NUS National University of Singapore | Centre for Banking & Finance Law
Faculty of Law

ACAMS 12th Annual AML & Anti-Financial Crime Conference - APAC

Managing AML/CTF Risk in the era of Transformation
26th – 27th April 2021

Conference Report

Rishik Elias MENON
Research Associate
CBFL, NUS Law

[CBFL-Rep-2101]
June 2021

This report is based on the proceedings of the 12th Annual AML & Anti-Financial Crime Conference – APAC organised by the Association of Certified Anti-Money Laundering Specialists held virtually on the 26th – 27th April 2021. The views expressed in this report reflect the author's personal opinions and do not necessarily reflect the policies or views of the Centre for Banking & Finance Law.

This report may be cited as: RE Menon, *ACAMS 12th Annual AML & Anti-Financial Crime Conference – APAC: Managing AML/CTF Risk in the Era of Transformation*, Centre for Banking & Finance Law, Faculty of Law, National University of Singapore, June 2021, report number [CBFL-Rep-2101] [https://law.nus.edu.sg/cbfl/wp-content/uploads/sites/5/2021/08/CBFL-Rep-2101-RMENON-Jun.pdf]

Centre for Banking & Finance Law
Faculty of Law
National University of Singapore
Eu Tong Sen Building
469G Bukit Timah Road
Singapore 259776
Tel: (65) 6601 3878
Fax: (65) 6779 0979
Email: cbfl@nus.edu.sg

http://law.nus.edu.sg/cbfl/

The Centre for Banking & Finance Law (CBFL) at the Faculty of Law, National University of Singapore, focuses broadly on legal and regulatory issues relating to banking and financial services. It aims to produce research and host events of scholarly value to academics as well as of policy relevance to the banking and financial services community. In particular, CBFL seeks to engage local and international bankers, lawyers, regulators and academics in regular exchanges of ideas and knowledge so as to contribute towards the development of law and regulation in this area, as well as to promote a robust and stable financial sector in Singapore, the region and globally.

ACAMS 12th Annual AML & Anti-Financial Crime Conference – APAC: Managing AML/CTF Risk in the era of Transformation

Rishik Elias MENON

Abstract

The Association of Certified Anti-Money Laundering Specialists ("ACAMS") held their 12th Annual Anti-Money Laundering ("AML") & Anti-Financial Crime Conference - APAC, on the 26th and 27th of April 2021 (the "Conference"). Themed "*Managing AML/CTF Risk in the Era of Transformation*", the Conference was virtually attended by over 500 participants from over 25 countries. Through panel discussions, round table talks and presentations, the Conference covered a number of topics relating to current anti-money laundering/counter financing of terrorism ("AML/CFT") trends, recent developments and best practices for AML/compliance professionals in the Asia Pacific ("APAC") region.

This report is divided into two parts. Part I of the report provides a brief summary of the various talks, and panel discussions that occurred at the Conference. Part II consists of a reflective commentary on some of the broader themes and observations arising from the Conference, concerning AML laws, policies and regulations.

TABLE OF CONTENTS

PART I

The intention of Part I of this report is to present the reader with a high-level overview of the programme, and the key points made during the various presentations, talks and panel discussions. These takeaways are based on the author's personal observations from attending the Conference as a participant. Due to some of the sessions being concurrent or the videos of these sessions not being available, summaries of these sessions are not provided.

Conference Programme

Monday, 26 April 2021 – Day 1 of Conference	
09:00 – 09:15	**Welcome Remarks – Day 1** **Scott Liles** – President & Managing Director, ACAMS **Hue Dang** – Senior Asia Pacific Leader, ACAMS
09:15 – 09:45	**Keynote Address – Day 1** **Arthur Yuen** – Deputy Chief Executive, Hong Kong Monetary Authority ("HKMA")
09:45 – 11:15	**General Session 1** *Regulatory Update: Analysing Regional AML Trends and New Developments across APAC* **Moderator** **Rick McDonell** – Executive Director, ACAMS **Speakers** **Stewart McGlynn** – Division Head, AML, HKMA **Thomas Mathew** – Chief General Manager, Department of Regulation, Reserve Bank of India ("RBI") **Hiroshi Ozaki** – Director, AML/CFT Policy Office, Strategy Development and Management, Financial Services Agency (Japan) ("JFSA")
11:35 – 12:45	**General Session 2** *The Conduct Agenda- Responsibility & Accountability* **Moderator** Kieran Beer – Chief Analyst and Director of Editorial Content, ACAMS **Speakers** **Mel Georgie B Racela** – Executive Director, Anti-Money Laundering Council, the Philippines ("AMLCP") **Dylan Lee** – Managing Director & Country Chief Compliance Officer (Singapore) & Asean Cluster Compliance Coordinator, Citibank Singapore **Alba Lema** – CEO, SMC Compliance **Fairlen Ooi** – Head, Group AML, Oversea-Chinese Banking Corporation Limited

13:45 – 14:45	**Concurrent Session 3A** *COVID-19 & Post-COVID-19: Staying current with the 'new' Normal* **Moderator** **Aaron Lau** – Head of Fraud Investigation & AML, AITLAU Management Services **Speakers** **William Au Ieong** – Director and Vice President, Tai Fung Bank Limited **Akil Baldwin** – Regional Attaché, Homeland Security Investigations, U.S. Consulate General Hong Kong and Macau **Lisa Kelaart-Courtney** – Director, Prevention and Compliance Division, Office of Anticorruption and Integrity, Asian Development Bank	**Concurrent Session 3B** *Financial Institutions' Dilemma: Developing a Risk-based Approach to Financial Institutions' AML Processes* **Presenter** **Chua Choon Hong** – Head of Compliance Solutions – APAC, Bureau van Dijk
14:50 – 15:50	**Concurrent Session 4A** *Transaction Surveillance – New Techniques, New Tools* **Moderator** **Zubin Chichgar** – Head, Monitoring & Analytics, Standard Chartered Bank **Speakers** **Eric Ang** – Head, Automation, Analytics & Artificial Intelligence, Group Compliance, UOB **Rashmi Dubier** – Managing Director, Head of AML-Asia, MUFG APAC **Keith Swanson** – Director of Fraud, Financial Crimes and Security Intelligence, Asia Pacific-Japan, SAS Institute	**Concurrent Session 4B** *Development of the Risk Tolerance Statement* **Moderator** **Aub Chapman** – Director, Aub Chapman Consulting Services **Speakers** **Scott Burton** – Managing Director & Regional Head of Anti-Financial Crime, Asia Pacific, Deutsche Bank **Ravi Duvvuru** – President & Chief Compliance Officer, Jana Small Finance Bank Limited. **Anzar Mulyantoro** – Head of AML/CFT Advisory, PT Bank Mandiri (Persero) Tbk
16:20 – 17:20	**Concurrent Session 5A** *Sanctions Update - What the Financial Institutions ("FIs") now must do* **Moderator** **Dr. Justine Walker** – Head of Global Sanctions and Risk, ACAMS **Speakers** **Charles Delingpole** – Founder & CEO, ComplyAdvantage **David Cope** – Managing Director and Head of Financial Crime Compliance, Goldman Sachs (Singapore)	**Concurrent Session 5B** *Bringing Artificial Intelligence ("AI") to life in AML – Why it matters, and why you need it today* **Presenters** **Michael Barrett** – Head of AML Product, NICE Actimize **Matthew Field** – APAC Market Director, AML, NICE Actimize

17:20 – 17:30	**Wrap-Up and Key Takeaways – Day 1** **Rosalind Lazar** – Regional AML Director – APAC, ACAMS
Tuesday, 27 April 2021 – Day 2 of Conference	
09:00 – 09:10	**Welcome Remarks – Day 2** **Hue Dang** – Senior Asia Pacific Leader, ACAMS
09:10 – 09:40	**Keynote Address – Day 2** **Loo Siew Yee** – Assistant Managing Director of the Policy, Payments & Financial Crime Group, Monetary Authority of Singapore (“MAS”)
09:40 – 11:00	**General Session 6** *Driving Outcomes - An Executive Roundtable* **Moderator** **Hue Dang** – Senior Asia Pacific Leader, ACAMS **Speakers** **Grace Ho** – SEA Head for AML & Sanctions, JP Morgan Chase Bank N.A., Singapore Branch **Ahmad Solichin Lutfiyanto** – Compliance Director, PT Bank Rakyat Indonesia (Persero) Tbk (“BRI”) **Soma Sankara Prasad** – Deputy Managing Director and Group Compliance Officer, State Bank of India (“SBI”)
11:30 – 12:45	**General Session 7** *Non-Bank FIs and Designated Non-Financial Businesses and Professionals (“DNFBPs”) – How we are managing our money laundering/terrorism financing (“ML /TF”) Risk* **Moderator** **Martin Dilly** – Director, Martin Dilly AML **Speakers** **Chen Jee Meng** – Head Regulatory, Corporate & Financial Crime Compliance, AIA Singapore **Simon Young** – Group Head of Financial Crime Risk Management, and Chief Compliance Officer, Overseas, Ping An Group
13:45 – 14:45	**General Session 8** *Assessing the whole system response to tackling illegal wildlife trade (“IWT”) and environmental crime* **Moderator** **Dr. William Scott Grob** – CGSS, AML Director – Americas, ACAMS **Speakers** **Steven Galster** – Chairman, Freeland **Brian Gonzales** – Head of Protection of Endangered Species, WWF-Hong Kong

