Plenitude

NAVIGATING THE MAZE

Regulatory Approaches to Transnational Fraud and Money Laundering in Singapore and Hong Kong

A Plenitude White paper

Executive summary

The Asia-Pacific (APAC) region is experiencing a trend towards stricter Anti-Money Laundering (AML) and fraud regulations. This trend accelerated in Hong Kong and Singapore when authorities uncovered several organised money laundering networks, which were moving illicit funds originating from scams and illegal gambling operations based in South East Asia. A series of successful law enforcement operations throughout 2023 and 2024 highlighted the scale, sophistication, and global reach of these criminal networks. This included the disruption of the biggest money laundering operation in Singapore's history. The uncovering of these networks prompted regulators in the two financial hubs to review gaps in existing AML frameworks, and to take action to strengthen existing regulations, with Singapore's new Anti-money Laundering and Other Matters (AMLOM) bill passed on 06 August being the latest example of this.

Operations uncovered vulnerabilities in routine compliance checks in key sectors, which criminals exploited as entry points to the APAC financial system. These sectors included digital assets, precious metals and precious stones dealers, real estate, high-value items dealers, wealth management, corporate service providers, and Single Family Offices. Regulators found widespread deficiencies in key financial crime control areas, such as Enhanced Due Diligence, Transaction Monitoring, and Suspicious Activity Reporting. The banking sector as a whole has also come under increased scrutiny for posing the highest ML risks to Singapore, as stated by MAS in its latest National Risk Assessment.

The exposure of these weaknesses emphasises the need for firms to continuously review and uplift their controls in line with evolving threats and ever-changing regulations. Several global and domestic based financial institutions (FI) were left with tens or hundreds of SG$ millions in AML exposure, underscoring the cost of inadequate financial crime controls. As a response, regulators in Hong Kong and Singapore have strengthened financial crime requirements across the key sectors. Efforts have also been re-focused on improving private-private and private-public cooperation in order to counter growing fraud and money laundering, launching new information-sharing platforms such as Hong Kong's FINEST and Singapore's COSMIC. Overall, these events reignited the regulators' preoccupation with combating fraud, as well as their concerns about faltering in the 'culture of compliance'. The UK and the EU, also worried about the increasing social and economic cost of fraud, are equally working to close the gaps in AML and fraud regulations, making this a global trend.

This paper aims to outline key aspects of the recent law enforcement operations and the resulting regulatory responses in Singapore and Hong Kong, showcasing a visualisation of the full scale of the criminal networks disrupted (see Map 1 and Map 2), and providing relevant firms with a starting roadmap for uplifting their AML and fraud controls. To stay on top of the fast-paced compliance landscape in the APAC region, firms should consider:

- reviewing and uplifting policies, standards and procedures to ensure they fully comply with regulatory requirements and guidance, in particular requirements around CDD and EDD;
- reviewing and optimising their existing Transaction Monitoring solutions and consider supplementing their existing systems with state-of-the art RegTech solutions;
- investing in upskilling staff so they are better equipped to apply AML and fraud standards more effectively, as well as to detect potential financial crime or fraud;
- enhancing Management Information Systems in order to monitor existing and emerging threats more effectively; and
- improving risk assessments to ensure they adequately cover evolving transnational criminal threats and assess ongoing control effectiveness.

Introduction

Following high-profile money laundering and fraud scandals over the last year, and aiming to remain in line with global trends, regulators in Singapore and Hong Kong have worked to strengthen domestic AML and fraud regulation. As a response to these scandals, The Monetary Authority of Singapore (MAS) and the Hong Kong Monetary Authority (HKMA) both emphasised the need for FIs to strengthen their financial crime compliance controls. Firms operating in the APAC region should therefore brace for tougher enforcement action and greater regulatory scrutiny on AML and fraud compliance.

Stricter AML and fraud regimes are likely to increase the cost of compliance, squeezing the bottom line. The implementation of tighter AML and fraud controls in the UK and other European jurisdictions, such as the PSR APP fraud mandatory reimbursement, has already increased the complexity and costs of compliance operations for global firms, and similar trends are expected in Asia. Firms should ensure that their financial controls systems are proportionate to their risk exposure and are effectively designed and calibrated to increase their efficiency.

In addition to promoting stronger controls for firms, regulators focussed on the role of public-private and private-private collaboration in their strategic response to growing money laundering and fraud threats. This was due in part to the fact that a lack of cross-organisational and cross-country information sharing enabled criminals to conceal their operations. Beyond the APAC region, the IMF also signalled its renewed focus on cooperation in FCC, with calls to boost information-sharing and cross-border collaboration in combating money laundering. As efforts to improve collaboration continued to grow, Hong Kong and Singapore developed their respective data-sharing platforms to help FIs to tackle fraud and money laundering (respectively, COSMIC [Collaborative Sharing of ML/FT Information & Cases] in Singapore and FINEST [Financial Intelligence Evaluation Sharing Tool] in Hong Kong). While still in its early stages, these systems are pioneering live integration of compliance information aimed at preventing suspected money launderers and scammers from moving across financial institutions undetected.

