling was simply to legally purchase Canadian tusks and slip them past border guards by strapping them underneath a modified trailer.

Once on U.S soil, Logan would then FedEx the long, spiralled tusks to a U.S.-wide network of illicit contacts.

Two of Logan's alleged contacts, Tennessee roofing contractor Jay Conrad, and unemployed New Jersey oil tank repairman Andrew Zarauskas, were first issued with a U.S. grand jury indictment in November of 2012 and are facing similar money-laundering charges.

Logan's Thursday arrest and pending extradition come only two months after a Canadian court handed him a fine of $385,000 and an eight-month conditional sentence in connection with the smuggling ring.

At the time, Environment Minister Leona Aglukkaq, who comes from Nunavut, told the territory's media that Logan's punishment was "the largest penalty ever handed down in Canada" for a wildlife offence of its kind.

According to an earlier indictment cited Thursday by the U.S. Department of Justice, Logan's money-laundering charges are related to "money earned from his illegal imports and sales of narwhal tusks in the United States."

http://news.nationalpost.com/2013/12/19/former-mountie-gregory-logan-who-ran-narwhal-tusk-smuggling-ring-facing-up-to-20-years-in-u-s-prison/

CHINESE TAIPEI

Fraud/Ponzi scheme case developed directly from suspicious or cash/threshold transaction reports:

392. In January 2012, the AMLD received an STR from Bank A describing that Mr. W, a foreign person-in-charge, chairman and general manager together with directors Mr. X and Ms. Y (Mr. X's girlfriend) jointly operated the Dream Company and on two consecutive business days just

before closing hour, Mr. X and Mr. Z, the Dream Company's accountant, withdrew large amounts of cash at Bank A.

393. They were, however, unable to provide a convincing answer to an employee of Bank A's questions pursuant to Bank A's Customer Due Diligence (CDD) practice with respect to the use of the funds. So Bank A filed an STR to the AMLD. Dream Company and the said individuals had been under investigation by the Taipei Field Division at the time if the STR filed to the AMLD.

394. After collecting Dream Company's background and analysing the relevant transactions, the AMLD discovered that the company might be using means akin to a Ponzi scheme to defraud investors. As a result, the AMLD referred the case to the Taipei Field Division.

395. In February 2012, one investor complained to the police that the Dream Company failed to pay the principal sum and interest invested by him, which were due. The police informed the relevant bank to flag some of the banking accounts of the Dream Company as "suspicious accounts".

396. Mr. W was alerted of this and fled away to Japan on 29 February of 2012. Mr. X and his girlfriend, Ms. Y also attempted to leave Chinese Taipei on March 6 but were arrested by the investigators at Taoyuan International Airport and then were caught into custody.

397. Following the investigation, the Dream Company had been found to be engaging in multi-level marketing to defraud its investors. It illegally raised, from investors in Chinese Taipei a sum in excess of NTD 2.5 billion (over USD 83.3 million) by allegedly promising investors that their investment would be used in the installation of coin-operated massage chairs in overseas supermarkets and theme parks. Investors who paid certain amounts of money, for example NTD 98,000 (USD3,500) or NTD318,000(USD11,000) for a unit of investment, would receive a monthly return of 30%.

398. The Dream Company stressed that investors would recover their principal sum and earn more than three times their initial investments within 10 months of investments. In reality, the Dream Company was "robbing Peter to pay Paul" in a manner akin to a Ponzi scheme where subsequent investors' money was used to pay the principal sum and interest of previous investors to defraud its investors.

399. During a raid on the Dream Company's premises on March 7 of 2012, the Taipei Field Division seized cash amounting to approximately NTD11 million (about USD400,000) and froze bank holdings of about NTD60 million(about USD 2 million).

400. The AMLD also helped trace the money flows and on the following day, found the illegal flow of funds into the bank accounts of Messieurs W, X, Y and Z. The AMLD then assisted in freezing the funds, which amounted to about NTD93 million (about USD3.1 million). The total amount of illegal funds seized was about NTD170 million (about USD5.5 million).

401. The AMLD also found that between August 2010 and February 2012, the Dream Company remitted over NTD1 billion (about USD33.3 million) of its illegal gains to its overseas branch in Japan. An additional amount of NTD8.4 million (about USD280,000) was remitted to a personal banking account maintained by Ms. Y in Malaysia.