	Chinali Patel – Consul – International Illicit Finance Policy Lead, British Consulate-General Hong Kong	
14:50 – 15:50	**Concurrent Session 9A** *Financial Technology & Innovation* **Moderator** **Andrew Chow** – Head Regulatory Business Transformation APAC, Bank Julius Baer, Singapore **Speakers** **Praveen Jain** – Head Financial Crime Compliance, Surveillance Solutions and Innovation, Standard Chartered Bank **Radish Singh** – SEA Financial Crime Compliance Leader - Deloitte Forensic, Deloitte & Touche Financial Advisory Services **Greg Watson** – Chief Operating Officer, Napier	**Concurrent Session 9B** *Misuse of Legal Persons - Why are we (still) missing the Red Flags?* **Moderator** **Mabel Ha** – Senior Advisor AML/KYC APAC, Bank Julius Baer **Speakers** **Cynthia Cheong** – Co-General Manager, Internal Audit Department, SMBC **Qi Chew** – Head of AML/CFT Department, Bank of Singapore **Bahroze Kamdin** – Partner, Deloitte Haskins & Sells LLP
16:20 – 17:20	**General Session 10** *Lessons Learned: Review of Recent Enforcement Actions – Banks and Beyond the Banks* **Moderator** **Rosalind Lazar** – Regional AML Director – APAC, ACAMS **Speakers** **Dr. Dian Ediana Rae** – Head, Indonesian Financial Transaction Reports and Analysis Centre (“PPATK”) **Neil Jeans** – Principal, Initialism **Daisuke Nagafuchi** – Japan Head of Financial Crimes Compliance, Financial Crimes Office for Japan, MUFG Bank	
17:20 – 17:30	**Closing Remarks and Conference Takeaways** **Rosalind Lazar** – Regional AML Director – APAC, ACAMS	

Summary of Proceedings

Welcome Remarks

Scott Liles, ACAMS President & Managing Director, opened the Conference by inviting the participants to ponder the sub-themes of “*what’s new?*” and “*what’s next?*” in the world of AML compliance. While most AML policy has evolved incrementally in a piecemeal fashion, Mr Liles noted that major global events or scandals, such as the 1MDB scandal, [1] have the power of accelerating regulatory changes in the industry. In today's era of transformation, the AML industry faces several external pressures, which will undoubtedly lead to a number of changes to the demands and challenges which AML professionals will face: challenges such as the advancement of technological tools in the financial services industry, the increasing focus on previously peripheral illicit activities (such as IWT and human trafficking), and the impact of the COVID-19 pandemic on the banking & financial services sector.

Mr Liles encouraged the attendees, especially those in the compliance industry, to use the Conference as an opportunity to receive practical guidance and lessons, and to build peer networks of professional support with fellow compliance practitioners, especially in the face of these upcoming challenges and changes.

Ms Hue Dang, ACAMS VP & Global Head of Business Development, discussed the history of ACAMS in the APAC region over the last 12 years. Focusing on how key jurisdictions in the region have slowly been adopted as full members of the Financial Action Task Force ("FATF"), the varying fortunes of some Asian jurisdictions which had previously been black or grey-listed by the FATF, and the recent regulatory and legislative responses of various APAC countries which had passed key national AML laws and regulations, as a response to the FATF pressures.

One of the most important developments, according to Ms Hue Dang, was how the conversation around AML had shifted from the "why of AML" to the "how of AML". The next stage proposed by Ms Hue Dang would be for society to stop thinking of money as mere "money", but to start asking "where did this money came from?" Ms Hue Dang also highlighted the negative impact of money laundering on the global economy, citing a 2017 United Nations Office on Drugs and Crime report on estimated drug trafficking proceeds.

Both Ms Hue Dang and Mr Liles reiterated the mission of ACAMS to "end financial crime", and to provide training, networking opportunities, and thought leadership to the AML compliance sector.

Keynote Address – Day 1

Arthur Yuen, Deputy Chief Executive of the HKMA gave the Keynote Address for Day 1 of the Conference. Reflecting on how he had to give his address virtually rather than in person, as he did back at the 10th ACAMS APAC Conference in 2018, Mr Yuen commented that COVID-19 had major consequences not just to the way events

[1] It should be noted, that while a number of high-profile enforcement actions and sanctions were taken in light of the 1MDB scandal, existing literature does not suggest that any legislative or regulatory changes to AML regimes around the world.

and conferences were organised, but also to the way financial services had to be delivered.

Digital on-boarding and relationship management services by FIs are no longer "good to haves" but are necessary in the face of COVID-19's social distancing restrictions. At the same time, COVID-19 has opened up a multitude of opportunities for money launderers to abuse the financial system. [2] Nonetheless, though AML remains a key concern for regulators, Mr Yuen reminded the AML professionals present not to lose sight of the core mandate of central banks and banking supervisory bodies during this period: to protect consumers and businesses, and to mitigate the economic disruption caused by COVID-19.

Technological Innovation

The role of technology in allowing banks, customers, and regulators to overcome the challenges posed by COVID-19 has already been mentioned. At the same time, FIs have leveraged on artificial intelligence/machine learning ("AI/ML") technology and data analytics to raise red flags on networks of fraudulent accounts that sought to exploit the FI's move to digitalisation during the COVID-19 pandemic. There have also been high demand from FinTechs seeking to engage HKMA on potential use cases.

Public-Private Information Sharing

The Fraud and Money Laundering Intelligence Taskforce ("FMLIT"), which was formed in 2017, [3] is an example of a public-private information sharing project that has facilitated the improved sharing of information between the FIs and Hong Kong's law enforcement agencies, and resulted in the seizure of approximately HK$692m in illicit funds. In the last year, in particular, FMLIT was particularly useful to issue threat alerts relating to COVID-19 fraud, and to allow FIs to develop appropriate risk mitigation measures. Though not strictly AML related, the rise of these scams have had a significantly negative economic and social impact, diverting public resources away from fighting the pandemic in order to respond to these frauds which targeted hospitals, healthcare facilities, and other vulnerable individuals.

Risk-Based Approach

Speaking on how Hong Kong's banking sector had embraced the "risk-based approach", and was moving away from mere box ticking. Mr Yuen gave credit to the HKMA for encouraging banks to embrace this approach, and suggested that it was

[2] See FATF, 2020. *Covid-19-related money laundering and terrorist financing: Risk and policy response*. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf

[3] HKMA, 2017. *Fraud and Money Laundering Intelligence Taskforce launched*. Retrieved from https://www.hkma.gov.hk/eng/news-and-media/press-releases/2017/05/20170526-3/

due to the Risk-Based Approach, that limited resources could be better allocated to tending to highest risk alerts, while allowing the banking sector to remain flexible and ensure business continuity in the face of crises like the COVID-19 pandemic. Similarly, Mr Yuen warned against viewing the FATF Mutual Evaluation Reports from a static compliance-oriented perspective. Rather, HKMA considers the implementation of FATF's risk-based approach as something on-going. Mr Yuen also noted that HKMA was capable of doing more to promote the adoption of the risk-based approach in the wider region.

Mr Yuen concluded his address by identifying three priorities for the AML/CFT industry, for the era of transformation ahead: (1) enhancing adaptability; (2) leveraging on regulatory technology ("RegTech"); and (3) encouraging data sharing.

Enhancing Adaptability

Addressing the regulators and supervisory authorities in the audience, Mr Yuen emphasised the importance of supporting FIs in ensuring their business continuity plans, through flexible and adaptable regulations. While the onus is not on the regulators to predict the future, it is important to react quickly with guidelines that suggest how AML/CFT standards can be maintained, yet applied to yet unknown circumstances and situations.

Leveraging on RegTech

The adoption of technology, and the rapid digitalisation of the FIs during COVID-19, should also not be seen as the end goal, but rather the beginning of a journey. Once again, regulators and supervisory authorities were told to take the lead in enabling innovations and encouraging FIs to adopt RegTech for their AML/CFT systems. Speaking of some of HKMA's recent initiatives, such as its AML/CFT RegTech Forum held in December 2019, [4] and a Case Studies and Insights Paper which was published in January 2021, [5] Mr Yuen emphasised the importance of regulators workings together with different sized FIs, to understand the AML/CFT eco-system, and to identify pain points in the system.

Some specific examples of how RegTech might be used, include the use of AI/ML powered transaction monitoring and screening processes, data analytics, and non-traditional data elements such as the tracking of IP Addresses. For FIs to be effective adapting such technology, they would equally have to prioritise investing in human capital: both data specialists, as well as experienced AML/CFT specialists would be needed to manage and maintain such systems. In this regard, Mr Yuen suggested

[4] See HKMA, 2019. *HKMA AML/CFT RegTech Forum Record of Discussion*. Retrieved from https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20191223e1a1.pdf

[5] See HKMA, 2021. *AML/CFT Regtech: Case Studies and Insights*. Retrieved from https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf

ACAMS served an important role as training providers to develop and equip AML/CFT professionals with the right skills to work with the technologists in the field.

Encouraging Data Sharing

Echoing his earlier call to increase public-private information sharing, Mr Yuen spoke of HKMA's on-going efforts to increase the number of banks on the FMLIT platform, to increase the overall quantity of data stored, and captured through its system, and therefore the quality of the data analytics in preventing ML/TF as well as potential fraud, such as by detecting sleeper accounts before they are activated for criminal purposes.

Keynote Address – Day 2

Ms Loo Siew Yee, Assistant Managing Director (Policy, Payments & Financial Crime Group), MAS was the keynote speaker for day 2 of the Conference.

Milestones Achieved

Ms Loo noted the successes borne out of MAS' public-private partnership project, the AML/CFT Industry Partnership ("ACIP"), which was launched in 2017. [6] To date, ACIP has been responsible for disseminating best practices regarding AML/CFT focused data analytic methods, as well as the general identification and dissemination of information regarding key AML/CFT risks and trends to the larger banking industry, especially in the last year when new COVID-19 related criminal typologies emerged.

Another example of public-private collaboration in the AML/CFT sphere that has proved useful in increasing operational efficiencies was 'Project POET' (Production Orders: Electronic Transmission). [7] Through the electronic communication platform, the Singapore Police Force's Corporate Affairs Directors ("CAD") and the partner FIs are able to send and reply to production orders, saving up to 97% of time spent in the process of dealing with production orders, and freed up manpower resources in dealing with these orders. The utility of the Project POET platform during Singapore's COVID-19 lockdown, and how it enabled important financial crime investigations to continue, despite the CAD and the FIs having to work remotely.