It is crucial for firms to understand the way in which the disrupted money laundering and fraud networks operated, because it will help them to identify their threat exposure and focus on their biggest vulnerabilities. Using open-source analysis, this paper visualises these illicit networks (see MAP 1 and MAP 2) in the APAC and beyond. Section 1 and 2 review the details of the law enforcement operations in Singapore and Hong Kong, respectively. Section 3 explains which weaknesses were already known to the regulators, and what steps were taken to address the issues. Section 4 looks at how regulators in Hong Kong and Singapore have worked to close new AML regulatory loopholes exposed by the law enforcement operations, singling out regional trends likely to continue throughout 2024.

Section 1

Singapore: a money laundering operation spanning from Cambodia to London uncovers key compliance vulnerabilities in the financial system

Key Highlight

Getting the Basics Right: EDD, TM, and SARs

Up-to-date risk assessments and well- calibrated KYC processes allows firms to identify emerging threats and protect themselves and their customers. In Singapore's money laundering scandal, weak EDD allowed criminals to launder their funds. However, institutions with adequate SoF checks, TM, and SARs processes successfully detected the money laundering operations.

In August 2023, the Singapore Police Force (SPF) disrupted the largest known money laundering operation in Singapore's history. The SPF seized SG$3 billion (£1.76 billion) in assets, mostly from 'scam centres' and illegal casinos in South-East Asia. The operation exposed key vulnerabilities in Singapore's financial system, including lax AML controls in real estate, precious metals & stones dealers, and wealth management and corporate services. It also highlighted the ineffectiveness of Enhanced Due Diligence (EDD) across its banking sector, especially Source of Funds (SoF) and Source of Wealth (SoW) checks. This prompted regulators to take action to improve AML controls (see section 3). This shows the importance of providing adequate and frequent training to staff, as well as nurturing a culture of compliance throughout the organisation.

This case highlighted the ease with which sophisticated, transnational criminal networks accessed services at reputable FIs bypassing EDD checks. Law enforcement investigations uncovered up to SG$100 million (£58M) in money laundering exposure and expected credit losses of SG$197 million (£115 million) at DBS, Singapore's biggest banks, mostly incurred from financing the real estate purchases of the suspects. International wealth management firms were also hit by the scandal, with Credit Swiss holding the largest amounts on deposit so far for the convicted. Their predicament highlights how critical it is to maintain a strong FCC framework. Firms should consider consistently investing in upskilling their staff in best practices, ensuring that their Transaction Monitoring systems are efficient and that their Suspicious Activity Reporting (SAR) escalation procedure is generating sufficient true positive leads.

This case shows that the absence of intra-governmental agreements and the lack of firm-to-firm data sharing remain key obstacles for effective cross-border collaboration, highlighting the importance of initiatives like Singapore's new COSMIC platform. Singapore's recent AMLOM bill addressed these shortcomings by enhancing data sharing provisions, and singling out SARs as key drivers of AML investigations. Therefore, firms should consider frequently auditing their management information system to ensure their data exploitation is effective and can identify suspected criminal activity.

Unpacking the money laundering operation

The criminal landscape of APAC is evolving rapidly, and firms who do not keep up with it risk leaving themselves vulnerable to criminal exploitation. In January 2024, the UNODC warned that the proliferation of scam centres and illegal casinos in South East Asia provided an extremely lucrative source of business for professional money launderers. Singapore's scandal proved this: the suspects in this case allegedly used proceeds from illegal online betting centres based in the Philippines to purchase assets in Singapore. The suspects were also linked to a known organised crime syndicate accused of human trafficking and modern slavery in prison-like scam centres in Cambodia.

The visualisation of this network in Map 1 shows that this organisation was transnational and global in reach, which made it hard to counter effectively without adequate cross-border information sharing. As discussed above, the proceeds of crime originated mostly in South East Asia. The placement and layering stage of money laundering took place via Singapore. During the integration stage, the laundered funds were used to purchase assets either locally in Singapore, with 152 real estate properties seized by SPF, or in other key financial hubs, such as the £44 million property purchases in London, and the £18 million in Dubai linked to the suspects. One key lesson from this scandal is the way in which the suspects used their international connections not only to move funds across borders, but also to conceal their own identities. The ten suspects, including several individuals wanted by Chinese authorities, were apprehended by the SPF with multiple passports, some of which they allegedly obtained by bribing officials in countries like Cambodia, Turkey, and Vanuatu (see Map 1), using spelling variations of their names. This highlights the importance of thorough onboarding checks, and the need to share information between organisations to be able to successfully identify criminals who use sophisticate tactics to hide their identity.

Sectors exploited by the criminal network

Precious metals and precious stones dealers, real estate, and high value items dealers were the main sectors exploited for the layering and integration of the illicit funds, highlighting a systemic failure in implementing AML checks. Authorities seized luxury cars, gold bars, designer handbags, watches and jewellery, wine and spirits, and luxury properties.

Corporate service providers, as well as the wealth management sector and Single Family Offices (SFO), also fell under scrutiny for facilitating the entry of illicit funds in Singapore. This prompted MAS to review its internal incentive administration processes for SFOs, and tighten them where necessary. MAS also underscored that one of its key priorities for 2023-2024 is to continue focussing ‘on asset and wealth managers’ compliance with the applicable laws and regulations’. MAS’s key actions will include greater scrutiny on AML/CTF requirements, and holding senior management accountable for their FI’s lapses.

How KYC checks detected the network

The SPF was eventually alerted to the existence of the criminal operation when some of the suspects failed routine compliance checks, including Source of Funds (SoF) and Transaction Monitoring checks. The detection of forged documents by employees of one bank, followed by a series of SARs being submitted, was instrumental in tipping law enforcement and launching the investigation. This shows that implementing effective Know Your Customer (KYC) controls throughout the lifespan of the business relationship remains the best insurance against reputational damage, financial loss, and disciplinary actions from regulators.

