HONG KONG

MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT REPORT

July 2022

CONTENT

FOREWORD BY FINANCIAL SECRETARY

Hong Kong is one of the world's freest economies. It is also among the world's largest and most sophisticated financial centres. While these longstanding strengths have given Hong Kong many competitive advantages, they also carry risks, including attracting money laundering and terrorist-financing activities. To address these risks, Hong Kong has put in place a robust and effective regime, one that meets international standards set by the Financial Action Task Force. Hong Kong has been a member of the international Task Force since 1991.

Periodically, the Government conducts a comprehensive risk-assessment, examining money laundering and terrorist-financing threats facing the city and its business sectors and industries, and the enhanced ways in addressing these threats by individual sectors. The risk assessment, clearly outlining our risk profile, is the foundation for the continuous enhancement of our efforts in these areas.

This report presents the findings of Hong Kong's latest risk assessment, completed in 2021. The money laundering and terrorist-financing landscape has continued to evolve since our last risk assessment, in 2018, particularly in regard to digital financial technologies. The Financial Action Task Force also revised its recommendation in 2020 requiring jurisdictions to assess proliferation financing risk in addition to money laundering and terrorist financing risks. Accordingly, the 2021 report offers a more detailed discussion of developments, from the emergence of new financial services, including virtual-asset offerings, to changes in the types of money laundering and terrorist-financing activities and the adoption of rules and techniques to prevent related crime, and includes Hong Kong's first assessment of proliferation financing risk. I am hopeful that the publication of this report will be of significant value to the private sector and Hong Kong society as a whole.

Hong Kong received a positive evaluation of its anti-money laundering and counter-terrorist financing system from the Financial Action Task Force in 2019. And I am confident that our 2021 report will also find favour with the inter-governmental, standard-setting body. The Government is committed to ensuring that Hong Kong remains one of the world's safest and cleanest cities in which to work, do business and enjoy life.

Paul MP Chan, GBM, GBS, MH, JP
Financial Secretary

HONG KONG'S AML/CFT POLICY

The Hong Kong Special Administrative Region ("HKSAR") Government adopts a multi-agency approach in constructing its AML/CFT regime. A high-level Central Coordinating Committee on AML/CFT ("CCC"), chaired by the Financial Secretary, steers the formulation of policies and implementation of the AML/CFT regime. It comprises members from the relevant Government bureaux and departments, financial regulators and law enforcement agencies ("LEAs"), which work together to take forward AML/CFT initiatives.

The Government is committed to upholding a robust AML/CFT regime that:

(a) Fulfills the international AML/CFT standards;

(b) Deters and detects illicit fund flows in and out of the territory, through the financial system or otherwise;

(c) Combats ML/TF and restrains and confiscates illicit proceeds effectively;

(d) Reduces ML/TF vulnerabilities of both financial and non-financial sectors in Hong Kong;

(e) Adopts a risk-based approach ("RBA") in applying compliance obligations to businesses and individuals;

(f) Fosters strong collaboration with other jurisdictions to disrupt global ML/TF threats; and

(g) Promotes the awareness and builds the capacity of private sector stakeholders in combatting ML/TF risks through engagements in AML/CFT efforts.

In line with the above principles, and in response to risks and gaps identified in this assessment, the Government will focus efforts in five major areas to enhance its AML/CFT regime:

(a) Enhancing the AML/CFT legal framework to keep in pace with international standards and evolving landscape in Hong Kong, implement updated standards in recent years and provide a legal framework for better implementation of risk-based regulation;

(b) Strengthening consistent application of risk-based supervision to ensure targeted regulation of the riskier areas faced by both the financial and non-financial sectors based on risk assessments;

(c) Stepping up regular and theme-based outreach and capacity-building to promote awareness and understanding of ML/TF risks by various sectors and the wider community on a continuous basis;

(d) Monitoring new and emerging risks to respond promptly to evolving patterns of predicate offences or terrorism, and modes of ML/TF; and

(e) Strengthening law enforcement efforts and intelligence capability to tackle domestic and international ML/TF, and enhance restraint and confiscation of the proceeds of crime, including through multi-agency cooperation/ partnership.

EXECUTIVE SUMMARY

1. As an international financial centre, Hong Kong attaches great importance to safeguarding the integrity of its financial systems by implementing international AML/CFT standards to deter and detect inward and outward flows of illicit funds. Hong Kong is an active member of international AML/CFT organisations, having been a member of the FATF since 1991 and a founding member of the Asia/Pacific Group on Money Laundering ("APG") since 1997.

2. Over the years, Hong Kong has built up a comprehensive AML/CFT regime comprising a robust legal framework, effective law enforcement, rigorous preventive measures, international cooperation, and public education and publicity. To ensure that the Government can make informed decision of formulating our AML/CFT policy, we recognise the need to update the risk assessment from time to time to keep our risk profiles up-to-date.

3. Hong Kong has made reference to the FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment and adopted the World Bank Tool in conducting its territory-wide risk assessment. The purpose of the assessment is to identify, understand and update the ML and TF risks to which Hong Kong is exposed, which then form the basis for the formulation of more targeted responses.

4. The risk assessment of money laundering and terrorist financing of Hong Kong ("HRA") which was published in 2018 served as a useful basis for this HRA. With the experience gathered during the 1st HRA, each competent authority is well versed with the World Bank Tool, which is widely recognised by the FATF community and used in a number of national risk assessments. Capitalising on the experience of the previous HRA, this HRA is forward-looking. Not only does it cover the fundamentals of Hong Kong's AML/CFT regime, but also changes since the 1st HRA as well as the next steps based on the major developments observed.

5. This assessment draws on extensive consultation, quantitative and qualitative data analysis and direct engagement with regulators, LEAs, government bodies and private sector entities. The aim is to update stakeholders of the ML/TF risks faced by Hong Kong and inform the formulation of mitigating measures. The 2nd HRA focuses on addressing the shortcomings identified in the mutual evaluation ("ME") report and the new requirements that have been or will be introduced by the FATF. There are a number of enhancements to the 2nd HRA, including (a) sectoral risk assessments on financial leasing business, non-bank credit card business and credit unions; (b) proliferation financing ("PF") risk assessment; and (c) information relating to latest trends and typologies as well as matters of international and regional concerns, e.g. impact of new technologies or the AML/CFT regulatory scene, impact brought by the COVID-19 pandemic, etc.

Key Findings

Ability to combat ML/TF/PF

6. Hong Kong's ability to combat ML/TF/PF is assessed as high, characterised by its robust legal framework, high-level political commitment, close partnerships among Government agencies and between the public and private sectors, fair and efficient prosecution and judicial process, and good external and international cooperation.

7. Given the cross-sectoral nature of ML/TF/PF matters, Hong Kong has put in place an established mechanism in the form of the CCC to provide steer on the formulation of the overall AML/CFT policies. Chaired by the Financial Secretary and with membership from relevant policy bureaux, LEAs and regulators, the CCC meets regularly to examine the effectiveness of Hong Kong's AML/CFT regime in light of the domestic situation and international developments, and spearheads measures to enhance the implementation of the AML/CFT policies and strategies under a risk-based and multi-agency approach.

8. Underpinning the work of CCC, the LEAs and the regulators is a comprehensive set of legislation which provides the legal basis and guidance for ensuring the compliance of relevant financial institutions ("FIs") and designated non-financial businesses and professions ("DNFBPs") with the relevant AML/CFT and counter proliferation measures[1]. Under the steer of the CCC, legislation is under constant review and amended as the need arises. For example, the AMLO was amended in March 2018 to introduce a licensing regime for trust or company service providers ("TCSPs"). In a similar vein, legislative proposals are introduced to establish establish a licensing regime for virtual asset service providers ("VASPs") and registration regime for dealers in precious metals and stones ("DPMS").

ML threat

9. As an international finance, trade and transport hub with strong links to the Mainland, Hong Kong is exposed to ML threats arising from both internal and external predicate offences. Internally, fraud and drugs-related crimes pose high and medium-high ML threats to Hong Kong. Externally, fraud again poses a high ML threat while drugs, corruption and tax evasion pose medium-high threats.

10. In terms of the channels for laundering proceeds for illicit activities, threat analysis reveals that banking sector and money service operators ("MSOs") continue to be exposed to relatively higher risks (assessed as "high" and "medium-high" ML threat respectively) given that ML syndicates often attempt to misuse corporate bank accounts and the MSO services for ML, trying to make use of Hong Kong's efficient financial and banking systems. Attempts at misusing banking and other financial and investment services (e.g. stocks and real estate) would commonly take place at the layering stage of ML, when money launderers would create complex layers of transactions to increase the

[1] The centre piece of the set of legislation is the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, Cap 615 ("AMLO"), which is the principal piece of legislation on AML/CFT matters. Apart from the AMLO, a host of legislation is in place to regulate the licensing/registration as well as operations/conduct of FIs and DNFBPs. There are also legislation addressing specific ML/TF/PF risks, including, for example, the Drug Trafficking (Recovery of Proceeds) Ordinance, Cap. 405; Organized and Serious Crimes Ordinance ("OSCO"), Cap. 455; United Nations (Anti-Terrorism Measures) Ordinance, Cap. 575; United Nations Sanctions Ordinance, Cap. 537 ("UNSO"); and Weapons of Mass Destruction (Control of Provision of Services) Ordinance, Cap. 526.

difficulties in tracing the origins of their funds. The analysis shows that the existing regulatory and preventive measures have been effective, with suspicious activities generally being promptly reported by the relevant sectors.

11. With technological advancement, the global payment landscape has been developing rapidly. Stored value payment products, internet and mobile payment services have gained popularity in Hong Kong, with increased linkages to bank accounts. Evolution in the modus operandi, ML typologies and techniques deployed by criminals have been observed, partly attributed to the accelerated and wide-spread application of technology during the pandemic. While virtual assets ("VAs") are not legal tender and still not generally accepted as a means of payment in Hong Kong, the increasing scale and popularity of VA activities in Hong Kong have led to an increased number of VA-related fraud cases.

ML vulnerabilities

12. With the efforts in capacity building and outreach activities to strengthen the sectors' understanding of emerging trends and address existing shortcomings, the sectors have improved their understanding of ML/TF risks and awareness of AML/CFT obligations. The Joint Financial Intelligence Unit ("JFIU") has continued to receive a large number of suspicious transaction reports ("STRs") and also seen an improvement in the quality of the reports received.

Enhancements in legislative framework

13. Certain gaps in AML/CFT legislation vis-à-vis the FATF recommendations were identified in the process of conducting the 1st HRA, following which legislative exercises have been pursued to address the gaps.