[6] MAS, 2017. *CAD and MAS Partner Industry Stakeholders to Fight Financial Crimes*. Retrieved from https://www.mas.gov.sg/news/media-releases/2017/cad-and-mas-partner-industry-stakeholders-to-fight-financial-crimes

[7] Ministry of Home Affairs, 2019. *Institute of Singapore Chartered Accountants (ISCA) Forensics & Cybersecurity Conference - Speech by Mrs Josephine Teo, Minister for Manpower and Second Minister for Home Affairs.* Retrieved from https://www.mha.gov.sg/mediaroom/speeches/institute-of-singapore-chartered-accountants-isca-forensics-cybersecurity-conference---speech-by-mrs-josephine-teo-minister-for-manpower-and-second-minister-for-home-affairs/

The Anti-Scam Centre, a partnership between the Singapore Police Force and major banks started in June 2019,[8] was another public-private partnership which played an important role in identifying and preventing scams during the COVID-19 period. The Anti-Scam Centre was responsible for intercepting S$6m of illicit funds arising from a COVID-19 related scam in March 2020.

Another success of ACIP was the identification of shell companies and pass-through accounts using their data analytic tools, and then sharing of this information and method to identifying such accounts to the wider industry. CAD and MAS has also worked with key banks through ACIP, using a hub-and–spoke model of analytics, to conduct further investigations and analytic studies into the activities of suspicious accounts. These collaborative efforts have resulted in the successful seizure of S$69m, including the interception of S$19m in incoming funds that was blocked through the proactive identification of suspicious accounts and transfers.

The Road Ahead

The importance of data analytic tools in the fight against ML/TF was highlighted, and MAS' support for FIs to integrate these tools into their AML/CFT systems. As an example of AML/CFT compliance systems could become more effective and efficient, FIs could use dynamic and trigger-based assessment of customer risk profiles and suspicious transactions that incorporate behavioural analytics of customers and their transaction histories.

Besides the integration of data analytic tools, the incorporation of strong governance processes is necessary to ensure that these tools remain relevant and effective. Strong data governance frameworks would ensure that analytic tools are being fed the right type of data inputs, in order to generate results that are effective and scalable. Systematic reviews of whether the tools are achieving desired objectives and outcomes, and measuring the effectiveness of these tools are also part and parcel of good governance oversight of compliance technology.

The role of trained and skilled AML/CFT compliance professionals to manage and operate these data analytic tools and systems cannot be forgotten. To this end, capacity building organisations such as ACAMS remain relevant and aligned with Singapore's skills framework for training and developing individuals in the financial services industry.[9]

[8] Ministry of Home Affairs, 2019. *The Ultimate Survival Guide to Scams.* Retrieved from https://www.mha.gov.sg/home-team-news/story/detail/the-ultimate-survival-guide-to-scams/

[9] See SkillsFuture Singapore and Workforce Singapore, 2019. *IBF unveils Skills Framework for Financial Services that charts skills needed for finance professionals and financial institutions to stay ahead*. Retrieved from https://www.ssg-wsg.gov.sg/news-and-announcements/27_Sep_2019.html

Tricky Terrain to Navigate

A number of new developments which posed a high AML/CFT risk were then highlighted, as they demanded the increased attention and supervision of the banking sector, AML/CFT professionals, and also the regulators. The first key risk being identified was the Digital Payment Token ("DPT"), due to its ability to facilitate high-speed, anonymous and cross-border transactions. DPT service providers are currently regulated under the Payment Services Act[10] and MAS' in-house unit has been tasked with proactively monitoring and detecting suspicious and unlicensed networks of DPT transactions. FIs considering offering DPT services were encouraged to similarly adapt necessary AML/CFT measures to mitigate ML/TF risks.

The Variable Capital Company ("VCC"), a new form of legal personhood created by the Variable Capital Company Act[11] in January 2020, also poses a new number of AML/CFT risks. MAS continues to monitor the situation closely, and would be scrutinising the kind of AML/CFT controls conducted by FIs dealing with VCCs.

Information sharing between banks remains an important tool in the fight against ML/TF, and criminals continue to exploit the lack of information sharing in their money laundering efforts. While the United Kingdom[12] and the United States[13] already have legal frameworks to facilitate this sharing of information between banks, Singapore is still considering the most appropriate way to implement such a framework, given Singapore's local banking demands and requirements.

Balancing AML with Social Outcomes

AML risk mitigation, however, always had to be balanced out against social objectives and wider policy goals, such as that of financial inclusion. Banks accounts serve vital functions of allowing individuals to pay bills, receive salaries, and even government pay-outs. Banks were reminded to not be overzealous in excluding former criminals, or individuals tainted by adverse media reports. Risk treatment strategies should be deliberate and targeted, to allow individuals to maintain bank accounts while risks of ML/TF be mitigated.

Acknowledging that the business case for allowing such accounts may be low, financial inclusion nonetheless remains a key social objective of the Singapore government. MAS is currently in the process of working with several banks in Singapore to create limited purpose bank accounts for high-risk individuals, which

[10] Payment Services Act 2019, No. 2 of 2019

[11] Variable Capital Companies Act 2018, No. 44 of 2018

[12] See Financial Conduct Authority, 2015. *Anti-money laundering taskforce* unveiled. Retrieved from https://www.gov.uk/government/news/anti-money-laundering-taskforce-unveiled

[13] See FinCen, 2020. *USA Patriot Act, Section 314(b) Fact Sheet*. Retrieved from https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf

would allow them to continue to transact for daily needs, and with white-listed accounts (such as for receiving their salaries or government pay-outs).

General Session 1: *Regulatory Update: Analysing Regional AML Trends and New Developments across APAC*

The first general session of the Conference, included regulators from three major jurisdictions in the APAC region: Thomas Mathew, Chief General Manager (Department of Regulation), RBI; Hiroshi Ozaki, Director (AML/CFT Policy Office), JFSA; and Stewart McGlynn, Division Head (Anti-Money Laundering), HKMA. The session was moderated by Rick McDonell, Executive Director of ACAMS and former Executive Secretary of the FATF.

COVID-19 and Digitalisation

The move towards online on-boarding in the last year due to COVID-19 was an experience that was broadly shared by the major jurisdictions. The number of accounts opened through online on-boarding in Hong Kong grew from about 18,000 in 2019 to 540,000 in 2020. Indeed, while online on-boarding was viewed in the industry as having a higher AML risk in the past, today it is recognised as a necessity.

The maintenance of a national digital identity database (the "Aadhaar" system[14]) in India has also facilitated online on-boarding for FIs, through its role in verifying identities in the know-your-client/customer ("KYC") process. The e-verification of identities through the Unique Identification Authority of India ("UIDAI") is arguably more reliable than verifying identities through physical forms and documents which were easier to forge.

JFSA had also allowed for a certain degree of KYC to be conducted off-site, leveraging on facial recognition technology, geo-tagging technology, and video liveliness checks. In many instances, however, the greater AML/CFT risk came *after* on-boarding, and a higher priority has to be placed on monitoring the on-going transactions of customers. The ability of sophisticated criminals to overcome these technological checks should not be underestimated.

FATF and the Risk-Based Approach

All three regulators spoke of their efforts to engage the FIs, and the role of regulators in issuing guidance papers to help their banks meet FATF's minimum standards. The in-built flexibility of the FATF's risk-based approach was also acknowledged as being particularly useful to FIs faced with increased COVID-19 restrictions.

[14] Unique Identification Authority of India, 2010. *Press Brief for National launch of Unique Identification Numbers (Aadhaar)*. Retrieved from https://uidai.gov.in/images/pressrelease/Press_note_for_launch_final.doc

It was noted that the Japanese financial sector, and even the JFSA themselves, were still adjusting from the shift from the rule-based approach to the risk-based approach. As regulators, JFSA had issued new guidelines in February 2018, and updated guidelines and FAQs in February 2021 to support the major banks with this change.

New ML/TF Typologies and Encouraging Technology

When asked about new ML/TF typologies, the regulators were in broad agreement that there were no radically new typologies to look out for. But while typologies remained the same, with the right use of technology, FIs could fine-tune their ability to screen higher risk customers and detect higher risk transactions. The rise in scams targeting financially illiterate and vulnerable segments of society was also mentioned.

The HKMA's has published various guidance papers[15] that provide case studies for FIs to learn from, on how to best optimize their existing technology, tap on existing public data and shared data, to improve their transaction monitoring systems, and to move away from the low-quality rule-based alert systems which typically generated large amounts of white noise and false positives.

JFSA has also been developing a proof-of-concept AML/CFT transaction monitoring technology that could be freely adopted by Japanese banks. This proposal was particularly intended to assist smaller FIs and financial services intermediaries who lacked the manpower, technology, or resources to invest in or implement large-scale AML/CFT systems internally.

Financial Inclusion

Given that India's "Aadhaar" system was voluntary, one participant queried if financial inclusion was a problem, especially for individuals who were not registered with the UIDAI. Mr Mathew responded that 90% of the Indian population had already been registered with the UIDAI, but even for those individuals who were not registered, RBI had been encouraging banks and FIs to allow the opening of "Small Accounts". [16] Such accounts with restricted use and high limits on transaction limits allowed banks to manage their risk, while allowing individuals without sufficient proof of identity to remain banked for daily needs. However, such accounts should only remain open for no more than a year, giving individuals sufficient time to get an Aadhaar number, and to eventually complete their KYC with the banks. The FATF

[15] See HKMA, 2021. *AML/CFT Regtech: Case Studies and Insights*. Retrieved from https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf

[16] RBI, 2013. *Financial Inclusion- Access to Banking Services – Basic Savings Bank Deposit Account (BSBDA) – FAQs*. Retrieved from https://rbidocs.rbi.org.in/rdocs/notification/PDFs/BSBC52_11092013.pdf

does recognise the issue of "financial exclusion", and this policy objective does remain a valid consideration for FIs to weigh in their balance of risks. [17]

FATF Travel Rule and Crypto-Currencies

Different regulatory bodies viewed risks posed by virtual asset service providers ("VASPs") and crypto-currencies differently. HKMA, for instance, valued early engagement through FinTech chatrooms and supervisory sandboxes. Mr McGlynn noted that most FinTechs dealing in the space of virtual assets and crypto-currencies wanted to be supervised and HKMA encouraged such early stage engagement.