The time it took for the criminal network to be detected raises questions about the likely laxity of AML onboarding and periodic checks across the financial sector. Regulators in Singapore and beyond share the concern that firms are overlooking financial crime compliance. The widespread incidence of anti-money laundering compliance failures among UK and APAC FIs in recent years has sparked fears that ‘compliance culture’[1] in many organisations is faltering. Following the SG$3 billion money laundering scandal, MAS issued a stern warning reminding FIs to ‘stay vigilant to ML/TF risks, and to ensure that funds flowing into Singapore are and remain legitimate’.

Singapore’s lawmakers also reviewed proposals to increase MAS’s investigative and enforcement powers to better supervise the country’s growing financial sector. The proposal underwent a second parliamentary reading in March 2024, and is yet to be finalised. The bill will strengthen MAS’ evidence-gathering capabilities and facilitate inter-agency coordination, including the power to compel individuals to attend interview and to enter premises without a warrant.

The current focus on AML compliance is not limited to Singapore: in the UK, the FCA warned of increasingly common failures in basic AML controls, and HM Treasury published a new consultation paper on how to improve the effectiveness of money laundering regulations.

FIs may consider getting ahead of the curve by consistently monitoring the effectiveness of their financial crime controls, and by reviewing in particular their EDD, SAR, and TM procedures.

Key AML Controls to Review

- Enhanced Due Diligence
- Transaction Monitoring
- Suspicious Activity Reports

Key sectors affected by ineffective AML / EDD checks

- Real estate
- Wealth management
- Corporate services providers
- Precious stones and metal dealers
- High-value items dealers

Self-Assessment Questions for FI’s

□ When is the last time you reviewed your EDD procedures, especially Source of Wealth and Source of Funds? Are they fully aligned with regulatory requirements, guidance and industry best practices?

□ How often do you provide training refreshes to your 1LoD and 2LoD?

□ When is the last time that you reviewed and calibrated your Transaction Monitoring systems?

□ Do you have adequate Unusual Activity Reporting and Suspicious Activity/Transaction Reporting escalation procedures?

[1] By ‘compliance culture’ we refer to the FCA definition of a set of habitual behaviour driven by leadership, governance, and policies that define how Financial Compliance is dealt with in an organisation.

Section 2

Hong Kong: HKPF tackles a growing network of scams fuelling international money laundering networks

Key Highlight

In with the new, but not out with the old

High-profile crypto scams in Hong Kong have increased the need for firms to upscale their fraud controls to counter digital fraud. They also provide a powerful incentive for digital asset firms to align swiftly with industry AML standards to protect their customers and their reputation. However, firms should also remain vigilant against older ML and scam tactics, which have seen no decline in popularity among criminal groups.

Much like in Singapore, recent law enforcement operations in Hong Kong prompted regulators to intensify their efforts to counter growing money laundering and fraud threats. Tougher enforcement action against domestic and international criminal organisations in Hong Kong disrupted networks laundering the proceeds of scams from Southeast Asia and South Asia, as well as local scam centres.

High-profile law enforcement operations in the digital asset sector, involving investment fraud and international money laundering in cases such as JPEX and Honax, have boosted Hong Kong's commitment to regulating virtual assets. They also prompted tougher regulations to counter growing fraud threats (see section 3).

Since regulators in APAC will likely continue to focus on combating fraud, firms operating in the region should consider making the recalibration of their fraud controls a priority. As authorised push payment (APP) fraud becomes more pervasive, effective communication with customers remains a lynchpin of good anti-fraud frameworks. Firms should monitor the implementation of the PSR's APP mandatory reimbursement in the UK, as Singapore is also contemplating a split liability model for fraud reimbursement.

Overall, recent law enforcement actions in Hong Kong have shown that criminal groups are still using old fraud and money laundering techniques, such as cold calling, alongside new techniques like generative AI-enhanced investment and romance scams. When calibrating their anti-fraud framework, firms should therefore understand emerging threats without overlooking lessons from the past.

The social and economic cost of fraud

One of the key developments driving Hong Kong's recent law enforcement crackdown was the sharp yearly increase in reported financial crimes in the Special Administrative Region. This prompted tougher enforcement action against domestic and international criminal organisations. In its last half-year report, the Hong Kong Police Force (HKPF) announced a 52% year-on-year increase in reported fraud cases, amounting to a total loss of HK$2.69 billion (£270 million). This led to stricter anti-fraud regulations in the hopes of reversing this trend (see section 3).

Aside from sophisticated international groups, smaller domestic criminal networks in Hong Kong are also a growing threat. Throughout several law enforcement operations in 2023-24, the HKPF dismantled local money laundering, scamming, and gambling rings. In one prominent case in August 2023, they arrested 458 people involved in the laundering of HK$470 million (£47.1 million) in proceeds of crime. These operations have a tangible effect because the organisations disrupted recruited money mules (both digital and physical) among children, elders, and unemployed and underemployed youth, highlighting the human cost of fraud.

Firms should expect regulators to continue focusing on combating fraud throughout 2024 due to the widespread economic and social harm it is causing. Firms should keep in mind that reviewing and enhancing their fraud controls will not only mitigate fraud loss, but will also improve existing customer experience, increase operational efficiency, and drive down overall compliance costs.