402. The Taipei District Prosecutors Office sought an imprisonment term of 18 years for Mr. W, the person-in-charge, and Mr. X, director of Dream Company; 16 years for Ms. Y, another director, and six months for the company's accountant, Mr. Z.

403. During the investigation, Bank A assisted the AMLD in freezing illegal gains in relevant accounts. After prosecution of the relevant parties, the AMLD notified Bank A to give administrative reward to the related employees. The AMLD also exchanged information on the

aforesaid ML with the FIUs of the relevant countries through the Egmont Group's Security Website. At present the Japanese LEA has initiated criminal investigations on Mr. W who had absconded to Japan.

HONG KONG, CHINA

OPEN SOURCE NEWS ITEMS

Birmingham football club boss Carson Yeung jailed for six years

By Grace Li and James Pomfret

HONG KONG Fri Mar 7, 2014 11:52am GMT

(Reuters) - Hong Kong businessman Carson Yeung was sentenced to six years in jail on Friday for money laundering in a high-profile case that law enforcement officials hailed as an important victory to combat money laundering in the global financial hub.

Yeung, 54, who was found guilty by a Hong Kong court on five counts of money-laundering some HK$721 million ($93 million) over several years, is a flamboyant self-made millionaire and owner of British football club Birmingham City.

In the detailed exposition of hundreds of suspicious transactions made by Yeung and multiple parties, the trial cast a rare spotlight on some of the murky channels and methods used by underground banks and money launderers in moving illicit capital between China, Hong Kong and the gambling hub of Macau.

"Maintaining the integrity of the banking system is of paramount importance if Hong Kong is to remain an international finance centre," said District Court Judge Douglas Yau. "The sentence must include an element of deterrence to discourage those who are in a position to exploit the system for their own gains through money laundering and to send the message that...the law will come down on them with full force."

Yeung, dressed in a dark suit, appeared relaxed and waved before being taken away. His defence lawyers declined to comment on whether he would appeal.

Police investigators, who described the case as a difficult one involving analysis of financial records from as far back as 2001, welcomed the sentence even though it was less than the maximum 14 years possible for such crimes.

"We overcame a lot of hurdles to get this result," said Gloria Yu, a police investigator, to reporters outside the courthouse. "We are happy...and encouraged because fighting money laundering is a very arduous task."

Yeung, a former hair stylist to Hong Kong's rich and famous, who pleaded not guilty, had told the court he amassed his wealth through his hair salons, share trading, property purchases, gambling in Macau and other investments.

MACAU CONNECTION

The trial, which lasted more than 50 days, revealed the businessman's close ties to Macau's casino world, both as an investor and gambler, and how that facilitated business investments that helped him amass further wealth.

Yeung told the court how he first started gambling in the former Portuguese enclave around 1997 and in 2004 was introduced to the Neptune VIP Club inside the Lisboa casino.

In 2005, two businessmen, Lin Cheuk-fung and Cheung Chi-tai, offered Yeung the chance to invest in junket operator Neptune Group. Junket operators bring in gamblers from mainland China and offer lines of credit and often collect debts from them.

A Reuters' 2010 special report found links between Cheung and organised criminal gangs, or triads, and a casino run by gambling goliath Las Vegas Sands in Macau. (reut.rs/1fcLwB5)

While Cheung hasn't been convicted of any triad-related crimes, his organised crime affiliation was corroborated by U.S. authorities and former and current police officials.

The Hong Kong court heard how Yeung had received hundreds of deposits of unclear provenance for what Yeung claimed to be winnings from his gambling. These included cash payments from Cheung and a tranche of cheques worth HK$72.5 million ($9.34 million) from Macau casino operator Sociedade de Jogos de Macau S.A., part of SJM Holdings Ltd, which is owned by gambling tycoon Stanley Ho.

Yu, the police investigator, admitted many aspects of the case remain unsolved including, crucially, the origination of much of the laundered cash. But she said that investigations would continue in a bid to bring others to justice.

The judge said that while Yeung wasn't the mastermind or "director" of a laundering scheme, "without his considerable skills in share dealings and connections to the Macau casinos, the laundering could not have gone on for such a long time and on such a large scale."