While FIs were initially banned by RBI from dealing with crypto-assets, this had since been overruled by the Supreme Court of India.[18] The RBI is now in the process of finalising a new set of policies and regulations to deal with crypto-assets and VASPs. While the RBI noted that block-chain based crypto-assets were at least traceable and immutable, regulators still had their concerns of ML/TF risks; especially in relation to accessing, controlling, or conducting real-time monitoring of the respective block-chains, and with the additional problem of anonymity behind the crypto-wallets.

All three regulators agreed that the FATF Travel Rule (i.e. Recommendation 16 of the FATF Recommendations) was the most important AML/CFT regulation for Virtual Asset Service Providers and FinTechs to be familiar with.

Public-Private Partnership

All three regulators talked broadly about the various meetings held between themselves and the respective banking associations of their jurisdictions, and the importance of such dialogue in ensuring compliance for FATF country evaluations, building the right type of compliance culture, and encouraging information sharing.

During the Q&A, one participant pointed out that information sharing was usually one-sided, in that banks shared information with the financial intelligence units ("FIUs") and the supervisory bodies, but banks never receive feedback as to *which* of their STRs actually result in the arrest of an actual financial criminal, as opposed to simply being a suspicious transaction. Such feedback, the participant noted, would certainly be of help to banks, who could then use their AI/ML technology and data analytics to fine-tune their ability to catch similar money launderers.

[17] See FATF, 2013. *FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion*. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf

[18] *Internet and Mobile Association of India v Reserve Bank of India* [2018], 2020 SCC OnLine SC 275. Retrieved from https://main.sci.gov.in/supremecourt/2018/19230/19230_2018_4_1501_21151_Judgement_04-Mar-2020.pdf

General Session 2: *The Conduct Agenda- Responsibility & Accountability*

The presenters for the second general session comprised Dylan Lee, Managing Director & Country Chief Compliance Officer (Singapore), Citibank Singapore; Ms Alba Lema, CEO, SMC Compliance; Mel Georgie B Racela, Executive Director (AMLC Secretariat), AMLCP; and Ms Fairlen Ooi, Head (Group AML), Oversea-Chinese Banking Corporation Limited. The four presenters gave separate presentations on the topics of corporate culture, responsibility and accountability. The session was moderated by Kieran Beer, Chief Analyst and Director of Editorial Content, ACAMS.

Risk Culture from Perspective of the FIU

Mr Racela presented the regulator's perspective of risk cultures across various regulated entities in the Philippines, by categorising them into two archetypes: the "cooperative" and "uncooperative" entity. Cooperative entities were receptive towards AML/CFT objectives, and engaged regulators on new regulations, whereas uncooperative entities viewed AML/CFT regulations as being counterproductive to business, and typically resisted any new implementations by the regulators.

The AMLCP used a "carrot and stick" approach of punishing and sanctioning uncooperative entities, and rewarding cooperative entities by further engaging them in public-private partnership programmes ("4P Programmes"). The 4P Programmes included training, sharing of best practices and AML/CFT typologies, and sharing information to help target particular predicate crimes. As an example of the success of this approach, the number of STRs filed, specifically for the purpose of identifying transactions relating to the production of child sexual exploitation material increased 1,350%, and the identification of suspects and persons-of-interest increased seven-fold.

Corporate Governance is Key

Ms Ooi's presentation focused on the important role of corporate governance and organisational structure in creating a good AML risk culture. Good risk culture is characterised by having a clearly documented and identified risk appetite, having adequate risk mitigation strategies, and having clearly communicated these to the entire organisation. Structures support the implementation of good AML/CFT programmes, and structures are key to defining roles and responsibilities in an organisation's AML/CFT programme. Defining exactly which persons in the organisational chart have specific oversight and responsibility over AML/CFT controls is what sets apart a good risk culture in practice from one in theory.

Senior Manager's Regime

Mr Lee spoke of the rise of senior manager's regimes across various jurisdictions, such as the UK, [19] Australia, [20] Hong Kong, [21] and Singapore, [22] and noted its importance in inculcating a strong compliance culture amongst regulated entities. Without a way of properly identifying particular individuals who were responsible, whether through clear organisation charts or ladders, "collective responsibility" had the danger of simply being "no one's responsibility".

The immediate benefit of such regimes were that those at the top, whether the Board or the duly appointed senior managers, would be incentivised to create the right risk culture throughout their organisations, as well as communicate this culture all the way down to the first line of defence, i.e. the business lines. In turn, business lines needed to own and manage risks, as well as make risk decisions with a proper understanding of the organisation's risk appetite. The best way to get individuals in the organisation to behave properly and in accordance with the organisation's AML framework, however, is simply to compensate them appropriately.

Whistle-blower Policies

Ms Lema spoke on best practices for whistle-blower reporting channels, and the importance of such channels within organisations to promote a culture of individual responsibility for senior managers. Using case studies of whistle blowers from prominent FIs such as Barclays Banks, Wells Fargo and JP Morgan, Ms Lema observed that oftentimes the whistle-blowers failed to receive sufficient protection or compensation from the regulators following their falling-out with their banks, while senior managers of these FIs received relatively light sanctions. There was thus a need for regulators to take whistle-blower protection more seriously, by adopting important safeguards such as anonymity.

The presentation then highlighted necessary features for a good whistle-blower reporting channel. Firstly, that employees are informed and sufficiently trained to understand their organisation's whistle-blower policy. Another key element is that such whistle-blower protocols have to be regularly measured for its effectiveness, and reviewed periodically to ensure its functionality.

[19] See Financial Conduct Authority, 2014. *CP14/13: Strengthening accountability in banking: a new regulatory framework for individuals*. Retrieved from https://www.fca.org.uk/publications/consultation-papers/cp14-13-strengthening-accountability-banking-new-regulatory

[20] See Australian Prudential Regulation Authority, 2018. *Information Paper: Implementing the Banking Executive Accountability Regime*. Retrieved from https://www.apra.gov.au/sites/default/files/information_paper_implementing_the_bear.pdf

[21] See Securities and Futures Commission (Hong Kong), 2016. *Circular to Licensed Corporations Regarding Measures for Augmenting the Accountability of Senior Management*. Retrieved from https://apps.sfc.hk/edistributionWeb/api/circular/openFile?lang=EN&refNo=16EC68

[22] See MAS, 2020. *Guidelines on Individual Accountability and Conduct*. Retrieved from https://www.mas.gov.sg/-/media/MAS/MPI/Guidelines/Guidelines-on-Individual-Accountability-and-Conduct.pdf

Concurrent Session 5B: ***Bringing AI to life in AML – Why it matters, and why you need it today***

This session was conducted by one of the Conference's "Knowledge Session Sponsor", NICE Actimize, and presented by NICE Actimize's Head of AML Product, Michael Barrett, and their APAC Market Director (AML), Matthew Field**.**

The presentation began with a brief overview of the financial regulatory landscape across APAC, and the general perspective of how key regulators and FIUs such as MAS, HKMA, JFSA and Australian Transaction Reports and Analysis Centre ("AUSTRAC") viewed AI/ML technology and data analytics. The general consensus being that AI/ML and data analytics were important tools for FIs to adopt into their AML/CFT systems, whether for the purposes of sanctions screening, or transaction monitoring.

The general benefits of AI have been proven and acknowledged in reducing the number of manual alerts, false positives, and increasing higher value alerts for compliance officers. Tapping onto larger data lakes, and publicly available or shared data pools also allows AI to perform more innovative functions, such as processing "free form data" at the on-boarding stage, and finding previously hidden relationships between customers and clients which might impact their risk profile.

General Session 6: ***Driving Outcomes - An Executive Roundtable***

The executive roundtable, featured three senior managers from FIs in the APAC region, Ms Grace Ho, Executive Director and SEA Head for AML & Sanctions, JP Morgan Chase Bank; Ahmad Solichin Lutfiyanto, Compliance Director, BRI; and Soma Sankara Prasad, Deputy Managing Director and Group Compliance Officer, SBI. The roundtable was moderated by Ms Hue Dang, ACAMS VP & Global Head of Business Development.

FATF Mutual Evaluations

The upcoming FATF mutual evaluation exercises in India and Indonesia was mentioned as having an immediate effect on SBI and BRI. As SBI is the largest bank in India, and BRI is the second largest bank in Indonesia, both speakers confirmed that their respective supervising authorities and regulators have been working closely with their respective banks for at least the last year and a half, to prepare for upcoming 2021 evaluation. The stakes are especially high for Indonesia, the last remaining G20 country due to become a full FATF member after this year's mutual evaluation.

It was suggested that the FATF mutual evaluations are more effective than even UN sanctions in catalysing a country into adopting AML regulations. Pakistan and Mauritius are examples of two countries, formerly grey-listed by the FATF, who have since rectified and adopted increasingly robust AML regimes.

Risk-Based Approach & Financial Inclusion

The role of compliance officers was noted as being especially important in a risk-based system. Compliance officers need to be holistic in understanding various ML/TF risks, as well as appreciating their bank's business needs, and even larger social objectives such as financial inclusion. Compliance officers also have a key role of assessing risks, and communicating these assessments to the front "business line" in banks.