Digital asset fraud enabled by social media

Against the backdrop of rising fraud cases in Hong Kong, digital asset scams continued to receive great attention. The two most prominent cases included JPEX and Hounax. Hong Kong's Securities & Futures Committee (SFC) took action against the crypto exchange platform JPEX in September 2023 for suspicious digital asset trading practices. JPEX falsely claimed to have obtained a Virtual Asset Trading Platform (VATP) license from oversea regulators, while it continued to operate without a license in breach of Hong Kong's new VATP licensing regime. Further information on JPEX's involvement in money laundering came to light following a report by Bitrace, a blockchain data analysis company. Bitrace alleged that over TRC20-USDT4[2] 190 million tokens (£149 million) were laundered through JPEX.

The role of social media in JPEX's fraud is likely to be a key concern for regulators in developing Hong Kong's anti-fraud strategy. The SFC alleged that JPEX relied on deceptive statements made by key opinion leaders (KOLs), who were often paid promoters, to attract potential investors. Victims lost an estimated HK$1 billion (£100 million). Social media's role in spreading online scams in Hong Kong mirrors a similar trend in the UK, US, and Europe. In the US, the Federal Trade Commission recently reported that one in four victims of fraud since 2021 said the fraud started on social media.

[2] Tether USDT, or TRC20-USDT, are the standard digital tokens issued on the TRON blockchain. They are a stablecoin pegged to the US dollar.

In Europe, Europol declared that online fraud schemes represent a major criminal threat to the European Union. Similarly, UK Finance's Annual Fraud Report 2024 shows that scams originating online accounted for 76% of total reported volume in 2023. UK regulators took action by expanding the existing promotion regime to include digital asset firms. Some firms, such as Santander, launched additional protection measures for transactions involving certain social media platforms. Firms operating in the APAC region should take notice of this development and consider the best course of action to boost their anti-fraud controls in line with local regulations, while also taking into account how local social media ecosystems contribute to spreading scams.

Since the JPEX case, fraudulent digital asset companies have continued to conceal their unlicensed status to garner credibility in the eyes of their perspective victims. One of these was the HK$120 million (£12 million) scam on Hounax. More recently, a HK businesswoman lost HK$41 million (£4.15 million) to a cryptocurrency scam; victims of crypto fraud have fallen prey to a new elaborate scam whereby fake law firms promise to recover stolen crypto. Because of these growing scams, digital asset firms operating in the region should ensure they are duly licensed and are complying under new AMLO regime.

Alongside crypto fraud, the HKPF warned about other common types of scams which are increasingly committed at an organised and industrial scale. Some examples included: online romance scams, which exploit a fictitious emotional connection between the victim and the scammer to extract financial resources from the victim; CEO email scams, which tricks employees to transfer their companies' funds to an account controlled by the fraudsters; and telephone deception scams, involving the impersonation of bank staff or tax officials to trick the victim into granting access to their accounts to the fraudsters. Firms operating in the APAC region should take into consideration the fact that the UK was successful in reducing the volume of impersonating scams by 37% year-on-year with a combination of anti-fraud public campaigns and better customer communications by FIs. Firms should therefore review their customer communications to ensure they are effective in preventing fraud.

Despite digital innovation, criminals still use old playbooks in ML and fraud

While some scammers take advantage of new digital technologies, such as generative AI, other rely on older schemes, such as cold calling, which recorded a net year-on-year increase in Hong Kong between 2022 and 2023. Money launderers, too, often still rely on well-known practices, such as using established businesses to conceal the flow of illicit profits.

For instance, in one prominent investigation, a known Hong Kong property developer allegedly laundered funds on behalf of an international gambling syndicate. He used his legitimate business as a front to funnel money from Hong Kong to Canada and Australia (See Map 2). After purchasing C$12 million (£7 million) in real estate assets in Vancouver, he used the properties as collateral to take out loans through his Hong Kong company, laundering funds through loan repayments. This case shows the importance for firms to ensure SoF, SoW, and adverse media checks are conducted thoroughly.

The use of precious stones to launder illicit funds is another example of how money launderers still rely on old tactics. In December 2023, a HK Custom's operation dismantled a network laundering illicit funds from India to Hong Kong under the pretence of diamond trading, worth HK$500 million (£50.1 million). This is similar to how precious stones & metal dealers were targeted by money launderers in the Singapore scandal discussed above.

The commerce of precious stones and metal is particularly susceptible to money laundering due to the difficulty in ascertaining their origins, and the ease of cross-border transportation. These cases show that in an age of digital innovation, firms should look to understand and prepare for future and emerging threats, without forgetting to protect themselves against old fraud and money laundering tactics. Developing a comprehensive fraud detection framework, grounded in comprehensive Key Performance Indicators (KIP) and Key Risk Indicators (KRI), will be key to this balancing act.

Hong Kong's anti-fraud response

Hong Kong responded to rising numbers of scams with more effective fraud preventions strategies built around public-private and private-private cooperation (see Section 4), such as the new FINEST platform. FINEST is a new bank-to-bank information sharing platform, aiming to increase banks' ability to share information for detecting and disrupting fraud and money mule account networks. It was the outcome of a private-public cooperation initiative involving the HKMA, the HKPF, and the Hong Kong Association of Banks (HKAB). These tools, however, can only be as good as the data captured by the firms using them. Effective money laundering and fraud controls cannot generate actionable data capable of informing a long-term strategy without an equally effective management information system. Hence, as firms prepare for regulators' rising expectations on cross-organisational information sharing and better data analytics, they should also ensure that their management information systems are capable of adequately and reliably capturing whether these controls are performing effectively.