14. FIs have been subject to the customer due diligence ("CDD") and record-keeping requirements under the AMLO[2] since 2012. After the commencement of the amended AMLO in March 2018, equivalent statutory requirements have also been mandated for DNFBPs. Legal professionals, accounting professionals, estate agents and TCSPs are subject to CDD and record-keeping requirements similar to those as FIs. TCSPs are required to obtain a licence from the Companies Registry ("CR"), subject to the fulfilment of a fit-and-proper test, before they can provide services in Hong Kong.

15. The implementation of the statutory AML/CFT regime under AMLO for DNFBP sectors has been generally smooth. Regulators of DNFBPs have gained more experience in risk-based supervision, and have been stepping up efforts to ensure consistent oversight, including the implementation of on-site and off-site inspections, capacity building initiatives and outreaching programmes to the sectors.

16. All companies are required by law to maintain legal ownership information by way of keeping registers of directors, members and company secretaries. To enhance transparency of corporate beneficial ownership in order to fulfil Hong Kong's international obligations, the Companies Ordinance (Cap. 622) ("CO")[3] was amended in 2018 to require a company incorporated in Hong Kong to obtain and maintain up-to-date beneficial

[2] Chapter 615 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap615
[3] Chapter 622 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap622

ownership information by way of keeping a Significant Controllers Register ("SCR").

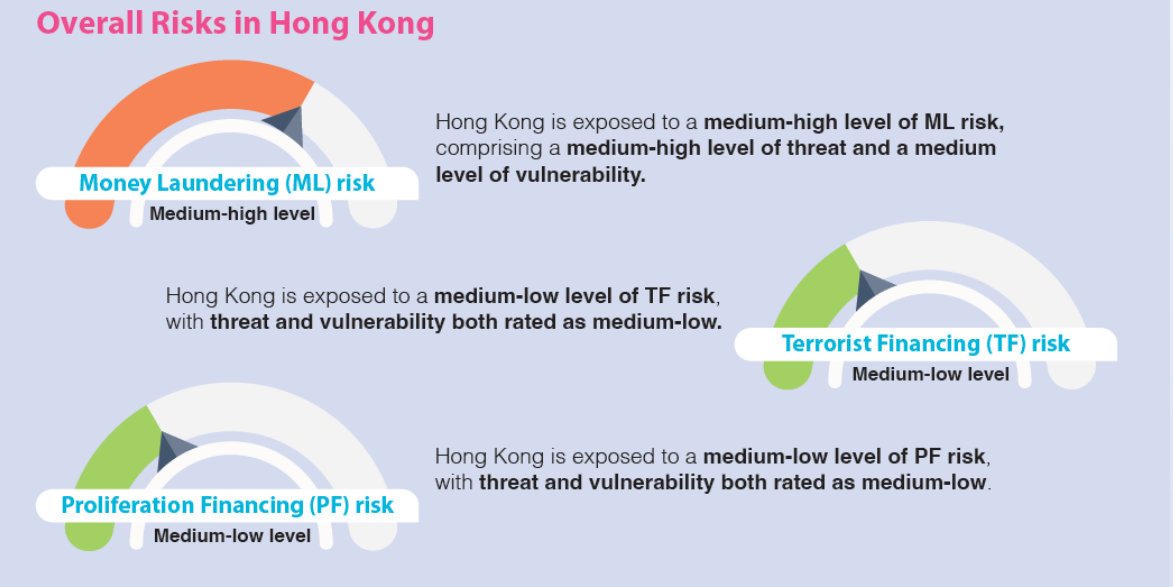
17. Having regard to FATF Recommendation 32, the Cross-boundary Movement of Physical Currency and Bearer Negotiable Instruments Ordinance (Cap. 629) ("the R32 Ordinance")[4] commenced operation in July 2018 to establish a declaration and disclosure system to detect the cross-boundary movement of large quantities of currency and bearer negotiable instruments ("CBNIs") into or out of Hong Kong. Powers are vested in the Customs and Excise Department ("C&ED") to restrain the movement of CBNIs suspected to be crime proceeds or terrorist property, to which asset recovery procedures may apply.

Overall ML risk

18. Overall, Hong Kong is exposed to a medium-high level of ML risk[5], comprising a medium-high level of threat[6] and a medium level of vulnerability[7].

TF threat

19. Hong Kong is assessed to have a "moderate" level of terrorism threat, and a medium-low level of TF threat. The threat of isolated incidents of financing extraterritorial terrorism remains, given Hong Kong's advanced and open financial system, and the cultural and economic links between certain segments of the community and regions affected by terrorism. However, after detailed investigations, there is no confirmed TF prosecution or conviction case in Hong Kong so far. On the other hand, it is observed that there was possible threat, though limited, posed by local radicals and indication of associated financing activities.



[4] Chapter 629 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap629

[5] The ML/TF risk of a jurisdiction comprises "threats" and "vulnerabilities".

[6] Threats refer to the scale and characteristics (or patterns) of the generation, inflows, and outflows of the proceeds of crime or funds linked with terrorism.

[7] Vulnerabilities refer to weaknesses or gaps in a jurisdiction's defences against ML/TF, measured with respect to relevant "input variables" (e.g. systemic measures and resources/manpower committed) at the territory-wide or sectoral level.

TF vulnerabilities

20. Hong Kong has a sound CFT framework which effectively criminalises TF through the United Nations (Anti-Terrorism Measures) Ordinance (Cap.575) ("UNATMO")[8] and the United Nations Sanctions Ordinance (Cap. 537) ("UNSO")[9]. The amendment of UNATMO in 2018 further enhances the prohibition on dealing with terrorist property and criminalises the financing of travel of foreign fighters.

21. Implementation of the R32 Ordinance, extension of CDD and record-keeping requirements to DNFBPs under the AMLO, as well as requirements for companies to keep beneficial ownership information were introduced in 2018 to help mitigate TF risks and complement ongoing CFT efforts by LEAs.

22. Further, the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region ("National Security Law") which was promulgated for implementation on 30 June 2020 also includes provisions to, inter alia, prevent, suppress and impose punishment for the offence of organisation and perpetration of terrorist activities.

Overall TF risk

23. Hong Kong is exposed to a medium-low level of TF risk, with threat and vulnerability both rated as medium-low.

PF threat

24. In response to FATF's revision of its recommendation in 2020 requiring jurisdictions to assess PF risk in addition to ML and TF risks, Hong Kong has conducted its first assessment of PF risk as an integral part of the 2nd HRA. The assessment does not only help the Government in formulating and enhancing its counter-proliferation strategy, but also informs the private sector of the overall PF risk of Hong Kong and facilitates their implementation of measures to mitigate risks posed by possible PF activities.

25. As at end-2021, designations by the United Nations Security Council ("UNSC") and its relevant Committees do not include any Hong Kong residents or companies incorporated in Hong Kong still in operation. In addition, no substantial evidence of PF activities in Hong Kong - no funds, assets and economic resources associated with persons or entities designated by UNSC - have been found in any of the investigations carried out so far.

26. Nevertheless, as Hong Kong is an international financial, trade and transportation hub with geographical proximity to proliferation-sanctioned states, Hong Kong may be exposed to external PF threat. On the whole, Hong Kong is assessed to have a medium-low level of PF threat.

PF vulnerabilities

27. As a leading international business centre providing an array of financial and professional services, Hong Kong's openness and business friendliness could be a vulnerability if exploited by proliferation actors. Hong Kong's status as a vibrant

[8] Chapter 575 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap575
[9] Chapter 537 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap537

transportation hub may also make it a target of those seeking to carry out UNSC-prohibited cargo activities. Also, the use of VAs as both a tool for fund raising as well as fund movement may be vulnerable to those seeking to evade sanctions outside the traditional financial system.

28. Despite the factors contributing to Hong Kong's PF vulnerability, Hong Kong has a robust counter-proliferation system underpinned by a comprehensive legal framework implementing sanctions imposed by the UNSC, including targeted financial sanctions ("TFS") against proliferation of weapons of mass destruction ("WMD"). The primary legislation is the UNSO, complemented by the Weapons of Mass Destruction (Control of Provision of Services) Ordinance ("WMDO") (Cap. 526)[10] and the Chemical Weapons (Convention) Ordinance ("CWCO") (Cap. 578)[11], and assisted by the strategic trade control regime under the Import and Export Ordinance ("IEO") (Cap. 60)[12]. An institutional framework with effective coordination and cooperation among policy bureaux, departments, LEAs and regulators/supervisors, as well as a well-implemented defence system by the private sector, has also been put in place. Hence, the overall PF vulnerability is assessed as medium-low.

Overall PF risk

29. Hong Kong is exposed to a medium-low level of PF risk, with threat and vulnerability both rated as medium-low.

[10] Chapter 526 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap526
[11] Chapter 578 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap578
[12] Chapter 60 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap60

Way Forward

30. In response to the risks identified in this assessment, five major areas of work are considered necessary: enhancing the AML/CFT legal framework, strengthening risk-based supervision and partnerships, stepping up outreach and awareness-raising, monitoring new and emerging risks, and strengthening law enforcement efforts and intelligence capability.

Enhancing the AML/CFT legal framework

31. To address gaps identified in the AML/CFT in fulfilment of Hong Kong's obligations under the FATF, the Government has pursued the following legislative exercises, which will further strengthen the AML/CFT capability of Hong Kong:

(a) Amend the AMLO to introduce a licensing regime for VASPs and subject them to a fit-and-proper test which is currently faced by other financial sectors. Licensed VASPs will be required to observe the AML/CFT requirements under the AMLO, as well as other regulatory requirements designed to ensure the protection of market integrity and investor interest;

(b) Amend the AMLO to introduce a registration regime for DPMS and subject registrants engaging in cash transactions at or above HK$120,000 to the AML/CFT obligations stipulated in the AMLO; and

(c) Address a number of technical issues relating to the AMLO, identified in the FATF's ME report on Hong Kong and other FATF contexts.

Strengthening risk-based supervision and partnerships

32. Financial regulators coordinate closely among themselves and with the LEAs and the JFIU as part of an increasingly proactive AML/CFT eco-system to better identify, understand and mitigate existing and emerging risks, and focus their supervisory efforts on areas identified to be of higher risk. Financial regulators review and update their AML/CFT Guidelines[13] from time to time to ensure that the requirements are in line with the latest

[13] http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/g33.pdf

international standards, local circumstances and legislative requirements. Ongoing supervisory efforts will be pursued to promote the implementation of risk-based AML/CFT systems that are critical for protecting the safety and soundness of FIs and the integrity of Hong Kong's financial system.

33. As regards DNFBPs, the relevant regulatory bodies have developed targeted supervisory strategies and issued guidelines[14] to facilitate practitioners to comply with the requirements under the AMLO. The Security Bureau ("SB") met with the relevant regulatory bodies of DNFBPs on a regular basis to facilitate mutual understanding of risks in the sectors and formulation of risk-based supervision and mitigation measures. SB also co-organised seminars/webinars with the relevant regulatory bodies of DNFBPs from time to time to enhance the awareness of the relevant sectors of the need and the ways to prevent ML/TF.