Yeung, who bought Birmingham City Football Club in 2009, stepped down last month as head of the club and its holding company, Birmingham International Holdings Ltd.

After Yeung was convicted, club officials said the verdict would have no impact on its day-to-day operations.

(Editing by Matt Driskill)

http://uk.reuters.com/article/2014/03/07/uk-soccer-birmingham-idUKBREA2609S20140307

Man who laundered HK$13b must pay HK$5m or get longer sentence

Thursday, 10 October, 2013, 3:16am

A mainlander who set Hong Kong's money-laundering record of HK$13.1 billion must hand over HK$5.2 million left in his bank accounts or face a longer jail term.

The Court of First Instance on Wednesday ordered Luo Juncheng, 22, to hand over the money in a month or have as much as five years added to his 10½-year sentence.

Madam Justice Ester Toh Lye-ping made the order in response to a Department of Justice application after the money was found in two Chiyu Bank accounts that Luo held personally or through a company he controlled.

Luo asked the judge why the money in his personal account should be seized.

"Once the prosecution proved you benefited from the crime, you are not allowed to keep the proceeds of the crime and therefore it should be confiscated," Toh said.

"If in the period I imposed, you do not hand over the money in your personal account and the account of the company you have control, I can impose additional imprisonment," she said. "Considering the amount involved, the term of imprisonment may be about five years."

Luo was found guilty by a Court of First Instance jury in January of dealing with property known or reasonably believed to represent proceeds of an indictable offence.

He made 4,800 deposits and 3,500 transfers through a Chiyu Bank account between August 2009 and April 2010, with most of the funds funnelled via internet transfers.

Sentencing Luo earlier, Toh said his crime was the most serious of its kind that she had seen before Hong Kong's courts and she could not find a case involving anywhere near such a large amount.

She said it was now urgent to review the maximum penalties for the offence, which was becoming more prevalent.

http://www.scmp.com/news/hong-kong/article/1327970/man-who-laundered-hk13b-must-pay-hk5m-or-get-longer-sentence

MACAO, CHINA

Money Laundering through Trading Companies

404. Technology Company B received frequent remittance, totally over MOP400 million (USD51 million) in 2 months from several trade companies incorporated in Jurisdiction X. As the bank did not find any transactions from the accounts of Company B that were related to its business, the use of the accounts did not obviously match with the stated business purpose. This case was finally reported to FIU.

405. Based on the intelligence received by FIU, it was revealed that one of the trade companies in Jurisdiction X was involved in a fraud case being under investigation in which the criminal proceeds were laundered through the trade companies. FIU then reported this case to law enforcement agencies for further investigation.

PAKISTAN

Abuse of Non Profit Organizations (NPOs)

406. Heavy remittances were being received from an NGO in USA into the personal accounts of Mr. Green. The funds received are later channelled through different accounts and withdrawals were mostly made in cash while few transactions involved transfer of funds to other individuals.

407. Mr. Green is working at an NGO which is not registered in Pakistan though it is registered in USA. Main activities of the NGO included doing social work for Northern Areas of Pakistan and Afghanistan. Mr. Green was maintaining five different accounts at different branches of the same bank. Mr. Green did not provide documentary evidence of the NGO where he was working while opening the accounts.

408. Four of these accounts were Mr. Green's personal accounts which were opened for the purpose of salary and saving, whereas one of the accounts was his sole proprietorship account. Mr. Green received huge amount of funds from the NGO head office situated in USA. These funds

were first being credited into the accounts which were being maintained at bank branches at remote area and then the funds were transferred to another account of Mr. Green in other area.

409. The funds after being credited to Mr. Green's personal account were mostly withdrawn in cash and few transactions were observed in which the funds were transferred to the accounts of different individuals involved in different businesses. Adverse information was also found on the risk screening database about the NGO and its CEO. There is a suspicion of fraud and embezzlement of funds.

Fraud

410. Mr. X defrauded innocent job seekers by giving bogus advertisements for jobs in the reputed newspapers and inducing the candidates to deposit PKR 400 to 600 (USD4 to USD6) in his account(s) as courier and application processing charges

411. Mr. X opened his personal account in ABC Bank. After one month of the establishment of the relationship, ABC Bank noticed numerous cash deposits of PKR 400 (USD4) in his account. ABC Bank came to know that Mr. X published an advertisement in a reputed newspaper inviting CVs on his email from jobseekers for different vacancies. After receiving CVs from the jobseekers he asked the jobseekers to deposit PKR 400 (USD4) in his account as the courier & application processing charges.