Key FCC Controls to Review

AML

- Source of Funds and Source of Wealth
- Adverse media screening

Fraud

- Customer communications

Self-Assessment Questions

For Digital Asset Firms

□ Is your business activity duly licensed and regulated?

□ Are you implementing AML controls in line with regulatory requirements, guidance and industry best practices?

For all FI's

□ Are your fraud controls in line with industry best practices? When did you last undertake a risk assessment and calibrate your controls?

□ Are your fraud controls effective? How does your fraud prevention rate compare with peers?

□ Is your Management Information adequate? Are you ready to share them with public and private entities?

Section 3

Known gaps: SG and HK targeted regulatory shortcomings in Crypto, Wealth Management and Single Family Offices

Key Highlight

Known AML Gaps

The law enforcement operations in Singapore and Hong Kong proved that criminals continued to exploit known weaknesses in local AML regimes by targeting specific sectors. Regulators had already been working to close AML gaps in the digital assets, precious stones + metal dealers, and wealth management sectors before news of the scandals broke out. This highlights Hong Kong and Singapore's continued efforts to remain vigilant.

The law enforcement operations in Hong Kong and Singapore intensified the regulators' focus on new anti-fraud responses and on strengthening AML compliance. In fact, regulators were already working to close known gaps in AML regulations by targeting some of the key sectors exploited by criminals before news of the scandals broke out, proving that they were not caught entirely by surprise by what transpired. In Hong Kong, authorities had already focused on regulating the digital assets sector, while in Singapore, MAS had taken steps to improve AML controls across the wealth management and Single Family Offices sectors.

Digital Asset regulations in HK

Concerning the Digital Asset sector, HKMA introduced new VATPs regulations in June 2023, including a new licensing regime, and AML guidelines for VATPs that included obligations to comply with the Travel Rule. The new licensing regime also applied to dealers of precious metals and precious stones, another key entry point to the financial system exploited by the money launderers. The digital asset space will remain a key focus point for firms to watch in 2024. Debates among regulators and industry stakeholder are reportedly ongoing, with the aim of finding the right compliance framework that will allow Hong Kong to fulfil its aspiration of becoming a global crypto hub while effectively managing financial crime risks.

Wealth Management AML guidance

Other key sectors exploited by professional money launderers in Singapore included wealth management and Single Family Offices. In June, MAS published its latest National Risk Assessment, assessing that banking (including wealth management) poses the highest risk of ML. MAS took a number of actions to tackle weak AML regulations in these sectors well before the SG$3 billion money laundering network was disrupted in August 2023. In March 2023, MAS published a circular on ML/TF risks in the wealth management sector, drawing attention to the need to monitor ML/TF risks from high growth areas. In June 2023, MAS published an information paper containing data analytics cases that FIs could use to detect and mitigate ML/TF risks from the misuse of Legal Persons. Lastly, in July 2023, MAS launched a public consultation on a revised framework to strengthen surveillance and defence against money laundering risks in Singapore's Single Family Office sector.

AML Prevention in the Account Sector

Following the SG$3 billion scandal, regulators identified corporate services providers such as accountants as another sector in need of more stringent regulations. As a result, Singapore's Parliament recently discussed the Accounting and Corporate Regulatory Authority (ACRA)'s proposed changes to AML prevention in the accounting sector. This included a proposal to increase penalties for Registered Filling Agents (aka. Corporate Service Providers) who fail to comply with AML regulations. The second proposed change introduced new restrictions for nominee directorships to combat the obfuscation of the ultimate beneficial ownership of companies. Firms should take notice of these proposals and monitor future outcomes.

Self-Assessment Questions for FI's

- □ Has your firm taken notice and implemented new AML/CTF regulations concerning Digital Assets, precious metal and stone dealers?
- □ Have you taken notice of the ML/TF risks highlighted by regulators in the Wealth Management, Single Family Office, and Corporate Service Provider sectors?
- □ Does your firm conduct a regular Business Wide Risk Assessment (BWRA)? Have you considered whether your firm is exposed to risks from any of the above mentioned sectors?
- □ Does your company provide adequate FCC training for new staff, as well as regular refresher session to align with new industry best practices?
- □ Does your company promote a culture of compliance by adopting an appropriate 'tone from the top'?

Section 4

Looking Ahead: New areas of focus in AML and Fraud prevention in Hong Kong and Singapore

Key Highlight

Is your MI up to par?

The importance of public-private and private-private information sharing is regaining the attention of regulators in the region, coupled with the launch of new data sharing platforms for banks. As a result, maintaining good records and having an effective Management Information System has become even more crucial for firms.

Following the disruption of the money laundering and fraud networks analysed above, regulators in Hong Kong and Singapore took action in two further areas: digital fraud prevention, and cooperation and information sharing. Combating fraud and promoting greater collaboration are likely to remain key areas of focus in 2024. Relevant firms should keep monitoring evolving regulatory expectations in these sectors and calibrate their controls accordingly. All FIs should also take notice of HKMA's recent statement on combating fraud with private-public information sharing, and prepare to uplift their management information systems accordingly.