On the topic of financial inclusion, India was noted for already achieving financial inclusion rates of close to 90%. The RBI had further set financial inclusion targets for banks to meet, and were specifically promoting "small accounts" to encourage previously unbanked individuals to open accounts. What sets these accounts apart is their limited KYC requirement, which caters to low-income individuals and those living in remote villages, without the full set of documentation required for a full KYC. These accounts are also limited in their capacity to transfer or hold money, mitigating any risks that these could be exploited for money laundering. From a social policy perspective, it is important that financial inclusion through these small accounts allows the Indian government to make direct benefit transfers to individuals, and which is arguably more beneficial to citizens than indirect subsidy programmes. These direct benefit transfers have been especially important in the last year, when the Indian government made a number of COVID-19 related benefit transfers to vulnerable populations.

It was observed that implementing the risk-based approach in countries such as India and Indonesia can be especially challenging, due to the large numbers of customers (in the millions) and the diversity of each customer's profile. BRI's approach so far has been to adopt a hybrid-banking model, composed of digital banking and physical branch banking, to cater to the different customer profiles, needs, and AML risks, while being as inclusive as possible. Nonetheless, BRI intends to play a role in bringing up Indonesia's financial inclusion rates from around 76% to 90%.

Hybrid-Banking

All three speakers spoke of the need for traditional banks to adopt new technologies, and the rising trend of digitalisation. BRI's "hybrid" banking model and use of mobile banking has allowed BRI to tap not just micro-financing borrowers, but also ultra-micro-financing clients. This approach has helped BRI become Southeast Asia's (and possible the world's) largest micro-financing bank.

Similar to BRI, almost 90% of SBI's transactions were now taking place digitally. However, there would always be some customers who prefer to bank in physical branches, and thus the need for banks to maintain a "Phy-gital [*sic*] model".

In Singapore, MAS had recently granted specific digital bank licences to particular banks and FinTechs. While supportive of the move to digitalisation, it was important that AML/CFT requirements of such digital banks remained level with traditional banks. The challenge for traditional banks, which are typically encumbered by their large size, bureaucracy, and legacy IT systems, is to be faster, more nimble, and reactive, while maintaining their safety, structure and reliability, in order to compete with digital banks and FinTechs.

To illustrate the challenges traditional banks face in balancing these demands, Ms Ho gave the example of real time payment processes and account validation services. On the one hand, consumer expectations for transaction speeds have gone up, fuelled by a number of FinTech remittance service providers; on the other hand, ML/TF controls need to remain in place, often to the detriment of transaction speed. Ultimately, a balance between speed and security can be in found with the right technology and operational processes.

Technological Tools to Manage Financial Crime Risks

Most banks were using AI/ML to cope with the increased ML/TF risks that comes with increased digitalisation. The best way to utilise these technologies would be to implement the FATF's risk-based approach, and calibrate the kind of due diligence and ML/TF controls put in place to suit the respective risk-levels of customers, products, and organisational risk appetite.

Digitalisation also carried an attendant risk of fraud, though this could be mitigated through technology. BRI had adopted AI technology as part of its fraud-prevention mechanisms. Both SBI and BRI have also adopted identity verification, anti-fraud liveliness tests, and facial recognition technology for their video KYC processes. The FATF has also issued very useful guidance to banks on the adoption of facial recognition technology for video-KYC processes. However, it was noted that technology could only go so far, and financial literacy and fraud awareness had to improve to protect vulnerable populations, such as senior citizens, who were prone to giving out their passwords to fraudsters.

Outsourcing Risks

Besides banks' own in-house technological capabilities, banks have also been increasingly relying on third-party service providers and technology provided by FinTechs to assist in their AML/CFT transaction monitoring processes. However, it should be noted that outsourcing brings along risks to a bank's business continuity. Before engaging such technology, FIs should ensure that the software being provided can be sufficiently scalable to suit the high number of customers and transactions managed by traditional banks.

Outsourcing service providers are also increasingly being regulated and required to meet minimum service standards. This second issue is increasingly one of national significance as financial systems are now viewed as the main targets for cyber-warfare, and governments are keen to shore up their cyber-defences of their national banking institutions. Vulnerable outsourced service providers thus represent a chink in this national cyber-armour.

Manpower Development and Compliance Culture

Besides these technological adoptions, the up-skilling and training of staff was equally important to manage these risks of financial crimes, and this effort had been undertaken thus far through online trainings during the pandemic. While online sessions allowed banks to train larger numbers of their staff simultaneously, there were doubts as to the effectiveness of inculcating a compliance culture without regular face-to-face interactions.

SBI has also been increasing its use of incentives and disincentives to encourage staff to stay updated, and receive certain compulsory AML/CFT certifications. These drives were necessary to keep staff up to date amidst constant regulatory, and also due to the upcoming FATF mutual evaluations and audits due to occur this year.

Digital Infrastructure

An important aspect of BRI's hybrid-banking model was the building up of its digital eco-system to support its various digital products and services. On the flip side, particular banks in India, such as HDFC Bank, were being sanctioned by the RBI and prohibited from launching any further digital products, due to not having properly managed digital infrastructure which was prone to technical faults and glitches and which could not cope with the customer demands and expectations.

JP Morgan, on the other hand, demonstrated the various cost savings an FI might enjoy through the embrace of digital infrastructure. A number of innovative digital projects embarked on by JPMorgan, such as the use of the blockchain technology through the Interbank Information Network for payment processes, have allowed the bank to save money on "pre-validation", whereas rejecting a transaction subsequently would be costlier for the bank.

Besides the importance of a bank's own digital infrastructure, a strong national digital infrastructure also has the potential to facilitate digitalisation, financial inclusion and even provide opportunities to feed key data to banks for the AML/CFT processes. Besides the example of having a national digital identity registry to facilitate e-KYC verification, such national digital identity registries could potentially even pave the way for international cross-border identity verification. A national financial data exchange platform would also be a highly facilitative national digital infrastructure, that would allow FIs to corroborate sources of wealth for on-boarding individuals. The use of a national block-chain system to allow major banks to clear and settle multi-currency payments, such as Project Ubin[23] run by MAS, was another example of potential cost-savings that could be shared by the industry through national-level investment.

General Session 7: *Non-Bank FIs and DNFBPs – How we are managing our ML /TF Risk*

Martin Dilly, Director of Martin Dilly AML moderated a panel discussion on the DNFBP perspective on AML/CFT regulations featuring Chen Jee Meng, Head (Regulatory, Corporate & Financial Crime Compliance), AIA Singapore, and Simon Young, Group Head of Financial Crime Risk Management and Chief Compliance Officer, Overseas, Ping An Group. A third speaker from the casino sector had to pull out of the Conference.

Mr Dilly outlined the general challenges faced by DNFBPs in implementing AML/CFT systems, and having to interpret regulations and guidelines that have been written with banks in mind. Another challenge faced by non-Bank FIs and DNFBPs was that they were generally smaller, and thus lacked in-house AML or compliance departments. This raised the question as to whether AML/CFT regulations were unduly costly for DNFBPs, though Mr Young and Mr Chen both acknowledged that to have different regulatory requirements for DNFBPs would be to create a loophole for money launderers to exploit.

From the perspective of Ping An Group, within which comprises a number of diverse businesses including financial and non-financial services, Mr Young noted that the compliance department of his group leveraged on AI/ML, data analytics and a strong technological infrastructure to conduct its KYC and CDD processes at a group level, even for sectors and businesses where AML/CFT controls were not required by regulators. The benefit of this approach allowed Ping An group to understand not just its customers and their sources of wealth, but also non-customers and entities they interacted with. It was noted that even some FIs were not at this stage of coordination, and various departments and divisions within banks (e.g. credit cards, investment banking, retail banking, etc.) acted in silos and conducted CDD and KYC through their own unique processes.

[23] MAS, 2020. *Project Ubin Phase 5: Enabling Broad Ecosystem Opportunities*. Retrieved from https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Project-Ubin-Phase-5-Enabling-Broad-Ecosystem-Opportunities.pdf?la=en&hash=91091CAD39265C03FF7A4253E70FBEE6D1177714

Though obtaining a “single customer view” might be beneficial, it is challenging for various reasons, such as legacy technological infrastructure, or for ethical reasons where DNFBPs may avoid an internal conflict of interest by adopting “ethical walls”. Furthermore, there is value in customising the AML/CFT measures for each unique product offered by a DNFBP. Applying a rule-based approach to different sectors, products, and geographies should also be avoided.

Despite the intuitive instinct of most DNFBPs or unregulated institutions to “keep their head down” and avoid drawing attention that might lead to regulation, Mr Chen noted that starting conversations with regulators often allow organisations to enjoy a first-mover advantage over their peers, especially when in a greenfield industry. Regulators, such as MAS and HKMA are always keen to dialogue with new industries and typically allow supervisory sandboxes when engaged.

General Session 8: ***Assessing the whole system response to tackling illegal wildlife trade and environmental crime***

Moderated by Dr William Scott Grob, AML Director (Americas), ACAMS, the session included presentations from Steven Galster, Chairman, Freeland; Brian Gonzales, Head of Protection of Endangered Species, WWF-Hong Kong; and Ms Chinali Patel, Consul (International Illicit Finance Policy Lead), British Consulate-General Hong Kong.

Mr Gonzales provided the audience with an overview of reports and resources published by governments and international non-governmental organisations (“NGO”) concerning IWT in general, and the role of financial institutions in fighting IWT in particular. Ms Patel spoke on the importance of public-private partnership as a tool to combat IWT, and in particular, the “4 Ps” of “pursue, prevent, protect, and prepare”. These “4 Ps”, according to Ms Patel, originated in the UK’s counter terrorism unit when it was seeking to formulate a whole system response to terrorism. The same principle of working with stakeholders across various sectors have since been applied in addressing various threats, from money laundering, to fraud, to human trafficking, and now, to IWT.