412. In view of above facts, ABC Bank terminated the relationship of Mr. X on the grounds that he may be running a job scam. After just a few days, Mr. X approached another branch of ABC Bank to open an account in the name of XYZ Corporation mentioning himself as the sole proprietor / CEO of XYZ Corporation. XYZ Corporation was meant to provide HR Consultancy & Recruitment Services. The bank identified Mr. X as the same person engaged in running a job scam and hence refused to open the account. Actually, ABC Bank had put the name & CNIC of Mr. X on the watch list, so that, he would not be able to open any account anywhere in their bank. ABC Bank also reported the STR to FMU.

413. As the ABC Bank refused to open an account for Mr. X, he went to DEF Bank and got two accounts opened i.e. one in his own name and other with title XYZ Corporation. Here he continued the same activity and many deposits of PKR 600 (USD6) were noticed in the account of XYZ Corporation. DEF Bank took notice of such transactions and closed his account.

414. After his account was closed in DEF Bank, Mr. X approached another Bank GHI and again got two accounts opened i.e. one in his own name and other with title XYZ Corporation. After around two months of opening Mr X's account, GHI bank received a complaint against XYZ Corporation for its involvement in deceptive recruitment activities. The complainant complained that XYZ Corporation had defrauded her and other job seekers by asking them to deposit PKR 600 (USD6) for processing and courier charges. GHI Bank closed both of Mr X's accounts on the suspicion that Mr. X may be running a job scam and reported the STR to FMU.

415. Meanwhile, Mr. X approached JKL Bank and opened an account with title XYZ Corporation. JKL Bank also observed many deposits of PKR 600 (USD6) in the account of XYZ Corporation. The activity was continued for up to two months. JKL Bank didn't terminate the relationship with XYZ Corporation, however reported STR to FMU. The transaction activity in the account, however, was stopped after two months leaving a balance of PKR 60,000 (USD600).

416. After his account was closed by GHI Bank, Mr. X then approached MNO Bank and got an account opened with title XYZ Corporation. The account was only opened to realize the proceeds of a pay order issued by GHI Bank at the closure of account in the name of XYZ Corporation.

417. Mr. X had used different letter heads for opening the bank accounts and also different recruitment letters, which all appeared fictitious. The above activity occurred for six months and

Mr. X generated around PKR 600,000 (USD6000) by defrauding innocent job seekers. A blog was also found on the internet showing XYZ Corporation as being a "Job Scam". In the blog people complained about the advertisement and the trend through which job seekers have been defrauded. The intelligence has been shared with LEA for further investigation.

USA

OPEN SOURCE NEWS ITEM

Missouri man gets 14 years for al-Qaida support

By BILL DRAPER, Associated Press

Updated 7:30 pm, Monday, October 7, 2013

KANSAS CITY, Mo. (AP) — A Kansas City businessman who swore an oath of allegiance to al-Qaida and three years ago pleaded guilty to providing financial support to the international terror group was sentenced Monday to 14 years in prison, despite a plea from his attorney for lenience because of the risk he took by becoming an informant against the organization.

Khalid Ouazzani, 35, who pleaded guilty in May 2010 to bank fraud, money laundering and conspiracy to support a terrorist group, was sentenced in federal court in Kansas City.
Federal prosecutors claimed Ouazzani provided more than $23,000 to al-Qaida and had pledged more, with the hope of eventually traveling to the Middle East to join the fight against the U.S.

In his guilty plea, Ouazzani admitted making false claims to borrow money for a used auto parts business and wiring the proceeds to a bank in Dubai. That money was used to purchase an apartment in Dubai that later sold for a $17,000 profit, which was given to al-Qaida. Ouazzani also admitted sending the terror group $6,500 from the sale of his business.

Ouazzani, a married father of two who became a U.S. citizen in June 2006, admitted in his plea bargain to bank fraud, money laundering and conspiracy to support a terrorist group after admitting he gave money and swore an oath of allegiance to the terror network in 2008.