34. The police-led platform, the Fraud and Money Laundering Intelligence Taskforce ("FMLIT"), which brings together banks and the Hong Kong Monetary Authority ("HKMA") to discuss cases, trends and typologies and share intelligence, became a permanent establishment in June 2019. Taking on board the recommendation of FATF, its membership was extended to include a greater number of member banks as well as the Independent Commission Against Corruption ("ICAC") and the C&ED which helps strengthen members' capability in the investigation of corruption and customs-related ML activities.

35. The latest development took place in 2021, when additional resources were provided to form a new Financial Intelligence and Investigation Bureau ("FIIB") under the Hong Kong Police Force ("HKPF") to further strengthen Hong Kong's AML/CFT capabilities in analysing intelligence and conducting ML/TF-related investigation. At the same time, a new Financial Data Analytic Platform is being developed, which will employ advanced technologies including data mining, machine learning and artificial intelligence to allow efficient processing of financial intelligence provided by its reporting entities.

Sustaining outreach and raising awareness

36. Outreach and awareness-raising efforts by the Government, regulators and the businesses and professions concerned will continue. It is important to ensure consistent adequate awareness and understanding by FIs and DNFBPs of the ML/TF threats and the high-risk patterns pertinent to them. This will facilitate more efficient and targeted detection of suspicious activities and better focus of AML/CFT systems on genuine risks.

37. The typologies, methods and trends of ML/TF identified in this assessment, as

---

https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/guidelines/guideline-on-anti-money-laundering-and-counter-financing-of-terrorism-for-licensed-corporations/AML-Guideline-for-LCs_Eng_30-Sep-2021.pdf

[14] https://www.hklawsoc.org.hk/-/media/HKLS/Home/Support-Member/Professional-Support/Vol-2-Eng/V-2-CH-24.pdf?rev=0b02c2251ff54e52a15ba789a3ad3872&hash=7702841FBE658D9376BCDA58A0E98E1B
https://www.hkicpa.org.hk/-/media/HKICPA-Website/HKICPA/section5_membership/Professional-Representation/aml/HKICPA_AML_Enforceable_GLs_Feb2018_20180228.pdf
http://www.eaa.org.hk/Portals/0/Sections/LGA/Circular/18-01_CRE.pdf
https://www.tcsp.cr.gov.hk/tcspls/portal/guide/62/eng/TCSP_G2-e.pdf

updated from time to time, will provide useful references for the industries. They will be disseminated in the Government's and regulators' outreach efforts.

Monitoring new and emerging risks

38. Risks may evolve with changes in patterns of predicate offences or terrorism and the related modes of ML/TF, as well as the development of new technologies creating new opportunities for unlawful activities. Hong Kong will continue to monitor risks and keep abreast of new and emerging typologies to ensure it responds appropriately and proportionately.

Strengthening law enforcement efforts

39. LEAs will continue to step up ML/TF investigation, leverage the use and exchange of financial intelligence and multi-agency collaboration to secure prosecution, restraint and confiscation of illicit proceeds, ensuring that efforts and resources are effectively expended in response to the evolving landscape of crime. Furthermore, LEAs will continue to strengthen international cooperation with overseas competent authorities, to identify and combat cross-border and transnational ML syndicates and their activities.

CHAPTER 1

INTRODUCTION TO HONG KONG

1.1 Hong Kong is a Special Administrative Region of the People's Republic of China ("PRC or China"). China resumed the exercise of sovereignty over Hong Kong on 1 July 1997 under the "One Country, Two Systems" principle.

Geographical Position

1.2 On the south-eastern coast of China, the HKSAR has an area of about 1 106 km², covering Hong Kong Island, Kowloon, the New Territories and 262 outlying islands. The Macao Special Administrative Region is about 60 kilometres west of Hong Kong and is linked by high speed ferries and a helicopter service as well as the Hong Kong – Zhuhai – Macao Bridge. Hong Kong has a 35-kilometre land boundary and a 191-kilometre sea boundary with Mainland China. The HKSAR Government exercises immigration control and there are 15 control points by air, land and sea[15].

Population

1.3 In end-2021, Hong Kong had a population of almost 7.40 million[16]. In 2021, locally born residents made up about 61.7% of the population, while another 29.9% were born in Mainland China, Macao or Taiwan, and the remaining 8.4% originated from elsewhere[17]. Among the last group, there were approximately 201 000 Filipinos and 142 000 Indonesians[18], the majority of both groups being women employed as foreign domestic helpers ("FDHs").

1.4 Hong Kong has one of the highest population densities in the world, standing at 6 801 persons per km² in 2021.

Government Structure

1.5 The Basic Law is a national law of the PRC and Hong Kong's constitutional document. It provides, *inter alia*, that the HKSAR is authorised to exercise a high degree of autonomy and enjoys executive, legislative and independent judicial power, including that of final adjudication. Foreign affairs relating to Hong Kong and defence are the responsibility of Central People's Government of the PRC.

1.6 The HKSAR has an executive-led political structure headed by the Chief Executive, who is advised on major policy decisions by the Executive Council. The Administration, the executive arm of the Government, is organised into the Government Secretariat and departments. Bureaux in the Government Secretariat formulate policies and initiate legislative proposals. Departments implement laws and policies and provide direct services to the community.

---

[15] Hong Kong International Airport, Hung Hom, Lo Wu, Lok Ma Chau, Man Kam To, Sha Tau Kok, Lok Ma Chau Spur Line, China Ferry Terminal, Macau Ferry Terminal, Tuen Mun Ferry Terminal, Shenzhen Bay, Kai Tak Cruise Terminal, Express Rail Link West Kowloon, Hong Kong-Zhuhai-Macao Bridge and Heung Yuen Wai

[16] 2021 Population Census Summary Results, Census and Statistics Department.

[17] 2021 Population Census Summary Results, Census and Statistics Department.

[18] 2021 Population Census Summary Results, Census and Statistics Department.

1.7 The HKSAR has a two-tier system of representative government. At the central level Legislative Council ("LegCo") legislates, approves public expenditure and monitors the performance of the Administration. At the district level, 18 District Councils promote development of district.

1.8 The HKSAR has an independent Judiciary responsible for the administration of justice and the adjudication of cases in accordance with laws.

Legal System and the Judiciary

1.9 The legal system of Hong Kong is based on the rule of law and the independence of the Judiciary. Under the "One Country, Two Systems" policy, Hong Kong has its own legal system based on the common law, and local legislation codified in the Laws of Hong Kong. Laws in force in Hong Kong include: (a) the Basic Law; (b) PRC national laws listed in Annex III to the Basic Law as applied to Hong Kong; (c) the laws previously in force in Hong Kong before 1 July 1997, including the common law, rules of equity, ordinances, subordinate legislation and customary law, except for any that contravene the Basic Law, and subject to any amendment by LegCo; and (d) laws enacted by LegCo. Legislation in force in Hong Kong is accessible on the Internet at https://www.elegislation.gov.hk.

1.10 The Basic Law provides that the Department of Justice ("DoJ") controls criminal prosecutions, free from any interference. The Judiciary, i.e. the courts of Hong Kong, is responsible for the administration of justice in Hong Kong and the adjudication of cases, criminal and civil, in accordance with laws. It exercises judicial power independently, free from any interference. It is fundamental to Hong Kong's legal system that members of the judiciary are immune from legal action in the performance of their judicial functions.

1.11 The courts of Hong Kong comprise the Court of Final Appeal, the High Court (which consists of the Court of Appeal and the Court of First Instance), the District Court, the Magistrates' Courts and other specialised Courts and Tribunals[19].

1.12 The Court of Final Appeal is the final appellate court within the court system with the power of final adjudication. It hears appeals involving important questions of law, including in particular points of public and constitutional importance, or where leave to appeal has otherwise been granted as provided in the governing ordinance. There are one Chief Justice, three Permanent Judges, and 14 Non-Permanent Judges. Final appeals are heard by the full court comprising five judges, usually including the Chief Justice, three permanent members, and one non-permanent member. The Court of Final Appeal may as required invite judges from other common law jurisdictions to sit on the court.

1.13 The Court of Appeal of the High Court hears appeals on civil and criminal matters from the Court of First Instance and the District Court, as well as appeals from the Lands Tribunal. It also makes rulings on questions of law referred to it by the lower courts. There are 14 Justices of Appeal, including the Chief Judge of the High Court and two Vice-Presidents.

[19] Including the Juvenile Court, the Family Court, the Coroner's Court, the Obscene Articles Tribunal, the Competition Tribunal, the Lands Tribunal, the Labour Tribunal, and the Small Claims Tribunal etc.

1.14 The Court of First Instance of the High Court, comprising 23 Judges, has unlimited jurisdiction in both civil and criminal matters. In its appellate jurisdiction, it hears appeals from the Magistrates' Courts and other tribunals. The most serious indictable offences, such as murder, manslaughter, rape, armed robbery, complex commercial fraud and drug offences involving large quantities, are tried in the Court of First Instance, by a judge sitting with a jury of seven (or nine on the special direction of the judge).

1.15 The District Court has limited jurisdiction in both civil and criminal matters. In its criminal jurisdiction, the court may try the more serious offences with the exception of a few very serious offences such as murder, manslaughter and rape. The maximum term of imprisonment it can impose is seven years. There are 44 District Judges, including the Chief District Judge.

1.16 The Magistrates' Courts exercise criminal jurisdiction over a wide range of offences. Although there is a general limit of two years' imprisonment or a fine of HK$100,000 certain statutory provisions give magistrates the power to sentence up to three years' imprisonment and to impose a fine up to HK$5 million. Prosecution of indictable offences commences in the Magistrates' Courts. Depending on the seriousness of a case, the DoJ may apply to have a case transferred to the District Court or committed to the Court of First Instance of the High Court. There are 70 magistrates, including the Chief Magistrate, sitting in seven Magistrates' Courts.

Law and Order

1.17 Hong Kong is one of the safest cities in the world[20]. There were 63 232 reported crimes (excluding corruption) in 2020, representing a crime rate of around 842 cases per 100 000 of population.

1.18 Established in 1974, the ICAC combats corruption independently from other LEAs, winning wide community support and international recognition. Hong Kong was rated one of the cleanest cities in the world in several international surveys, with marked improvements in both score and ranking in 2019 and 2020[21].

Economy

1.19 Hong Kong is one of the world's most open economies with a business-friendly environment characterised by free trade, a mature financial regulatory regime and legal system, simple taxation and low tax rates, and advanced transport and telecommunications infrastructures.

1.20 The Hong Kong economy expanded at an average annual rate of 3.9% over the past two decades, faster than many other advanced economies. Over the same period,

---

[20] For instance, Hong Kong is ranked as the 8th safest cities in a 2021 ranking compiled by the Economist Intelligence Unit.