Digital fraud prevention

The economic cost of digital fraud is an increasingly central topic in Hong Kong. Digital fraud, such as crypto or investment fraud, is often joined with sophisticated money laundering operations, as in the case of JPEX, further exacerbating the financial losses for the victims and the economic losses for Hong Kong. To counter these threats, the HKMA published a new circular on 'Enhanced approaches to combat digital fraud'. The circular draws attention to three tools: information sharing (both public-private and private-private), real-time fraud monitoring systems, such as FINEST, and a pre-transaction alert mechanism for Fast Payment Services (FPS) transactions currently under development. Firms should take note of this data-centric strategy and assess the extent to which their existing anti-fraud systems can be integrated with these new tools.

Firms may also look at recent regulatory advancement in the UK. This can provide firms with an understanding of what stricter anti-fraud policies can look like. The new requirement for Authorised Push Payments (APP) fraud reimbursement developed by the UK Payment Services Regulations (PSR) are due to come into force in October 2024. These establish a 50-50 financial responsibility to reimburse victim of fraud for sender and receiver firms, establishing stricter timeframes for reimbursement and ensuring greater customer protection. Firms should consider how anti-fraud policies the UK may impact their global operations, and how organisations can get ahead of potential upcoming changes in APAC fraud regulations.

Cooperation and Information Sharing

A number of public-public, private-private, and private-public initiative have emerged in Hong Kong and Singapore in the last year to more effectively counter money laundering and fraud. Firstly, in an attempt to boost institutional cooperation, the HKPF established a dedicated working group in collaboration with the SFC to monitor and investigate illegal activities related to VATPs. Firms operating in the digital asset sector in Hong Kong should therefore expect more intrusive scrutiny in their activities and should ensure their licensing status is settled as soon as possible. Singapore's own public-public initiative involved the launch of a new inter-ministerial committee to review and strengthen the country's AML regime. While this will not have an immediate effect on firms' Business-As-Usual operations, firms should monitor it to detect any high-level strategic shifts in Singapore's AML approach.

Secondly, RegTech provider Know Your Customer's recent collaboration with JETCO aims to deliver live registry access to FIs in Hong Kong, in a bid to improve speed and access to financial crime compliance checks. All firms operating in the Special Administrative Region should pay attention to this type of private-private initiatives, as they promise to deliver more efficient compliance solutions in the face of growing regulatory expectations.

Finally, in April 2024 Singapore launched its own COSMIC platform. The platform aims to boost private-private information sharing by allowing FIs to securely share information on potential financial crime concerns. These initiatives are important because they provide firms with a controlled environment to share sensitive data. If these initiatives prove successful, firms should prepare for more pressure from regulators to engage in cross-organisational information sharing. For this reason, it is crucial for all firms to invest now in auditing and calibrating their management information systems, so that when this level of data sharing becomes expected of them, they will be able to meet new regulatory expectations.

Firms should expect this focus on private-public and public-public information sharing to continue into 2025, as signalled by Singapore's AMLOM bill. The bill identifies a systemic failure in early detection of ML risks due to data compartmentalisation amongst government agencies, and sets up new information sharing arrangement between tax agencies and the Financial Intelligence Unit, mirroring existing practices in the UK, US, and Hong Kong. Additionally, it allows AML regulators, such as Council for Estate Agencies and the Accounting and Corporate Regulatory Authority, to access SARs filed by regulated entities, enabling them to better comprehend ML risks in the real estate and accounting sectors, which have been severely impacted by the S3$ billion scandal. Therefore, with the growing regulatory emphasis on SARs as tools for early detection of ML risks, firms should ensure that their internal detection and escalation processes are in line with industry best practices.

Conclusion

The scale and global reach of the dismantled money laundering networks across the APAC region heightened the need for greater international cooperation to tackle financial crime. While firms wait for more diplomatic agreements and data infrastructure to boost information sharing within and across borders, it is crucial for FIs to proactively review and invest in their financial crime framework, systems and controls in order to drive more effective and efficient risk management. This means ensuring that financial crime controls are adequately designed and calibrated to detect both old and new fraud and money laundering techniques and typologies.

As we have seen in the sectors above, key actions include:

- reviewing and uplifting policies, standards and procedures;
- reviewing and optimising existing Transaction Monitoring solutions;
- investing in upskilling staff; and
- improving risk assessments to ensure they adequately assesses evolving transnational criminal threat, and assess ongoing control effectiveness.

About Plenitude

Plenitude provides market-leading Financial Crime Compliance (FCC) advisory, transformation, technology, data analytics, and managed services. We are committed to building a secure financial system, safeguarding society, and empowering our clients to meet their regulatory obligations.

Appointed to the FCA's Skilled Person Panel for Financial Crime, we enable our clients to stay ahead of emerging risks and evolving regulations by optimising systems and controls, leveraging the latest AI-powered technology and data analytics, in order to drive greater effectiveness, efficiency and sustainability, reducing the overall cost of compliance.

Our best-in-class team come from a variety of backgrounds and disciplines. This breadth and depth of industry and deep subject matter expertise, alongside our scalable, full-service offering and tech-enabled delivery, enables us to meet all of our clients' needs, inspiring confidence and delivering excellence.

We work with a broad range of retail, commercial and investment banks, insurers, asset managers, as well as payment service firms, electronic money issuers, FinTechs and crypto firms across the world, ranging from startups to global financial institutions. We have a proven delivery track record and have provided advisory and transformation services on some of the most challenging projects in the industry.