At Ouazzani's sentencing hearing Monday, his attorney, Robin Fowler, asked U.S. District Judge Howard Sachs for a five-year sentence — Ouazzani already has served roughly 42 months — because his cooperation with federal authorities had landed his two co-conspirators in jail. That makes him a snitch and a Muslim who provided support to al-Qaida, both of which puts his life behind bars in danger, Fowler said.

Assistant U.S. Attorney Brian Casey said the government recommended 15 years — sharply reduced from the roughly 30 years he could have gotten under sentencing guidelines — for supporting the terrorist group and committing bank fraud.

Sachs noted that the charge of supporting al-Qaida is a serious crime, and despite Ouazzani's cooperation in the separate case he needed to be adequately punished. "He did cooperate, as the judge stated, but that doesn't erase what he did," U.S. Attorney Tammy Dickinson said after the hearing. "A lot of damage, a lot of lives could have been lost with that $23,000."

Federal officials said last year that Ouazzani was part of a small terror cell with two New York men, Sabirhan Hasanoff and Wesam El-Hanafi, both of whom pleaded guilty in June 2012 to their roles in the conspiracy.

After he was arrested in February 2010 on 33 counts, Ouazzani waived his Miranda rights and told investigators about Hasanoff and El-Hanafi. When confronted by information Ouazzani provided, the

two New Yorkers pleaded guilty last year, Fowler said. Without his cooperation, both might still be involved with terrorism, he said.

Ouazzani, who wrote an eight-page letter to the judge apologizing for his actions, addressed the court before Sachs handed down the sentence.

"I make no excuses for the crimes I committed," he said. "I'm not proud of the mistakes I've made. I'm ashamed."

Ouazzani's contributions to al-Qaida went through Hasanoff, a Brooklyn accountant at PricewaterhouseCoopers who moved to Dubai in 2007, according to court documents. El-Hanafi, who accepted Ouazzani's oath of allegiance to al-Qaida, was an information security specialist in Brooklyn with Lehman Brothers before moving to Dubai around 2005.

The three met in Brooklyn in May 2008 to discuss membership in the terrorist organization, about a year after El-Hanafi had connected with two experienced terrorists in Yemen, court records show.

Those terrorists — referred to in court documents as "Suffian" and "The Doctor" — later told FBI agents after being arrested in Yemen that the Americans believed the money and equipment they sent were being set aside for their military training that eventually would land them in Somalia, Iraq or Afghanistan.

Instead, The Doctor admitted he and Suffian divided the material loot between themselves, gave some of the money to the families of Islamic martyrs and bought a few cars.

Though the Americans apparently were scammed out of tens of thousands of dollars, federal prosecutors said they still aspired "support violent extremist Islamic causes."

http://www.ctpost.com/news/crime/article/KC-man-to-be-sentenced-for-supporting-al-Qaida-4874591.php

5. USEFUL LINKS

Anti-Corruption Research Network

418. The Anti-Corruption Research Network (ACRN) is an online platform and the global meeting point for a research community that spans a wide range of disciplines and institutions. ACRN is a podium to present innovative findings and approaches in corruption / anti-corruption research, a sounding board to bounce off ideas and questions, a marketplace to announce jobs, events, courses and funding. The periodic spotlight section also looks at specific corruption issues and highlights key research insights and contributions on the selected topic.
http://corruptionresearchnetwork.org/

Basel Institute of Governance

419. The Basel Institute on Governance is an independent not-for-profit competence centre specialised in corruption prevention and public governance, corporate governance and compliance, anti-money laundering, criminal law enforcement and the recovery of stolen assets.
http://www.baselgovernance.org/

Center for Global Counterterrorism Cooperation (CGCC)

420. The CGCC is a non-profit, nonpartisan policy institute dedicated to strengthening international counterterrorism cooperation. It works to build stronger partnerships to prevent terrorism among many actors and across many levels:
- the United Nations, regional organizations, and states
- communities, police, and governments
- researchers, practitioners, and policymakers
- survivors of terrorism around the world