[21] For example, The Fraser Institute 2020 Economic Freedom of the World as the freest economy. The World Economic Forum 2019 Global Competitiveness Report ranked Hong Kong the 3rd most competitive economy. These surveys include corruption as one of the indicators. Whereas Hong Kong was ranked 11th in the Transparency International Corruption Perceptions Index 2020, the World Bank 2020 Worldwide Governance Indicators ranked Hong Kong 17th out of 209 economies under the dimension of Control of Corruption.

per capita gross domestic product ("GDP") rose about 66% in real terms, posting an average annual growth rate of 2.6%. In 2021, GDP at current market prices reached HK$2,861.6 billion (or around US$370 billion), and per capita GDP of HK$386,983 (or close to US$50,000) was among the highest in Asia.

1.21 Hong Kong's financial markets offer high levels of liquidity and are governed by effective and transparent regulations that are in line with international standards. Together with other important financial centres, such as London and New York, Hong Kong's markets play a vital role in the global financial system which operates round the clock. Hong Kong also provides an important gateway to the Mainland China economy and financial system. The financial sector employs 273 700 people, accounting for 7.5% of the city's total workforce, and 23.3% of its GDP in 2020. Hong Kong was the world's sixth- and Asia's second-largest banking centre, with assets of HK$26.4 trillion at the end of 2021. The city's stock market capitalisation, at about HK$42.4 trillion[22] as at the end of 2021, ranked seventh among stock exchanges in the world and fourth in Asia. The asset management business is highly international, with about 64% of assets under management coming from investors outside Hong Kong as at the end of 2020.

1.22 The overriding objective of Hong Kong's monetary policy is currency stability defined as a stable external exchange value of Hong Kong's currency against the US dollar, at around HK$7.8 to US$1. The interbank money market is also well established, supported by a robust real-time gross settlement interbank payment system enabling transactions in US$, HK$, Euro and Renminbi ("RMB") to be settled in real time.

1.23 Amid continuing internationalisation of the RMB, Hong Kong is the world's largest offshore RMB business hub supporting cross-border trade transactions, investment, financing and asset management through the development of RMB bonds, loans and equity products. In 2021, RMB trade settlement handled by banks in Hong Kong amounted to RMB7.1 trillion and RMB deposits amounted to RMB944.7billion[23].

1.24 Active international engagement and cooperation with global partners, such as membership of the Asia-Pacific Economic Cooperation forum, World Trade Organization, World Customs Organisation, etc., participation in the Trade in Service Agreements of the World Trade Organization, and the automatic exchange of financial account information in tax matters ("AEOI") coordinated by the Organisation for Economic Co-operation and Development ("OECD"), enable Hong Kong to maintain its status as an international financial and trading centre. In 2021, the city accounted for 3.1% of world merchandise trade amounting to US$1,382 billion[24], its principal trading partners being Mainland China, the US and Taiwan[25].

1.25 Hong Kong is an active participant in global standard-setting bodies such as the International Monetary Fund, the World Bank, the Basel Committee on Banking Supervision, the International Organization of Securities Commissions ("IOSCO"), the International Association of Insurance Supervisors, the FATF and the APG.

---

[22] Main board and GEM board. Source: Hong Kong Exchange website.

[23] HKMA Annual Report 2021.

[24] TID: https://www.tid.gov.hk/english/aboutus/publications/tradestat/wmttt.html

[25] TID: https://www.tid.gov.hk/english/trade_relations/mainland/trade.html

CHAPTER 2

RISK ASSESSMENT METHODOLOGY

2.1 The HRA lays a solid foundation for Hong Kong's anti-money laundering ("AML"), counter-financing of terrorism ("CFT") and counter proliferation financing ("CPF") regime. In the 4th round ME, Hong Kong has been commended by the FATF for having a good level of understanding of its ML and TF risks, which is mainly attributed to the 1st HRA and other extensive analysis, data and intelligence collection and engagement work among the LEAs, regulators, private entities and international counterparts.

2.2 This assessment builds on our understanding of the risks identified in our 1st HRA conducted in 2018 based on the World Bank National Risk Assessment Tool ("the World Bank Tool"). In conducting the 2nd HRA, we continue to adopt the World Bank Tool and make reference to the FATF Guidance papers including the FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment issued in February 2013, FATF Terrorist Financing Risk Assessment Guidance issued in July 2019 and FATF Guidance on PF Risk Assessment and Mitigation issued in June 2021. The scope of the assessment is also expanded to cover PF risk assessment which will help the formulation of the overall CPF strategies in Hong Kong. In-depth analysis of the key developments in the financial and non-financial sectors including the development of virtual bank, stored value facility ("SVF") and VASP sectors as well as the enhancement of the MSO and TCSP sectors will also be highlighted.

2.3 Through the identification of specific threats or vulnerabilities that are the causes, sources or drivers of ML/TF/PF risks, we have put in place effective controls, policies and procedures to mitigate the ML/TF/PF risks in Hong Kong.

The World Bank Tool

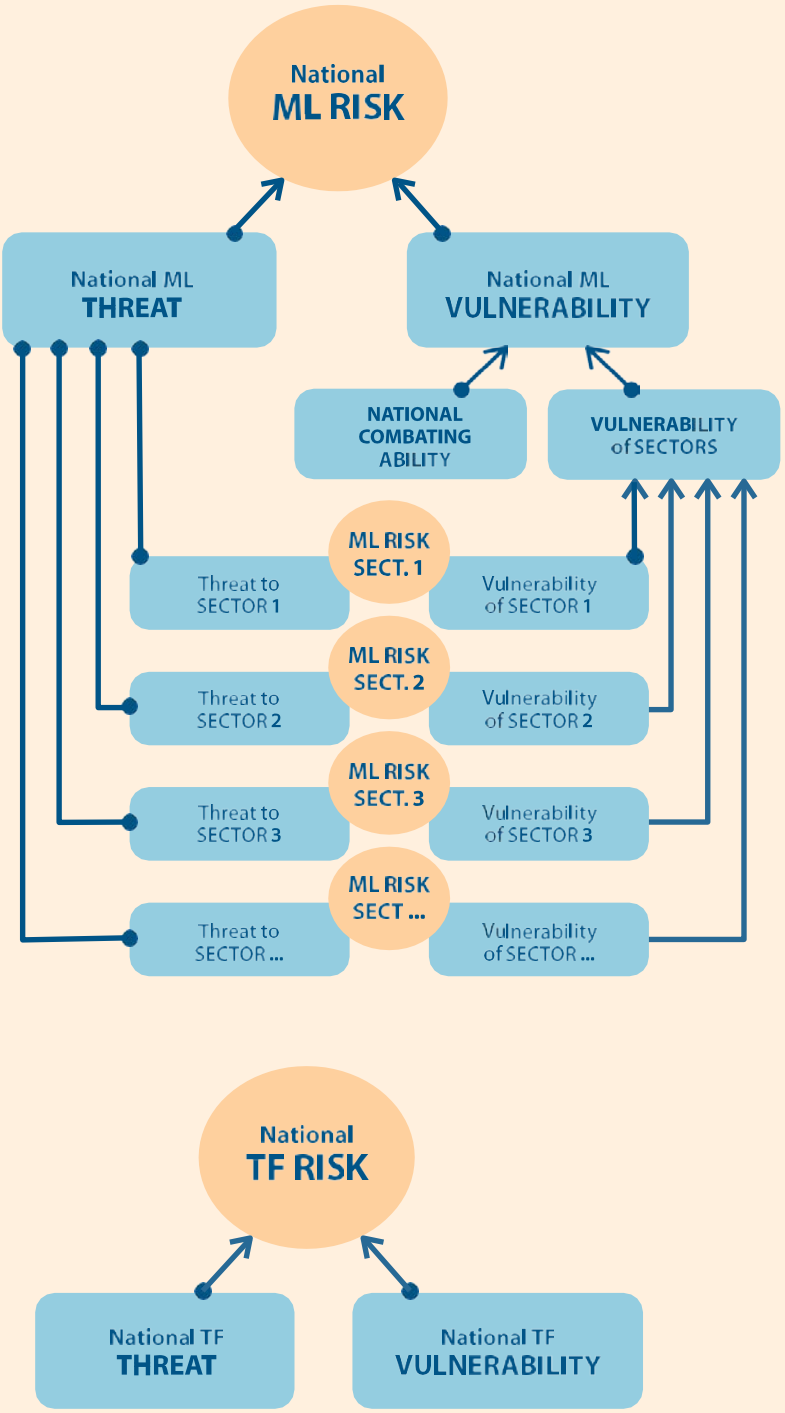
2.4 The World Bank Tool enables jurisdictions to identify the main drivers of ML/TF risks through a methodological process based on the understanding of the causal relations among risk factors and variables relating to the regulatory, institutional, and economic environment. In essence, the ML/TF risk of a jurisdiction comprises "threats" and "vulnerabilities". Threats refer to the scale and characteristics (or patterns) of the generation, inflows, and outflows of the proceeds of crime or funds linked with terrorism. For ML, this points to an assessment of the internal and external threats, including the predicate offences that generate crime proceeds, the total size of the crime proceeds, the sectors in which proceeds are invested and laundered, and other relevant factors. For TF, threats point to the direction of TF funds, and the sources and channels used. Vulnerabilities refer to weaknesses or gaps in a jurisdiction's defences against ML/TF, measured with respect to relevant "input variables" at the territory-wide or sectoral level[26].

2.5 The ML risk of a jurisdiction is the combination of threats and vulnerabilities at the territory level, which is a function of threats and vulnerabilities of individual sectors, as well as the jurisdiction's AML controls, which determine the jurisdiction's ability to combat

[26] The "input variables" include the AML/CFT legislative framework, the effectiveness of law enforcement and supervision, quality of suspicious transactions reporting, AML/CFT awareness, inherent factors such as geographic/demographic characteristics/the size of the economy or sector concerned, etc.