Our depth of expertise and quality of service, combined with our commercial integrity, competitive rates and innovation, is second to none. Discover more about our services and see why our integrity, passion and delivery excellence have been praised by so many clients.

Written by: Valentina Pegolo

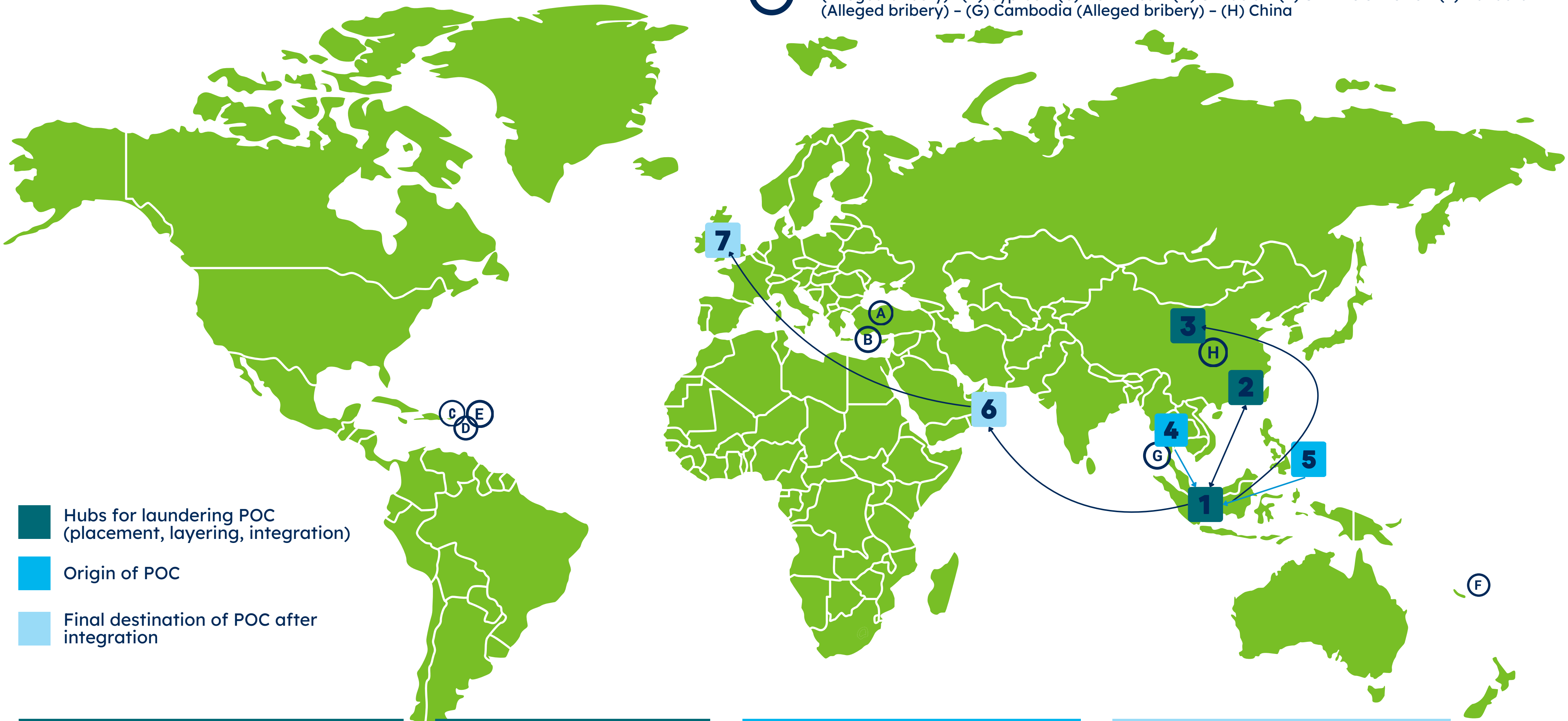
To learn more about how we can support your firm, email us at: **enquiries@plenitudeconsulting.com**

Map 1: Singapore's $3Billion Money Laundering Operation

→ International movement of proceeds of crime into financial hub (placement)

→ International movement of laundered POC for further layering or final placement

○ Countries whose passports have been found in the possession of the 10 accused: (A) Turkey (Alleged bribery)- (B) Cyprus – (C) Dominica – (D) St Lucia – (E) St Kitts & Nevis – (F) Vanuatu (Alleged bribery) – (G) Cambodia (Alleged bribery) – (H) China



■ Hubs for laundering POC (placement, layering, integration)

■ Origin of POC

■ Final destination of POC after integration

(1) Singapore

Authorities busted a ML rink for an estimated total of SG$3B of assets, arresting 10 suspects with Chinese passports

(3) China

All 10 of the accused hold Chinese passports, alongside other nationalities

(5) Philippines

Several of the accused are linked to illegal gambling operations in the Philippines

(7) London

Purchase of 3 properties in London by 2 of the suspects for a total of £44M in Oxford & Canary Wharf

(2) Hong Kong

2 of the accused controlled several HK companies, mostly registered with HK$1 in capital. One of the accused kept more than £5.5M within HK branches of prominent European and Chinese banks