421. The CGCC builds these partnerships through collaborative research and policy analysis and by providing practical advice. CGCC develops innovative counterterrorism programming and training and assists key stakeholders to develop sustainable solutions to preventing terrorism. CGCC is working to improve intergovernmental cooperation at the global, regional, and sub-regional levels; support community-led efforts to counter violent extremism; ensure respect for human rights and the rule of law; and empower civil society and victims of terrorism to speak out. As transnational threats evolve, CGCC is also working to foster a new generation of holistic, rule of law-based responses to organized crime and other forms of transnational violence.
http://www.globalct.org

The Egmont Group

422. For FIU information and links to FIUs with websites.
http://www.egmontgroup.org/

Global Financial Integrity

423. Global Financial Integrity (GFI) promotes national and multilateral policies, safeguards, and agreements aimed at curtailing the cross-border flow of illegal money. In putting forward solutions, facilitating strategic partnerships, and conducting research, GFI is making efforts to curtail illicit financial flows and enhance global development and security.
http://www.gfintegrity.org/

FATF/ FATF-Style Regional Bodies
CFATF - Caribbean Financial Action Task Force (FSRB)
EAG - Eurasian Group (FSRB)
ESAAMLG - Eastern and South African Anti Money Laundering Group (FSRB)
FATF - Financial Action Task Force
GAFISUD - Grupo de Acción Financiera de Sudamérica (FSRB)
GIABA - Groupe Inter-Gouvernemental d'Action Contre le Blanchiment de l'Argent en Afrique (FSRB)
MENAFATF - Middle East and North Africa Financial Action Task Force (FSRB)
MONEYVAL - Council of Europe, Committee of Experts on the Evaluation of AML Measures and FT

Regional Organisations
ADB/OECD Anti-Corruption Initiative for Asia-Pacific
OCO - Oceania Customs Organisation (Secretariat)

International Organisations
Commonwealth Secretariat
IMF - International Monetary Fund
UNODC - United Nations Office on Drugs and Crime
UNODC-GPML - Global Programme on Money Laundering
WCO - World Customs Organization (English)
World Bank - AML/CFT

6. ACRONYMS

ADB - Asian Development Bank
AGD - Attorney General's Department
AML - Anti-Money Laundering
AMLD - Anti-Money Laundering Department
APG – Asia/Pacific Group on Money Laundering
ATM - Automatic Teller Machine
AUSTRAC - Australian Transaction Reports and Analysis Centre
CFT - Countering the Financing of Terrorism
CRA – Canada Revenue Agency
CTED - Counter Terrorism Executive Directorate
CTR - Cash Transaction Report
DNFBP - Designated Non-Financial Businesses and Professions
EAG – Eurasian Group
ECOWAS - Economic Community Of West African States
EDD - Enhanced Due Diligence
EFT - Electronic Funds Transfer
FATF - Financial Action Task Force
FEMA – Foreign Exchange Management Act (India)
FinCEN - Financial Crimes Enforcement Network
FINTRAC - Financial Transactions Reports Analysis Centre (Canada)
FIU - Financial Intelligence Unit
FMU – Financial Monitoring Unit (Pakistan)
FSRB – FATF-Style Regional Bodies
FTZ – Free Trade Zone
GIF – Financial Intelligence Office (Macao, China)
HOSSP - Hawala and Other Similar Service Provider
ICRG – International Cooperation Review Group
IFTI - International Funds Transaction Instruction
INTERPOL - International Criminal Police Organisation
INTRAC – Indonesian Financial Transaction Reports and Analysis Centre
LEA - Law Enforcement Agency
JIB - Investigation Bureau, Justice (Chinese Taipei)
ML - Money Laundering
MLA - Mutual Legal Assistance
MOU - Memorandum of Understanding
NGO – Non-Government Organisation
NPO – Non-Profit Organisations
PCA - Principal Customs Areas
PEP - Politically Exposed Person
RCMD - Royal Malaysian Customs Department
RCMP – Royal Canadian Mounted Police
SALW – Small Arms and Light Weapons
SAR – Suspicious Activity Report
SCTR - Significant Cash Transaction Report
SECP – Security Exchange Commission of Pakistan
STR - Suspicious Transactions Report
SUSTR - Suspicious Transactions Report
TBML - Trade Based Money Laundering

TCSP - Trust and Company Service Providers
TF - Terrorism Finance
UN - United Nations
UNSCR – United Nations Security Council Resolution
VAT - Value Added Tax
WG – Working Group