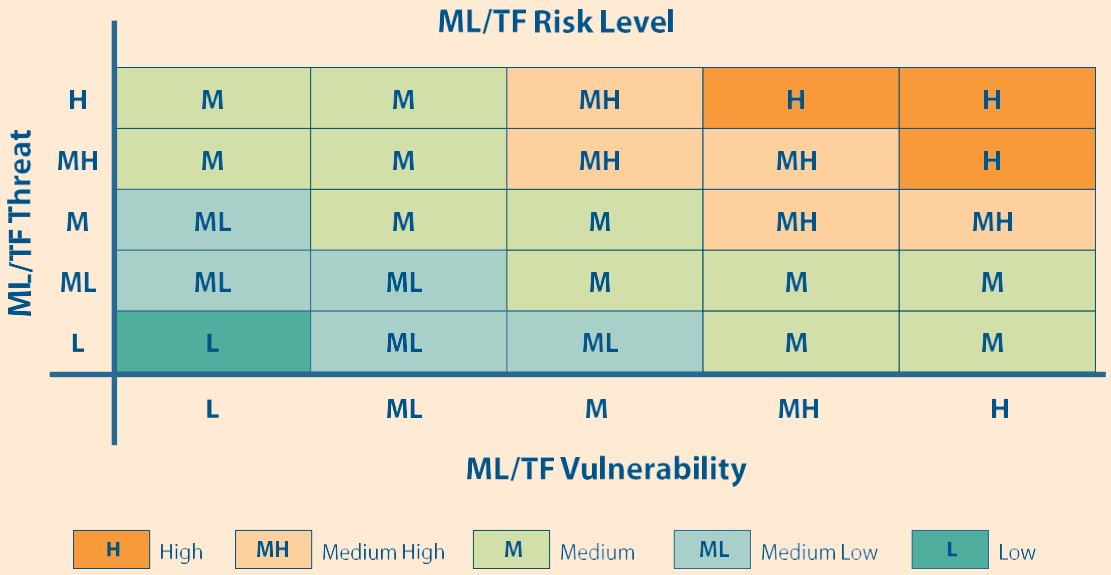
ML activities. The TF risk of a jurisdiction is an outcome of TF threats and vulnerabilities. Ratings (low, medium-low, medium, medium-high and high) are assigned to ML/TF threats and vulnerabilities, based on available qualitative and quantitative information, to generate results that can be represented graphically on a risk-level heat map. Figure 2.1 is a graphical overview of the World Bank Tool and Figure 2.2 shows the risk-level heat map[27].

Figure 2.1: Graphical overview of the World Bank Tool



[27] The description in paragraph 2.4 is based on World Bank Introduction to the National Risk Assessment Tool, June 2015 and figures 2.1 and 2.2 are reproduced from the same document.

Figure 2.2: Risk-level heat map



The Risk Assessment Process

2.6 Established in June 2014 under the direction of the CCC[28], the Steering Committee of the ML and TF Risk Assessment in Hong Kong ("the Steering Committee") continued to oversee the conduct, monitor the progress, and evaluate the findings of the HRA. The Steering Committee is chaired by the Financial Services and the Treasury Bureau ("FSTB") and members include the SB, the Commerce and Economic Development Bureau ("CEDB"), the DoJ, the HKPF, the C&ED, the ICAC, the HKMA, the Securities and Futures Commission ("SFC"), and the Insurance Authority ("IA")[29]. To reflect the expanded scope of Hong Kong's regulatory regime and the enhanced focus of 2nd HRA, its membership was expanded in October 2019 to include the CR, which oversees the licensing regime for TCSPs under the AMLO and the AML/CFT conduct of money lenders licensed under the Money Lenders Ordinance ("MLO") (Cap. 163)[30], as well as the Inland Revenue Department ("IRD") which assists in reviewing the ML threats arising from tax crimes. The members formed multi-disciplinary teams with experienced practitioners to conduct the assessment for the sectors under their purview.

2.7 The assessment process includes extensive information-gathering and scoping through record reviews, data and statistical examination, literature reviews (on typologies studies, ME reports etc.), as well as engagement with regulators, LEAs and stakeholders in the private sector. Similar to the 1st HRA which adopted a five-year timeframe for data collection and analysis, the 2nd HRA covered data spanning from 2016 to 2020, though the quantitative foundation for the current round has been substantially expanded, e.g. over 9 000 ML investigation, conviction, restraint and confiscation cases from all LEAs[31] in 2016-

[28] The CCC is a high-level Committee chaired by the Financial Secretary to steer the AML/CFT work in the Government.

[29] The IA took over the regulatory functions of the then Office of the Commissioner of Insurance, which was a government department, on 26 June 2017.

[30] Chapter 163 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap163

[31] HKPF, C&ED, ICAC and the Immigration Department ("IMMD").

2020 have been examined.

2.8 The 2nd HRA comprised two stages. The first stage involved the collection, collation and analysis of all proceeds generating crimes (e.g. figures relating to local and foreign predicates, including investigation, prosecution, confiscation, and formal and informal co-operation), having regard to updates and enhancements that have been made to the legal, regulatory and law enforcement framework on AML/CFT regime. A Stakeholders Workshop was held to discuss and deliberate the updated enforcement figures and AML/CFT framework, whereas the interim findings was also agreed upon amongst concerned stakeholders. The interim findings were then reported to the Steering Committee, along with risk mitigation measures proposed to address relevant ML/TF risks. During the second stage, the assessment was updated having regard to the enhanced mitigation measures implemented. The findings were consolidated and reported to the Steering Committee in 2021.

2.9 The 2nd HRA updates the ML/TF threats and vulnerabilities from both the territory-wide and sectoral perspectives. Drawing on our experience in the 1st HRA and the recommendations tendered by the FATF in relation to ML/TF risk understanding, we have expanded the HRA to include more in-depth and nuanced assessment on the following aspects –

(a) Risk assessment on PF in Hong Kong;

(b) In-depth analysis on the SVF and VASP sectors;

(c) Highlights of the latest developments in various sectors, e.g. virtual banks ("VBs");

(d) Inclusion of financial leasing, non-bank credit card businesses and credit unions;

(e) Detailed and focused assessment of threats in particular foreign corruption, foreign tax evasion, cross-border cash movements, and trade-based ML and emerging threats in the region such as wildlife trafficking and human trafficking; and

(f) Expanded coverage of legal persons and legal arrangements to include all forms of legal persons and legal arrangements operating in Hong Kong including relevant foreign companies and foreign legal arrangements.

Organisation of Report

2.10 In line with the Risk Assessment methodology, this report is organised as follows:

(a) Chapter 3 on the overall AML/CFT framework includes analyses of factors such as the quality of AML/CFT policies and strategy, judicial and legal framework, financial intelligence and investigation units, cross-boundary cash control, and the effectiveness of domestic and international cooperation;

(b) Chapter 4 on ML threats assesses the threats posed by various predicate crimes, taking note of the potential involvements of domestic and international crime syndicates, reflecting their sophistication, knowledge and expertise in ML activities. The prevalence and significance of ML and predicate offences, including information on investigations, prosecutions, restraint, confiscation, form of proceeds of crime, and business sectors involved were taken into account;

(c) Chapters 5 to 7 on the sectoral ML risks analyse the ML risks of relevant sectors, including financial institutions ("FIs"), designated non-financial businesses or professions ("DNFBPs") and corporate arrangements (i.e. legal persons and arrangements);

(d) Chapter 8 on TF risk outlines the landscape of terrorism and examines factors underlying the TF threat and vulnerability of Hong Kong; and

(e) Chapter 9 on PF risk outlines the CPF regime and examines factors underlying the PF threat and vulnerability of Hong Kong.

CHAPTER 3

OVERALL ML/TF COMBATING ABILITY

3.1 This Chapter outlines and analyses factors affecting Hong Kong's ability to combat ML activities. It examines the AML/CFT legal and institutional frameworks, external and international cooperation, and the prosecution and judicial process.

AML/CFT Legal Framework

3.2 Our AML/CFT legal framework has high convergence with international standards, including the pertinent Articles of the Vienna Convention[32], the Palermo Convention[33], the Terrorist Financing Convention[34], relevant United Nations Security Council Resolutions ("UNSCRs") and the FATF Recommendations.

ML offences

3.3 ML offences are prescribed under sections 25 of the OSCO[35] and of the Drug Trafficking (Recovery of Proceeds) Ordinance ("DTROP")[36] (Cap.405). These two provisions criminalise the dealing with[37] property known or reasonably believed by the person to represent proceeds of indictable offences[38] or of drug trafficking. Under the OSCO, proceeds of an indictable offence include proceeds of a crime committed elsewhere, if the crime would also have constituted an indictable offence had it been committed in Hong Kong. It is not necessary for the prosecution to prove the commission of or the specific conduct of the indictable offence or drug trafficking, or to prove that the property in question is in fact the proceeds of an indictable offence or drug trafficking[39]. The maximum penalty for ML is imprisonment for 14 years and a fine of HK$5 million.

TF offences

3.4 The UNATMO implements, inter alia, a decision of the UNSCR 1373 relating to measures for the prevention of terrorist acts. Sections 7 and 8 criminalise the provision or collection of any property to commit terrorist acts; and the act of making any property or financial (or related) services available, or collecting property, or soliciting financial (or related) services, to or for the benefit of a terrorist or terrorist associate. The maximum penalty for either of these offences is 14 years' imprisonment and a fine of unlimited amount.

---

[32] The 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.

[33] The 2000 United Nations Convention Against Transnational Organized Crime.

[34] The Terrorist Financing Convention (formally, the International Convention for the Suppression of the Financing of Terrorism) is a 1999 United Nations treaty designed to criminalise acts of financing acts of terrorism.

[35] Chapter 455 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap455

[36] Chapter 405 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap405

[37] "Dealing", in relation to property, includes receiving, acquiring, concealing, disguising, disposing of, converting, and bringing into or removing from Hong Kong the property; and using the property to borrow money or as security.

[38] "Indictable offences", as opposed to "summary offences", refer to the more serious crimes in common law jurisdictions.

[39] There are strong policy reasons: the predicate offence is likely to have taken place in another jurisdiction not susceptible to proof in Hong Kong, and the proceeds of such crimes are likely to have passed through various layers and transformations aimed at concealing their provenance. (See paragraphs 90-91 of *HKSAR v Yeung Ka Sing, Carson and Another* [2016] HKCFA 54).

3.5 The UNATMO was amended in 2018 to prohibit any person from dealing with specified terrorist property and property of specified terrorists or terrorist associates, as well as to criminalise, among other things, the financing of the travel of individuals between states for the purpose of perpetration, planning or preparation of, or participation in, terrorist acts or the provision or receiving of terrorist training, in line with the FATF recommendation to enhance the freezing mechanism of terrorist property and UNSCR 2178 which affirms the need to combat threats by foreign terrorist fighters.

TFS related to PF

3.6 The UNSO[40] empowers the Chief Executive to make regulations to give effect to instructions given by the Ministry of Foreign Affairs of the PRC to implement sanctions[41] imposed by the UNSC against persons and places outside the PRC. As far as TFS related to PF are concerned, the United Nations Sanctions (Democratic People's Republic of Korea) Regulation (Cap. 537AE) ("DPRK Regulation")[42] and the United Nations Sanctions (Joint Comprehensive Plan of Action— Iran) Regulation[43] ("the Iran Regulation"), both made under the UNSO, implement UNSC sanctions against DPRK and Iran. The maximum penalty for contravening TFS under the two Regulations is imprisonment for seven years and a fine of unlimited amount.