(4) Cambodia

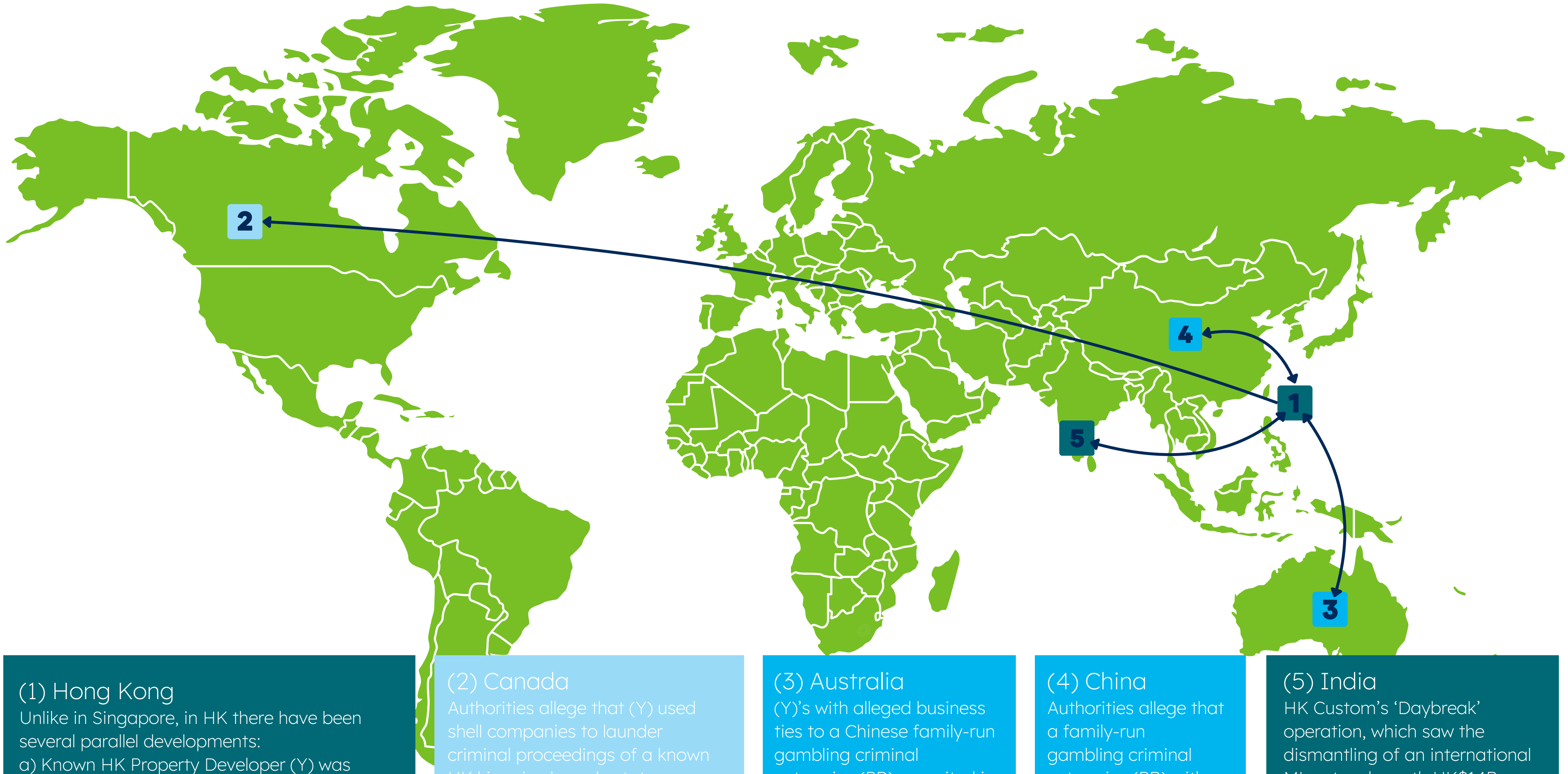
Several of the accused are linked to illegal gambling operations in Cambodia

(6) Dubai

Several of the accused have links to the UAE through properties, business investments and personal relations (i.e purchase of £18.4M condominium unit

Map 2: Transnational links in Hong Kong money laundering operations

→ International movement of laundered POC for further layering or final placement



(1) Hong Kong

Unlike in Singapore, in HK there have been several parallel developments:
a) Known HK Property Developer (Y) was found to have business links to HK & Chinese organised crime involved in ML, with operations spanning from Australia to Canada
b) Increase in domestic ML, Scam & Fraud rinks
c) Operation 'Daybreak' disruption of HK$14B ML network

(2) Canada

Authorities allege that (Y) used shell companies to launder criminal proceedings of a known HK kingpin via real estate purchases in Vancouver, backed by loans taken out by HK shell companies. (Y) was also accused of laundering money through British Columbia casinos, as well as underground banks.

(3) Australia

(Y)'s with alleged business ties to a Chinese family-run gambling criminal enterprise (PB) was cited in a lawsuit by Australian authorities for alleged involvement in organized crime and ML. Authorities also alleged links between this enterprise + human trafficking/sex slavery

(4) China

Authorities allege that a family-run gambling criminal enterprise (PB) with business ties to (Y) was implicated in ML in a past court case in China.

(5) India

HK Custom's 'Daybreak' operation, which saw the dismantling of an international ML network worth HK$14B, confirmed that proceeds from mobile app scam originated in India were laundered in HK under the pretence of precious stones trading