Pursuing wildlife traffickers begins with sharing information between key organisations, like the WWF, law enforcement agencies, and financial institutions. This often requires strong legislation to allow such investigation in the first place, so as to build the necessary evidence against the traffickers. Prevention, in the context of IWT, has to do with reducing the demand for wildlife produce, as well as helping those involved in IWT find legitimate means of earning a livelihood and contributing to the economy. The most important two pillars, to protect and prepare, involve increasing awareness about IWT, and include the work of NGOs, WWF, FATF, ACAMS and other bodies in sharing IWT-related ML typologies in order to equip

AML compliance professionals with the knowledge to identify and detect IWT-related transactions.

Mr Galster presented a case study of a successful seizure of about US$11m in illicit funds connected with an IWT syndicate in Thailand known as “Hydra”, which was the fruit of collaboration between Thailand’s FIU and Freeland, an NGO focused on fighting IWT and human trafficking. Some of the key trends and features of IWT, Mr Galster noted, included the source of funds being China and Southeast Asia, and the final destination of funds being Africa. The majority of illegal animal parts and hardwoods were also being shipped by sea freight, rather than by air, implicating the key ports on both the East and West coasts of Africa. Another key feature of the entities dealing with IWT was that they typically masked their illegal trade with “legal animal-related businesses”, such as private zoos, un-opened zoos, tour companies, and even explicitly animal-related transport companies.

Freeland was also involved in organising various roundtables and bringing together law enforcement agencies across Asia and Africa. These meetings were highly productive in creating and sharing intelligence that led to the eventual capture and disruption of major organised crime syndicates dealing in IWT. It appeared that FIUs were not engaged earlier in the process, and in hindsight it was noted how useful the FIUs have been in generating evidence and in building a stronger case for prosecution.

Looking to the future, it is likely that legislators and regulators around the world would be making IWT a priority area, together with drug trafficking, terrorism financing and human trafficking. AML compliance departments who fail to identify IWT typologies are thus likely to face increased sanctions in the future. Discussions are also taking place among NGOs to lobby ASEAN into setting up a wildlife repatriation fund, wherein a portion of IWT-related funds seizure would have to be re-invested into conservation efforts.

COVID-19 has had an impact on IWT. Firstly, trade to China (and especially wildlife trade) had slowed down, potentially due to the wildlife-based theories surrounding the origins of COVID-19. While shipping routes remain open, the drop in demand has led traffickers to hoard and store their trafficked goods like futures commodities, waiting for the demand to pick up again.

It was also noted that crypto-currencies are not being used by IWT, given the instability in the value of cryptos, though other commodities like gold are sometimes used.

In a concluding call to action, the three speakers noted the important role played by FIUs, the financial sector, and the shipping sector in helping to identify IWT related typologies and red flags, and encouraged an increase in general awareness which would help identify similar cases. In particular, they encouraged the AML compliance professionals at the Conference to take courses such as the free ACAMS-WWF Illegal Wildlife Trade Certificate course.

Concurrent Session 9A: *Financial Technology & Innovation*

This session was moderated by Andrew Chow, Head Regulatory Business Transformation APAC, Bank Julius Baer. The speakers included, Praveen Jain, Managing Director and Head Financial Crime Compliance, Surveillance Solutions and Innovation, Standard Chartered Bank; Ms Radish Singh, Partner, SEA Financial Crime Compliance Leader, Deloitte & Touche Financial Advisory Services; and Greg Watson, Chief Operating Officer, Napier.

Banks Engaging FinTech

The first major trend noted was that banks were more willing to work with FinTechs (defined broadly as providers of financial technology software) today, than they were 5-6 years ago. This co-operation did not always mean partnering with FinTechs, and sometimes took the form of FIs acquiring smaller FinTechs, or simply starting their own in-house R&D incubators. Regardless of the form, it was a recognition of a need by traditional banks to be innovative and flexible in their technology solutions, as well a recognition of the limitations of some of their legacy technological frameworks.

It was also acknowledged that there was no single technological solution in the drive towards optimisation, and that sometimes it could take the form of automation technology, AI/ML, or blockchain technology, depending on the organisational and business needs or technological pain points to be addressed. Given the diversity of issues faced by banks, and their differing needs, the approach taken in engaging FinTechs could also be varied. While some banks could consider engaging multiple partners or FinTech providers, thereby diversifying their risk, some would prefer working with a single FinTech provider in co-creating a customised technological solution to meet or even replace the bank's legacy technological eco-system.

Given the oversaturation of players in the market at the moment, it was also forecasted that the numbers of RegTechs and FinTechs in the industry are likely to fall, and the players are likely to consolidate in the near future. It was also noted that there was a large number of FinTechs with great expertise in technology, but few with the requisite domain knowledge to truly understand the needs of banks.

Digital Banks

It was noted that the rise of digital banks and the journey towards digitalisation began more than 5 years ago, first with digital on-boarding, and now with digital transactions and an increasing number of digital products. The regulatory requirements of digital banking means that special attention should go into designing these banks' AML/CFT systems. New players in the industry, especially, might find implementing a rigorous AML/CFT system more challenging than traditional banks, given their lack of historic client data; data being the key ingredient for most AI/ML based KYC and suspicious transaction monitoring systems.

One of the benefits of being a digital bank, which all three speakers noted, was the opportunity to start afresh in terms of its technological infrastructure, and the management of its "data lake". While traditional banks are often forced to stitch together existing silos of data from different originating sources to create a useable data lake, new digital banks starting with a clean slate have a chance to create a single customer view on data across all their products, which traditional banks sometimes find challenging.

Payment Systems and Blockchain Technology

Payment services typically pose high ML/TF risks due to their high speeds. While major players, like Stripe and Revolut, have brought huge benefits to consumers, allowing them to move money quickly with low fees, regulators need to ensure that these payment service providers don't become a "weak link" in the overall fabric of the financial system, by ensuring that their ML/TF risks are properly mitigated and meet the same minimum AML/CFT standards as traditional FIs.

Traditional FIs also need to consider the nesting risks posed when payment service providers seek to open accounts with traditional FIs. In order to properly assess the ML/TF risk profiles of such payment service providers, traditional FIs would need to understand, not just the business model, but also the KYC, transaction monitoring and CDD controls put in place by the payment service providers. When such payment service providers are still small and are operating like a start up, they are even more likely to keep evolving their product, and correspondingly, their risk profiles would also keep changing. The same challenges apply to crypto-currency exchanges seeking to open bank accounts.

Understanding Crypto-Currencies

All three speakers acknowledged that there was no avoiding or ignoring crypto-currencies as a product in the financial world. Even traditional banks, such as DBS have started moving into spaces previously occupied by digital banks like Sygnum, exploring the possibility of setting up a crypto-exchange and holding virtual assets.

One of the biggest difficulties in regulating crypto-exchanges was the fragmented nature of regulations across the world, with jurisdictional responses ranging from a laissez faire approach to more conservative and cautious responses. A big reason is that traditional methods of understanding risks cannot be applied to Cryptos.

Regulators now need to understand processes such as crypto mining as a potential source of wealth; whether or not a crypto-currency is backed by a fiat-currency or another underlying asset, and the methodology used to achieve such backing; and even whether the blockchain is publicly available and can be analysed to understand flows of transactions.

While traditional banks typically lack the requisite domain knowledge in crypto-currencies to appropriately assess risk, a growing number of specialised service providers, like Chainanalysis and Napier, are able to help traditional actors overcome their knowledge gap. Banks also need to ensure that their own staff in the business line, AML compliance departments, and those designing in-built technology controls, are adequately trained to broadly understand the products that they are dealing with, and at the very least the resources and providers they can resort to where necessary.

Central Bank Backed Digital Currencies

On the topic of central bank backed digital currencies ("CBDCs"), such as what has been implemented or proposed respectively in Cambodia[24] and China,[25] concerns remained around the anonymity of crypto-wallet addresses and its attendant ML/TF risks. The key for these CBDCs to succeed lay in their design, and if KYC measures or checks could be in-built into their design, the result could be a robust and well-regulated crypto-currency.

It was also suggested that CBDCs might pose privacy concerns and allow increased government surveillance of personal transactions. Mr Jain explained that deciphering block chain transactions and digital wallets had never been a straightforward task, though theoretically being on the block chain makes the movement of CBDCs more traceable than cash. Ms Singh noted that privacy laws and controls would likely be built into the system. Mr Watson balanced this view, by suggesting the trade-off between personal privacy and collective security may not be such a bad thing, if it means law enforcement is better able to trace criminal proceeds, for the greater welfare of society.

General Session 10: *Lessons Learned: Review of Recent Enforcement Actions – Banks and Beyond the Banks*

The final session of the Conference featured discussions on recent enforcement actions by regulators. The panellists included Dr. Dian Ediana Rae, Head, PPATK; Neil Jeans, Principal, Initialism; and Daisuke Nagafuchi, Japan Head of Financial

[24] See SORAMITSU, 2020. *Kingdom of Cambodia Launches Central Bank Digital Currency, Co-Developed with Fintech Company SORAMITSU*. Retrieved on https://soramitsu.co.jp/bakong-press-release/pdf

[25] See People's Bank of China, 2019. *Announcement on Fraudulence of Issuing and Promoting Digital Fiat Currency in the Name of PBC*. Retrieved on http://www.pbc.gov.cn/en/3688110/3688181/3921119/index.html

Crimes Compliance, MUFG Bank. It was moderated by Ms Rosalind Lazar, Regional AML Director (APAC), ACAMS.

Westpac Banking Corporation Fined A$1.3bn

The first case study was on the recent civil claim brought against Westpac Bank by the Australian FIU and regulator, AUSTRAC. This case has only been the third time AUSTRAC has relied on the civil claim regime to file an action against a bank, and at A$1.3 billion, is the largest claim so far.