3.7 Under the WMDO[44], any services which may assist in the development, production, acquisition or stockpiling of WMD in or outside Hong Kong are prohibited. Examples of such services include financing, sourcing of materials and provision of professional and consulting services, technological information or know-how. The maximum penalty for offences under the Ordinance is imprisonment for seven years and a fine of unlimited amount.

3.8 To prevent Hong Kong from being used as a conduit for proliferation of WMD, a strategic trade control system is also instituted under the IEO and its subsidiary legislation, the Import and Export (Strategic Commodities) Regulations[45], to regulate the movement of strategic commodities into and out of Hong Kong. Import, export and transshipment of strategic commodities (including munitions[46], dual-use goods[47], and other sensitive items intended for use in the production, development or use of WMD) are prohibited unless accompanied by valid licences issued by the Trade and Industry Department ("TID"). The processing of a licence application includes a technical assessment process and a risk assessment process. Under section 6A of the IEO, it is a criminal offence to violate the licensing requirements, and the maximum penalty is imprisonment for seven years and a fine of unlimited amount.

---

40 Chapter 537 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap537

41 "Sanctions" is defined under the UNSO to include complete or partial economic and trade embargoes, arms embargoes and other mandatory measures decided by the UNSC, implemented against a person or a place outside the PRC.

42 Chapter 537AE of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap537AE

43 Chapter 537BV of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap537BV

44 Chapter 526 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap526

45 Chapter 60G of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap60G

46 For example, firearms, ammunition, explosives, bombs and rockets, tanks and toxicological agents, etc., and equipment and technology for the production of these weapons.

47 For example, nuclear materials, facilities and equipment; materials, chemicals, micro-organisms and toxins; electronics; computers; telecommunications and information security; sensors and lasers; navigation and avionics; marine; propulsion systems, space vehicles and related equipment.

Suspicious transaction reporting

3.9 Under sections 25A of the OSCO and the DTROP, and section 12 of the UNATMO, any person who knows or suspects that any property represents proceeds of an indictable offence/drug trafficking, or is terrorist property must report his/her knowledge or suspicion to the authorities as soon as is reasonable or practicable. Failure to do so constitutes an offence punishable by HK$50,000 and up to three months' imprisonment.

Customer due diligence and record-keeping requirements

3.10 The AMLO supports the prevention and detection of ML/TF activities by requiring FIs and DNFBPs to conduct CDD on their customers and keep records for a specified period. Effective implementation of CDD rules is aided by a number of sector-specific AML/CFT Guidelines, which are published under the AMLO by respective regulators and self-regulatory bodies, and may be taken into consideration in any court proceedings under the AMLO. FIs and DNFBPs, including their management or employees, are subject to criminal or supervisory sanctions for breaches of the AMLO requirements. The maximum penalty for the most serious offence under the AMLO is a fine of HK$1 million and imprisonment for seven years. Disciplinary actions that may be imposed on an FI include a public reprimand, an order for remedial action, and a pecuniary penalty not exceeding the greater of HK$10 million or three times the amount of the profit gained (or cost avoided) by the FI as a result of a contravention.

3.11 Following the inclusion of DNFBPs (including legal professionals, accounting professionals, estate agents, TCSPs) under the regulatory framework of AMLO since 1 March 2018, the Government introduced a bill into the LegCo to amend the AMLO to introduce a licensing regime for VASP and a registration regime for DPMS in 2022. Same as other FIs and DNFBPs, licensed VASPs (as one of the FIs) and registered DPMS engaging in regulated activities (as one of the DNFBPs) will also be subject to the CDD and record-keeping requirements under the AMLO.

Currency and bearer negotiable instruments

3.12 Pursuant to the FATF Recommendation 32, the R32 Ordinance came into operation on 16 July 2018. It establishes a declaration and disclosure system on the cross-boundary transportation of large quantities of CBNIs into and out of Hong Kong, and provide powers to restrain the movement of CBNIs suspected to be crime proceeds or terrorist property, to which asset recovery procedures could apply. The system does not restrict the free flow of legitimate capital. The R32 Ordinance empowered the C&ED to be the primary law enforcement agency.

3.13 Under the R32 Ordinance, for travellers, any person arriving in Hong Kong at a specified control point set out in Schedule 1 to the R32 Ordinance and in possession of a large quantity of CBNIs (i.e. total value of more than HK$120,000) must make a written declaration to a Customs officer. Any person arriving in Hong Kong other than at a specified control point (e.g. travellers arriving on cruise ships berthing at anchorages), or is about to leave Hong Kong, upon the requirement of a Customs officer, must disclose whether the person is in possession of a large quantity of CBNIs. If so, the person must make a written declaration. For a large quantity of CBNIs imported or exported in a cargo consignment, an advance electronic declaration must be made via the Currency and Bearer Negotiable Instruments Declaration System. Customs officers can seize and detain CBNIs if the CBNIs are reasonably suspected to be crime proceeds or terrorist property, and the seized CBNIs

are subject to the confiscation or forfeiture mechanisms under the OSCO, the DTROP or the UNATMO.

3.14 Criminal sanctions apply to failure to comply, with a maximum penalty of a fine of HK$500,000 and two years' imprisonment. A payment for specified offence will apply to certain first-time offenders[48] in lieu of criminal prosecution.

Restraint and confiscation/forfeiture of crime proceeds and terrorist property

3.15 The OSCO[49] contains provisions for the restraint and confiscation of proceeds of an indictable offence and the DTROP[50] has similar provisions for proceeds of drug trafficking. Applications for restraint can be made to the Court of First Instance against the realisable property (assets and funds) of a person, against whom proceedings for an offence have been instituted. Upon conviction, the Court of First Instance or the District Court may make a confiscation order in respect of proceeds of at least HK$100,000 of a specified offence under the OSCO, or proceeds of any amount of a drug trafficking offence under the DTROP. The Court of First Instance may also make a confiscation order against absconders or deceased persons. In addition, a civil forfeiture regime is available under section 24D of the DTROP in respect of monies in excess of HK$125,000, seized and detained during import into or export from Hong Kong and representing proceeds of drug trafficking or property used or intended to be used in drug trafficking.

3.16 Proceeds of corruption may also be recovered under section 12 of the Prevention of Bribery Ordinance ("POBO")[51] (Cap. 201), which empowers a court (of any level) to make a "restitution order" against a person guilty of a bribery offence to pay to the Government or to such person or public body and in such manner as the court directs the amount or value of any advantage received by the person. Upon conviction of the offence of possession of unexplained pecuniary resources or property, i.e. resources or property falling under section 10(1)(b) of POBO, the Court may, under section 12AA of POBO, confiscate any pecuniary resources or property in the defendant's control up to the value of unexplained resources or property.

3.17 Section 6 of the UNATMO provides for the freezing of suspected terrorist property under the direction of the Secretary for Security. Under section 13, the Court of First Instance may order the forfeiture of terrorist property which represents any proceeds arising from a terrorist act, or which was used or is intended to be used to finance or otherwise assist the commission of a terrorist act. The UNATMO was amended in 2018 to enhance the freezing mechanism of terrorist property by introducing a 'blanket' freezing provision prohibiting any person from dealing with specified terrorist property and property of specified terrorists or terrorist associates. The amendments came into operation on 31 May 2018.

---

[48] Travellers who have not previously contravened the declaration or disclosure requirements, who have not been previously been convicted of ML or TF offences, and whose CBNIs are not reasonably suspected to be crime proceeds or terrorist property, may pay a fee to discharge their statutory liability.

[49] Section 15 of the OSCO for restraint order; Section 8, Schedule 1 and Schedule 2 of the OSCO for confiscation order.

[50] Section 10 of the DTROP for restraint order. Section 3 of the DTROP for confiscation order.

[51] Chapter 201 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap201

3.18 The Criminal Procedure Ordinance[52] also provides for the disposal of property and instrumentalities related to crime, including ML/TF cases and the predicate offences. The court (of any level) can order the property to be returned to the owner or be forfeited.

3.19 Restraint and confiscation of crime proceeds and confiscation of terrorist property that have flowed from Hong Kong to other jurisdictions, or vice versa, are permissible under the framework of mutual legal assistance ("MLA") in criminal matters, as discussed under the section of "External and International Cooperation".

High-level Commitment and Institutional Framework

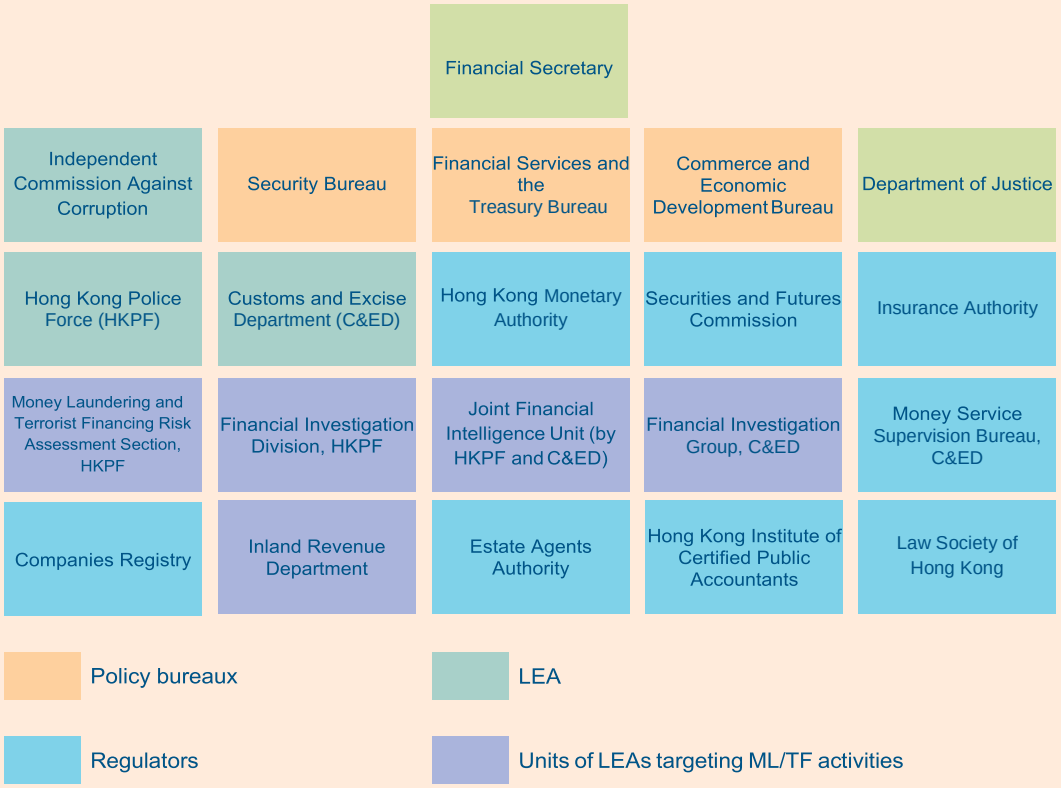
3.20 As one of the world's major financial centres, Hong Kong attaches great importance to safeguarding the integrity of the territory's financial system and recognises the importance of maintaining a comprehensive and robust AML/CFT regime. This requires high-level political commitment from the Government and close collaboration and coordination among policy-making bodies, financial regulators, LEAs and others.

CCC

3.21 The Financial Secretary chairs the CCC, established in 2008, to oversee the HKSAR Government's AML/CFT policies and strategies. The CCC comprises senior representatives from the Government bureaux/departments with responsibilities for policy making or law enforcement: the FSTB, the SB, the CEDB, the DoJ, LEAs (the HKPF, the C&ED and the ICAC), financial regulators (the HKMA, the SFC, the IA, the Money Service Supervision Bureau ("MSSB") of the C&ED) and other regulators including CR. Other bureaux and departments (such as the IRD and the TID) attend as necessary. The CCC meets regularly to examine the effectiveness of Hong Kong's AML/CFT regime in light of the domestic situation and international developments. It spearheads measures to enhance the implementation of the AML/CFT policies and strategies under a risk-based and multi-agency approach. Below the CCC, an AML Regulation and Supervision Co-ordination Group, chaired by the FSTB and comprising the aforementioned financial regulators as members with other policy bureaux and LEAs invited as necessary, acts as a forum for discussion of issues relating to implementation of the AML/CFT regime.

[52] Chapter 221 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap221

Figure 3.1: Key stakeholders in the coordination and implementation of AML/CFT policies and strategies in the HKSAR Government



Policy bureaux

3.22 The FSTB is responsible for coordinating the Government's efforts to deliver AML/CFT policies, strategies and legislative initiatives endorsed by the CCC. The FSTB monitors the overall effectiveness of Hong Kong's AML/CFT regime and compliance with the FATF Recommendations, and facilitates cooperation among stakeholders. The SB is responsible for overall counter-terrorism strategy, and supports the FSTB in a number of AML/CFT policy areas such as CDD and record-keeping measures for DNFBPs, and the declaration/disclosure system for CBNIs. The CEDB is responsible for coordinating the implementation of UNSCRs against PF and overseeing the WMD and strategic trade control regime.

Financial regulators

3.23 The HKMA, the SFC, the IA and the MSSB of the C&ED are "relevant authorities" under the AMLO for their respective sectors and have powers to ensure compliance with CDD and record-keeping requirements. The regulators have issued guidelines, aligned with each other to the extent possible, on how they expect regulatees to comply with the AMLO requirements. They also issue sector-specific guidance including circulars and frequently asked questions ("FAQs"), as well as arrange outreach and capacity building activities on AML/CFT matters including training, seminars and other education for their sectors. Details of work of the financial regulators and the risk assessment of their respective sectors can be found in Chapter 5.

3.24 In addition to the powers under the AMLO, the HKMA, the SFC and the IA have extensive powers to regulate their sectors under specific legislation (the HKMA under the Banking Ordinance ("BO")[53] (Cap. 155) and the Payment Systems and Stored Value Facilities Ordinance ("PSSVFO")[54] (Cap. 584), the SFC under the Securities and Futures Ordinance ("SFO")[55] (Cap. 571), and the IA under the Insurance Ordinance ("IO") (Cap. 41)[56]. These include licensing, requiring institutions to establish appropriate systems and controls including for AML/CFT, powers to appoint independent auditors or managers, and powers to enforce compliance and impose sanctions. Meanwhile, the Commissioner of Customs and Excise ("CCE") is empowered to regulate MSOs under the AMLO. All the regulators adopt an RBA for supervision of their sectors, and review their RBA from time to time.

3.25 The regulators participate in international bodies related to the industries that they regulate, including forums related to AML/CFT. They coordinate domestically via the AML Regulation and Supervision Co-ordination Group on policies and supervisory matters, the AML Regulatory Enforcement Co-ordination Group on enforcement matters, and through multilateral and bilateral contacts as required.

Designated Non-financial businesses and professions regulators

3.26 The CR, Estate Agents Authority ("EAA"), the Hong Kong Institute of Certified Public Accountants ("HKICPA"), and the Law Society of Hong Kong ("LSHK") are the designated regulatory authority/bodies in supervising the AML/CFT compliance under the AMLO for their respective DNFBPs. The regulators have issued guidelines and FAQs, and arranged outreaching and capacity building initiatives, including training and seminars for their sectors on AML/CFT matters. Details of their supervisory work and capacity building efforts are set out in Chapter 6.

DoJ

3.27 The Prosecutions Division of the DoJ prosecutes trials, including of ML/TF offences, and advises on and/or institutes proceedings to restrain and confiscate or forfeit crime proceeds or terrorist property. The Law Drafting Division and other relevant divisions work with policy bureaux from time to time on preparing legislation to update the AML/CFT legislative framework. The International Law Division processes requests for MLA and surrender of fugitive offenders and advises on legal matters in relation to the FATF and international AML/CFT standards in conjunction with other divisions of DoJ.

LEAs

3.28 The investigation of ML and TF offences rests primarily with the HKPF and the C&ED, with the ICAC investigating ML offences that are facilitated by or connected with corruption. Hong Kong's LEAs have a reputation for integrity and effectiveness[57] and for

---

[53] Chapter 155 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap155

[54] Chapter 584 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap584

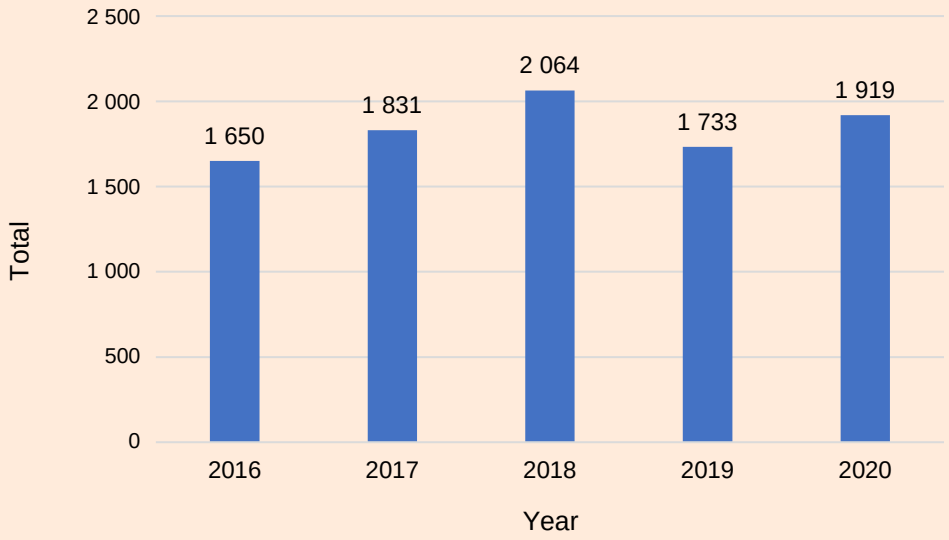
[55] Chapter 571 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap571

[56] Chapter 41 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap41

[57] The "Corruption Perceptions Index 2020" published by the Transparency International stated that, Hong Kong is one of the least corrupt economies in the world that ranks 11 out of 180 countries, and scores 77 out of 100 points. The overall corruption scene in Hong Kong's civil service has remained generally stable over the years. Hong Kong is ranked 6th out of 162 countries for the "Reliability of Police" in the Human Freedom Index 2020 published by the Fraser Institute.

fair and rigorous enforcement of the law. Laws[58], regulations[59], codes[60] and orders[61] are in place to preserve the integrity of investigating officers. The HKPF, the C&ED and the ICAC have also implemented measures, including vetting and regular interviews, to ensure a high standard of conduct and integrity among investigators at all times.

Figure 3.2: Number of ML investigations



HKPF

3.29 The HKPF is the primary LEA for ML/TF and predicate offences investigation under the Police Force Ordinance[62] (Cap. 232), the OSCO, the DTROP and the UNATMO.

3.30 Previously housed under the Narcotics Bureau ("NB") for historical reasons[63], the formations responsible for AML work in the HKPF traditionally comprised (i) the Financial Investigation Division ("FID") which specialises in investigating ML and TF relating to drugs and organised crimes, as well as tracing and confiscating proceeds under the OSCO, the DTROP and the UNATMO; (ii) the JFIU (more details of JFIU can be found in para. [3.38-3.39]) and (iii) a Risk Assessment Unit ("RAU") which assists the FSTB in conducting the HRA. With a view to strengthening Hong Kong's AML/CFT capabilities in the face of evolving crime landscape, these three formations were detached from the NB to form a new FIIB with effect from 1 June 2021. As part of the restructuring, extra resources have also been allocated to strengthen the manpower of the FIIB in both financial investigation and intelligence gathering. Under the new FIIB set-up, the RAU was expanded to take up a headquarters role, assuming additional responsibilities such as policy and strategic analysis, training for LEAs and capacity-building for the private sector. The establishment of the FIIB marked a key milestone which showcases Hong Kong's commitment in fulfilling the international AML/CFT standards and safeguarding the financial system of Hong Kong sustaining our status as an international financial centre.

---

[58] For example, the Prevention of Bribery Ordinance. See footnote 42.
[59] Civil Service Regulations.
[60] Civil Service Code.
[61] Disciplinary and integrity related orders are issued by the respective departments and units.
[62] Chapter 232 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap232
[63] The FATF's purview covered only ML in respect of drug trafficking when it was established in 1989. Based on historical reason, formations responsible for AML work in the HKPF are housed under its Narcotics Bureau.

3.31 Other crime investigation teams or units (at headquarters, regional or district levels) also conduct ML investigations during enquiries into predicate offences, or other serious or organised crimes. In particular, the Commercial Crime Bureau ("CCB") is responsible for investigating serious, complex and syndicated commercial crimes and business fraud and the Cyber Security and Technology Crime Bureau ("CSTCB") is responsible for carrying out technology crime investigations. Different formations within the HKPF closely coordinate and cooperate on matters related to ML cases.

C&ED

3.32 The C&ED has established the Financial Investigation Group ("FIG") under the Syndicate Crimes Investigation Bureau to investigate ML cases with predicate offences under the C&ED's purview, e.g. smuggling, intellectual-property and drugs offences, and to trace, restrain and confiscate proceeds of such offences. The C&ED has expanded the capacity of FIG with new injection of manpower since October 2020 to enhance the enforcement capability against ML activities. FIG will continue to work closely with the Mainland and Macao Customs as well as other overseas LEAs against cross-boundary and transnational ML syndicates.