The AML/CFT offences that Westpac were found guilty of included record keeping failures, CDD assessment failures, failures to report suspicious transactions, failures to conduct on-going due diligence, and a number of failures involving the making of International Fund Transfer Instruction ("IFTI") reports. As a result of these failures, Westpac had effectively been a weak link in the chain of reporting, and had been responsible for "dumbing down" the quality of information and data concerning international wire transfers across the Australian financial sector. Besides the IFTI reporting failures, it was also revealed through the investigations that Westpac had failed to file STRs on multiple transactions worth close to A$0.5m linked to the online procurement of child sexual exploitation material in the Philippines by Australians.

The investigation into Westpac originally started out over its IFTI reporting failures, however it was soon discovered that the there were more fundamental AML/CFT non-compliance issues systemically found across Westpac. Besides the non-compliance of AML/CFT controls within Westpac, there was also a larger failure to properly re-assess risks on an on-going basis, whether the risk of clients, or of their own products. The important take-away from the investigations and the fine was that in the eyes of AUSTRAC, responsibility and accountability for these failures lay squarely at the feet of Westpac's board. The sizeable fine was also meant as a wake up call to the boards of other banks across Australia, to do their part in ensuring compliance, and in inculcating a strong risk culture within their respective FIs.

Deutsche Bank Fined US$50m

The second case study of the session was on the recent Deutsche Bank case in relation to their banking relationship with high-profile child sex trafficker, Jeffrey Epstein. The fine imposed by the New York State Department of Financial Services in July 2020 amounted to US$150m and was primarily for failures by Deutsche Bank to report over US$13m worth of suspicious transactions relating to Epstein's sex trafficking operations and pay-outs to possible victims and co-conspirators. The failure to report STRs, and to escalate such suspicious transactions, was especially egregious, given the Deutsche Bank had already flagged Epstein as a high-risk customer.

Besides the Epstein-related charges, Deustche Bank was also found to have failed in maintaining adequate ML/TF controls, especially in relation to its correspondent banking accounts with Danske Estonia and FBME Bank. It was found that Deutsche Bank continued facilitating over US$618bn worth of correspondent transactions for FBME Bank, despite FBME being sanctioned by the United States' Financial Crimes Enforcement Network ("FinCen"). Similarly Deutsche Bank had facilitated over 340 transactions for Danske Estonia to high-risk Russian accounts despite being flagged internally by Deutsche Bank's own transaction monitoring system. In both these cases, Deutsche Bank was found to be lacking proper AML/CFT controls over these high-risk correspondent-banking relationships, or to have simply disregarded red flags and risk indicators.

This case reflects, once again, the importance of the board of directors to properly implement a risk culture within the bank and the importance of setting the tone from the top. This means more than simply having AML/CFT protocols and standards in place, but truly checking that they have been implemented correctly and consistently.

The view of the FIU

The third presentation was on the Indonesia AML regime as a whole, and the role of investigations and regulations in meeting the Indonesian government's AML/CFT policy objectives: particularly to combat ML/TF, and to encourage a robust financial sector that inspires investor confidence.

Though the PPATK has sanctioned over 27 banks over AML/CFT failures, none of these sanctions have been made public. This privacy, and avoidance of negative press stands in cultural contrast to the Western regulatory approach of publicly "naming and shaming" big names in the sector with correspondingly large fines, to serve as a warning to other players in the industry.

STRs reported by FIs form a key ingredient in helping FIUs piece together a clear picture of a potential financial crime. In this context, PPATK aims to improve the quality of STRs by sanctioning banks who fail to file STRs. Sanctions should, however, be seen as one of many approaches in a regulator's toolkit. It is also important to rely on public-private partnerships to engage with banks directly as this allows for more targeted AML investigations by the PPATK for the purpose of identifying and preventing financial crimes.

In order to improve the overall AML/CFT systems of FIs, it was reiterated that banks had to set the tone from the top, as well as embrace technology to improve their compliance and monitoring systems. Ultimately, audits of banks by FIUs was not just about fault-finding, but for the purpose of improving Indonesia's banking & finance sector, especially in the context of preparing for the FATF mutual evaluations.

PART II

Part II of this report is a reflective commentary by the author on some of the recurring themes that emerged over the course of the Conference. Two main themes are considered in this part: ‘Regulation & Policy’, and ‘Criminal Activity/Proceeds’. The views expressed are the author’s personal opinions and do not necessarily reflect the policies or views of the Centre for Banking & Finance Law.

Theme 1: Regulation & Policy

The commentaries grouped under this theme focus on the regulatory approaches undertaken by regulators so far, and the challenges faced by regulators in fine-tuning and balancing various policy objectives with AML policy goals. The intention is not to propose “solutions” but rather to take a step back, and to re-frame key issues or concepts within the world of AML compliance in a broader academic context of regulation and policy studies.

A. Public-Private Information Sharing: Window Dressing or a New Regulatory Approach?

Across both days, a number of speakers from the public sector spoke of the importance of “public-private partnerships” as an important means of fighting money laundering. Besides the keynote speakers from HKMA and MAS, regulators and FIUs from India, Indonesia, and the Philippines all talked about PPP in general as a regulatory approach towards AML, and some spoke in particular of “public-private information sharing” as an important way of making AML policy more efficient and effective.

Examples of “Public-Private Partnership” and “Information Sharing”

But what exactly did these speakers mean when they spoke of Public-Private Partnerships in the context of AML, and Public-Private Information Sharing in particular? Ostensibly, it meant different things for different speakers in different jurisdictions. For the RBI, AMLCP, and PPATK, public-private partnership appeared to be understood from the point of view of the regulator’s role as “thought-leader”, sharing AML typologies and best practices with the industry, and in certain instances, facilitating training for AML professionals in the private sector. For HKMA and MAS in particular, the buzzwords when they spoke of Public-Private Information Sharing appeared to refer to technological platforms and associations, such as FMLIT and

POET, which expedited the speed of communication between FIUs, regulators and banks which were with invited or which had opted into the platform.

Co-Option of the Private Sector

Though such platforms do indeed expedite the speed of communication between the FIs and the regulators, they can hardly constitute a game-changing new approach towards AML regulation. As mentioned by the speaker from MAS, public-private information sharing adopts a "hub and spoke" model, wherein information is fed to the public sector FIUs from the private sector FIs. However, this has always been the model of AML regulation from its very inception. The purpose of legislation and regulation requiring FIs to file STRs to FIUs and regulators has always been understood as a means through which law enforcement agencies could co-opt the private sector to collate information and intelligence on potential flows of illicit funds. However, FIs remain in the dark concerning the STRs which they have filed, and which (if any) of these STRs actually correlate to instances of ML/TF. The only information shared by the public sector with the private sector is typically in the form of specific orders relating to the freezing or seizure of assets. Fundamentally, there is an imbalance in the nature and direction of information flows between the FIUs and the FIs, which can hardly be described as "sharing".

Future Potential of Public-Private Information Sharing

Despite the calls to increase "public-private information sharing", the present trends indicate that regulators are more than satisfied with the current approach, which might be better labelled "private to public information transfer". But what if there was an actual change in approach, and law enforcement agencies and FIUs shared data with FIs regarding which STRs resulted in actual arrests, seizures, prosecutions or convictions? With such feedback from FIUs, FIs might be able to fully utilise their data analytic technology and optimise their STR systems for the purpose of reporting more "high value" suspicious transactions. This would be a desirable outcome for all parties interested in combatting money laundering and terrorism financing.

There is undoubtedly a risk involved in such public to private sharing of feedback: data savvy money launderers who access this information would be able to analyse the trends expected by the FIUs and FIs, and reverse engineer their laundering methods to avoid detection. Safeguarding against potential data leaks would thus have to be a high priority in any jurisdiction that implements such two-way systems of public-private information sharing.

Besides the possibility of private sector FIs receiving feedback from the regulators, private sector FIs could share data with each other for the purpose of optimising their AML systems and processes. This is an approach which has large untapped potential. Once again, the legal safeguards involved in designing the framework for such private-private information sharing would have to be a top priority, to ensure that data is used purely for the purpose of AML/CFT measures, and not misused by FIs seeking to understand customer profiles and business activities of their competitors. Though a tentative step in this direction of private-private information sharing, the UK's Joint Money-Laundering Intelligence Taskforce ("JMLIT") model appears to present a feasible means of allowing FIs to share and receive information on a voluntary basis[26]. The overall quality of the JMLIT eco-system of data depends, of course, on the extent to which FIs are willing to contribute towards it. Questions remain if such sharing of data for AML purposes might be misused, or if there is sufficient goodwill by the FIs to avoid such fallout.

B. Fine-tuning the Risk-Based Approach: Financial Inclusion and Digitalisation

Financial exclusion as an unintended consequence of AML measures have long been a talking point amongst policymakers, both at the national level and also within the FATF. The multiple occasions in the Conference when issues of financial inclusion arose reflect its continued importance as a topic, and the continued challenge faced by policy-makers and regulators in striking the right balance between financial inclusion and AML control.

COVID-19 as an Opportunity for Financial Inclusion

The apparent diametric opposition between AML concerns and financial inclusion was especially notable when the topic of COVID-19 and digitalisation was raised. Almost unanimously, all speakers agreed that COVID-19 and digitalisation brought an increase in ML/TF risks, while at the same time the increased adoption of technology represented a boon for financial inclusion. Speakers from India and Indonesia (from both the private and public sectors) in particular, were especially cognizant of their government's social policy objective to financially include remote and underserved segments of the population, and spoke of tangible targets set by either the government or the FIs themselves.

Interestingly, the ML/TF risks that have typically accompanied digital KYC and on-boarding were downplayed, with most speakers pointing to technological safeguards such as National Digital Identity databases, for example Singapore's MyInfo or India's Aadhaar system, or other anti-fraud checks, including facial recognition technology and liveliness checks. There is little wonder that this international shift in AML risk appetite from aversion to embracing digitalisation as a "necessity" took place in the course of a global pandemic that threatened global banking markets.

[26] See Financial Conduct Authority, 2015. Anti-money laundering taskforce unveiled. Retrieved from https://www.gov.uk/government/news/anti-money-laundering-taskforce-unveiled

Divided Priorities

Implicit in the risk-based approach is the need for FIs to balance ML/TF risks with business considerations, and at a higher level, for policy makers to similarly balance ML/TF risks with a wide range of policy objectives, ranging from encouraging economic and financial innovation, protection of personal data rights, and promotion of financial inclusion. In a pre-COVID-19 world, it was not too far of a stretch to argue that AML/CFT policy objectives could be pursued alongside economic objectives, especially considering the negative economic consequences of being grey or blacklisted by the FATF as a result of falling short of its Recommendations. However, as a result of the economic consequences of COVID-19, the primacy of economic policy objectives over AML/CFT objectives has been made clear, especially in jurisdictions where central bankers have been tasked to double-hat as AML/CFT regulators.

Tailored Inclusion

A new development in connection with financial inclusion that is worth noting is the move by certain jurisdictions like Singapore and India, to allow for highly limited "small accounts" for the purpose of limited white-listed transactions (such as for receiving salaries and government benefits) which can be opened with limited KYC, or for the purpose of allowing high-risk customers (such as formerly convicted criminals) to retain access to banking facilities for daily needs. While this move certainly mitigates ML/TF risks, and appears to tick the barest of requirements towards being "banked", it does raise questions concerning the quality and degree of banking facilities and access that needs to be granted before the social objective of financial inclusion can be substantively said to have been truly met.

Theme 2: Criminal Activity/Proceeds

This final thematic discussion pays particular attention to the relationship between AML policy and criminal activity/proceeds; a relationship that is often overlooked, taken for granted, or not clearly articulated. The first sub-theme relates to the nuanced differences between money laundering and fraud, and the role of banks in preventing fraud. The second sub-theme involves taking a closer look at two predicate crimes, illegal wildlife trafficking and human trafficking, and drawing key lessons about the dangers of AML compliance work becoming too abstract and divorced from criminal law.

C. Financial Literacy and Scam Protection in the Context of AML Policy

In the context of COVID-19, and coinciding with the move towards digitalisation and the increased offering of remote services, most jurisdictions across APAC have reported a significant rise in phone and online scams, especially targeting vulnerable and financially illiterate populations. This rise was reported in both highly urbanised jurisdictions like Hong Kong and Singapore, as well as countries with significant rural populations like India and Indonesia.

Responding to Fraud

The importance of responding to fraud was evident, as several jurisdictions have seen the development of formal public-private partnerships, such as FMLIT or the Anti-Scam Centre, whereby law enforcement agencies work closely with FIs to share information concerning scams, and work towards detecting and preventing criminals from successfully appropriating funds from vulnerable individuals. At the same time, even without an explicit public mandate, fraud prevention remains a core function in most banks, for the purpose of protecting their customer's property.

Legal Framework for Fraud Prevention

At this point, it is important to remember a key difference between fraud and money laundering. While money laundering involves the movement of illicit funds through the financial system for the purpose of hiding its illicit origins, fraud is a predicate offence in itself. Frauds and scams typically involve deceiving individuals into releasing confidential information which allows scammers to access and appropriate funds in their banks. Sometimes fraudsters even persuade their victims into transferring monies to their accounts directly, by deceiving them into believing that the monies would be repaid, as in a loan or investment. An individual might also be deceived into facilitating a money laundering operation, though in such an instance, they typically do not lose any of their own money in the process, as they simply move monies through their account according to the money launderer's instructions.

This distinction between money laundering and fraud is important for a legal reason. AML frameworks and legal regimes require FIs to report STRs to FIUs under pain of law and regulation. But there is no legal obligation for a bank or non-bank FI to invest technology or manpower into designing or implementing fraud prevention systems or mechanisms in their processes (save, perhaps for an implied contractual or tortious duty owed to their customers to maintain proper security and anti-fraud systems, though the extent of this duty has not been explored in depth in case law).

It then appears that banks have largely undertaken fraud prevention as part of a larger commercial goal of inspiring consumer confidence in their banking products. But such commercial motivations to implement anti-fraud measures may not extend to underserved and remote populations, who are arguably less financially literate to begin with, and have fewer options when it comes to choosing which FI to bank with. Indeed, the speakers from SBI and BRI, both major banks in India and Indonesia respectively, placed the burden of financial literacy and scam awareness squarely at the feet of the government.

Further Regulation or Partnership?

How, then, should law enforcement and regulators move forward in this space of fraud-prevention? Should they move towards the AML model of regulatory co-option, obligating FIs to have anti-fraud systems, to make suspected fraud reports to fraud-dedicated FIUs? Arguably such a move would not be too onerous on FIs, given that similar systems and infrastructures are already in place for the purpose of AML reporting. On the other hand, is the light-touch regulatory approach taken by certain jurisdictions, or the public-private partnership model without any legal or regulatory obligation, sufficient in this sphere?

Regardless of the approach to be taken, it seems inevitable that FIs will be playing an increasingly important role in fraud prevention in the years to come. Especially as more countries move towards "cashless economies", and financial criminals increasingly leverage on technology to target and scam their victims.

D. Illegal Wildlife Trafficking & Human Trafficking: Keeping Sight of the "Why" of AML

One of the ACAMS representatives noted in her welcome remarks that she hoped that most of the Conference discussion could be focused on the "how" of AML rather than the "why". Yet, the sessions on the IWT, human trafficking and child sexual exploitation gave good reason to not lose sight of the "why" of AML, in the practice of the "how".

Different Typologies for Different Predicate Crimes

One of the key takeaways from the session on IWT was how transactions relating to IWT could easily go unnoticed by existing AML/CFT systems, unless the AML compliance staff in question were specifically educated to look out for specific typologies relating to IWT. While AML compliance staff are typically familiar and well versed with "standard" ML typologies, such as nesting, smurfing, structuring or under-invoicing, a lack of knowledge concerning IWT could lead to these transactions going unnoticed.

IWT-related money laundering tend to hide behind the legal wildlife trade, and businesses such as seafood restaurants, private zoos, or animal transporting services. Even at the point of entering a port, customs officers unfamiliar with legal sport hunting certifications may be uncertain as to when actual cargo far exceeds the documented amounts based on legal limits. There is also a geographic pattern to IWT, where funds tend to originate from East and Southeast Asia, and the illicit fund flows tend to be channelled towards Africa.

Transaction-Specific Risk Profiles

In another session concerning the multiple AML/CFT failures of Westpac Bank, a speaker commented on how a number of transactions being made by Westpac customers were related to the financing of child sexual exploitation material through criminal syndicates in the Philippines. Notably, the profile of the customers, typically middle-aged men with a known income and source of wealth, were not "high risk" in and of themselves. But the types of transactions being made, in small denominations, to the Philippines where these men had no families, businesses, or friends, were suspicious for their specific customer profiles, and should have triggered alerts for the bank. Once again, this reflects the importance of understanding how specific typologies can vary depending on the specific predicate crimes in question.

Keeping Predicate Offences in Mind

While most AML professionals are trained to identify and detect large flows of money originating from unknown sources of wealth (presumably criminal activity) which cannot be explained from a business perspective, most AML professionals do not think to ask *what* is the predicate crime generating this income. But as illustrated in the above cases of IWT, human trafficking and child sexual exploitation, the specific types of predicate crimes can have a very tangible imprint on *how* moneys are laundered which may not fit the conventional methodology.

However, once we acknowledge the importance of keeping in mind the predicate crime, a number of attendant issues emerge. Such as what types of crimes should AML compliance officers be concerned with? For example, it is easy to make a case that AML officers should be concerned with fighting terrorism and proliferation financing due to the high stakes of a potential terrorist attack, and human trafficking and IWT are emotionally loaded issues due to the relatable or sympathetic nature of their victims. However, should AML compliance officers be equally concerned with detecting petty theft? From a resource allocation perspective, AML departments simply cannot concern themselves with every conceivable crime across the world.

Another issue is what degree of customer profiling should AML departments be engaged in for the purpose of reporting profile-specific "unusual transactions". The earlier example of why this was important pertained to middle-aged Australian men making small transfers to the Philippines and preventing the funding of child sexual exploitation material. However, where does one draw the line as to when a particular type of transaction be deemed suspicious for a particular customer profile? Should the transfer of money from a Muslim-affiliated charity to a Middle Eastern jurisdiction be deemed suspicious or run-of-the-mill? Should any and every payment from customers of Chinese nationality to a seafood company trigger alarms of potential IWT? Besides the potential social backlash from such profiling, questions have to be asked as to the amount of “noise” that might be generated in an FIU’s data lake as a result of these efforts, and a potential diversion of resources away from higher quality hits and red-flags.

Given the potential issues raised above, it is unlikely that AML professionals would actively seek to identify or report on predicate crimes or profile-specific “unusual transactions” that have not already come to the AML industry’s attention. To be proactive in this regard would be to divert resources unnecessarily, and potentially create noise that distracts the FIU from piecing together a clearer picture of potential crime. On the other hand, to be in lockstep with the rest of the industry, and to simply follow up on typologies that have already been established (even at the risk of under-reporting) would be far more desirable for the AML professional, as it safeguards their FI from being fined or sanctioned (to the extent that every other FI in the industry would have followed the same typologies in filing STRs) without unnecessary costs.

This does not mean that the AML industry remains stagnant and indifferent to new crimes or ML/TF typologies. There have been a number of times when the AML industry has collectively updated its list of typologies and awareness for crime-specific or profile-specific “unusual transactions”. The current AML industry-wide campaign led by the WWF and ACAMS to raise awareness on IWT-related money laundering typologies can be seen as the latest example of such an “update”; and in the foreseeable future, IWT-related money laundering typologies will simply be viewed as belonging to the conventional suite of ML/TF typologies that all AML professionals are to be familiar with.