3.33 The C&ED also safeguards the certification and licensing systems, which are of vital importance to Hong Kong's trading integrity. The C&ED carries out cargo examination at control points, factory inspections and consignment checks and is a member of the Hong Kong Compliance Office set up to assist the Central People's Government in implementing the Chemical Weapons Convention in Hong Kong through the Chemical Weapons (Convention) Ordinance[64] (Cap. 578). As noted above, the MSSB under the C&ED licenses and regulates MSOs under the AMLO.

3.34 The C&ED is the enforcement agency of the strategic trade control system in Hong Kong instituted under the IEO and its subsidiary legislation, the Import and Export (Strategic Commodities) Regulations. The C&ED ensures that the licensing system is not abused by illegal imports and exports by conducting intelligence-led inspections and verifications on import and export of strategic commodities and investigating cases of abuse.

3.35 The C&ED is also the proposed regulator responsible for registering as well as overseeing and monitoring the AML/CFT practices of dealers in precious metals and stones under AMLO to be amended (see section 6.6 under Chapter 6 for more details).

ICAC

3.36 The ICAC is primarily responsible for investigating corruption complaints. The financial aspect of corruption or related offences, including fund flow analysis and tracing of proceeds of crime, is encapsulated in investigation of the main offences. ML offences facilitated by or connected with corruption are pursued if revealed in the course of corruption investigations.

[64] Chapter 578 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap578

3.37 The ICAC has a dedicated Proceeds of Crime Section[65] that deals with the restraint and confiscation of assets under the OSCO, and a specialized Forensic Accounting Group[66] to support frontline officers in handling complex corruption cases, ML and other offences.

JFIU

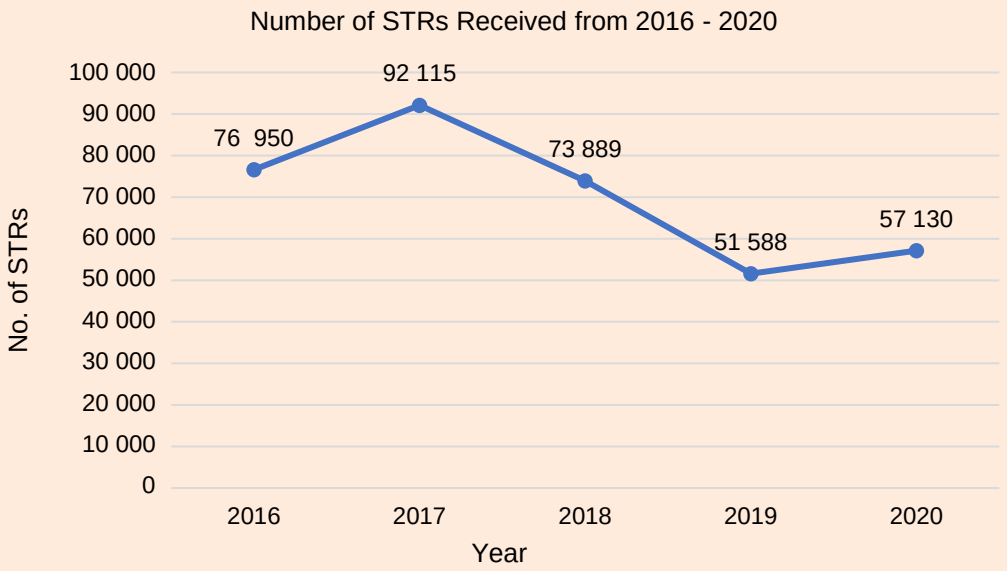
3.38 Having become one of the formations under the FIIB in June 2021, the JFIU continued to be the dedicated unit jointly operated by the HKPF and the C&ED to receive, analyse and disseminate STRs filed by FIs, DNFBPs and members of the public, and study typologies of ML and TF cases. On receipt of each STR, the JFIU will examine and conduct intelligence analysis in accordance with its risk-assessment mechanism, examining aspects of the report, including its degree of suspicion, severity and level of risk. Valuable intelligence from STRs is developed and/or disseminated to investigative units of LEAs or other agencies, enabling them to intervene and disrupt ML/TF activities, assisting investigations and leading to successful prosecutions. With enhanced manpower, the JFIU also conducts proactive intelligence gathering.

3.39 The number of STRs continued to increase and reached its peak in 2017, partly due to an improving AML/CFT compliance culture since implementation of the AMLO in 2012. The number then dropped to 51 588 in 2019 due to the enhancement of the quality of STRs through outreaching work. Numbers of so-called "super STRs", containing multiple data points, including hundreds of suspects, thousands of accounts and numerous transactions, have increased significantly as more sophisticated financial institutions have strengthened capabilities and better leveraged the use of technology. While containing a rich source of data, super STRs require extensive analysis to develop further intelligence for operational use. In 2020, the number of STRs increased to 57 130. With the rapid development of financial technology ("fintech") in Hong Kong, it is anticipated that STRs received will continue to grow alongside the increasing number of reporting entities including stored value facility operators, VBs, and VASPs. To keep pace with the technological advancement in FIs and ensure that the JFIU maintains sufficient capabilities of processing financial intelligence provided by its reporting entities, the JFIU is developing a Financial Data Analytic Platform ("FDAP"). Further details of the FDAP could be found in the "Next Step" section.

[65] This section has an establishment of one Chief Investigator, two Senior Investigators and two Assistant Investigators. The strength of staff deployed for asset tracing/ forfeiture may be subject to change depending on the workload.

[66] One Chief Forensic Accountant, two Senior Forensic Accountants and eight Forensic Accountants.

Figure 3.3: Number of STRs received by JFIU



Multi-agency approach and public-private partnership

3.40 Members of the CCC collaborate on various levels. Policy bureaux, in implementing the AML/CFT policy initiatives and taking forward legislative exercises under the direction of the CCC, consult relevant Government agencies and stakeholders in the community. Feedback from these engagements plays a vital role in shaping policies.

3.41 In 2014, a Memorandum of Understanding ("MOU") on supervisory and enforcement matters was signed among the relevant authorities under the AMLO (the HKMA, the SFC, the IA and the C&ED) to underpin the exchange of information ("EOI") and mutual assistance. Under the MOU, two coordination groups were established:

(a) The AML Regulation and Supervision Co-ordination Group is chaired by the FSTB and comprises the HKMA, the SFC, the IA and the C&ED as well as representatives from other agencies including the HKPF. The group's objectives include monitoring the operation of the AML/CFT regulatory regime for financial sectors and sharing information and insights on regulatory and supervisory issues of common concern. This group coordinates implementation of policies directed by the CCC, and

(b) The Anti-Money Laundering Regulatory Enforcement Co-ordination Group, comprising the HKMA, the SFC, the IA and the C&ED, who chair meetings in rotation. The FSTB joins as needed. There are regular meetings to share outcomes of AML/CFT investigations and enforcement actions.

3.42 The SFC signed MOUs with the HKPF and the ICAC in August 2017 and August 2019 respectively to formalise and strengthen cooperation which cover referral of cases, joint investigations, exchange and use of information, mutual provision of investigative assistance, to make the combating of financial crimes and illicit activities in the securities and futures markets more effective. Under the MOUs, the SFC has been conducting joint operations with the HKPF and the ICAC to tackle serious financial crimes in the securities and futures markets and related offences such as ML and fraud. The success is demonstrated in a number of operations conducted jointly by SFC and

HKPF/ICAC against market manipulation and other securities fraud and associated ML activities.

3.43 The HKPF, the C&ED and the ICAC cooperate closely on policy and operational matters, information sharing and intelligence. Under mechanisms and liaison channels provided for or permitted by law, investigative authorities are able to obtain financial information and intelligence from other authorities and mount joint operations to combat financial crime. Building on the experience of the 1st HRA and recommended action of the ME Report, the data collection mechanism amongst LEAs was enhanced and expanded in the 2nd HRA to ensure data is being continually and constantly monitored, tracked and updated. ML/TF related enforcement statistics, including investigations, prosecution, conviction, restraint and confiscation was regularly provided by LEAs and the Risk Assessment section of the FIIB being the central HRA data hub. The enhanced quantitative basis would ensure a more solid identification and assessment of ML/TF/PF risks and hence a more comprehensive and updated assessment product.

3.44 Established as a pilot project among the HKPF, the HKMA, the Hong Kong Association of Banks ("HKAB") and 10 local retail banks in May 2017, the FMLIT has been committed to fighting against financial crime and ML activities through strengthening its public-private-partnership model. Through regular meetings of the FMLIT's Strategic and Operations Groups, senior representatives formulate and adjust its directions, allowing professional fraud and ML investigators from the HKPF and the banking sector to work side by side in tackling serious financial crimes and ML activities. The FMLIT provides a formal structure for banks, regulatory authorities and LEAs to improve collective understanding of current and emerging threats, as well as sharing of intelligence, with a view to detecting, preventing and disrupting serious financial crimes and ML activities. Since FMLIT's establishment in May 2017, upon meetings and cooperation with the banking sector, as at the end of 2020, 299 culprits had been arrested in intelligence-led operations with HK$692 million of crime proceeds being prevented from being dissipated/restrained/confiscated, including HK$106 million on financial losses prevented. In addition, over 10 000 bank accounts previously unknown to LEAs were discovered through tactical intelligence exchange. Further details are featured in Chapter 5 in respect of the AML/CFT work of the banking sector.

Box 3.1 - Major developments of FMLIT over years: Strengthening public-private partnership

Expansion of Membership

FMLIT became a permanent establishment in June 2019. Taking on board the recommendation of FATF, its membership was extended to include the ICAC and the C&ED which helps strengthen members' investigative capability in the investigation of corruption and customs-related ML activities. Five additional local retail banks joined the FMLIT in 2020 while all eight virtual banks that commenced operation in Hong Kong have also been onboarded in 2021 to expand the scope of financial crime and market footprint covered. The current membership of FMLIT consists of the HKPF, the HKMA, the ICAC, the C&ED, the HKAB and 23 banks (including 15 local retail banks and 8 virtual banks) in Hong Kong.

A Centralised Liaison Point and Intelligence Platform

In order to maximize the reach of anti-deception and AML outreaching initiatives, the FMLIT has taken up the role as the centralised liaison point between the public (HKPF and HKMA) and private sector (member banks) to facilitate the dissemination of publicity materials produced by HKPF and HKMA to member banks for further publicising. In parallel, the FMLIT Secretariat also provides a centralised hub for receiving member banks' observations on emerging financial crime trends and ML typologies, which facilitates the production of more relevant and timely publicity materials to raise public awareness on topical financial crime risks.

FMLIT Alerts Function

The Alerts Function provides the infrastructure for the LEAs, regulatory authorities and member banks to co-author alerts on typologies, trends and topical issues. As at December 2021, the FMLIT Alerts Function has published 21 alerts covering a broad range of ML topics such as trade-based ML, money mule and mule account characteristics, ML risks associated with new payment methods ("NPMs"), COVID-19-related financial crime risk, etc. All FMLIT Alerts include indicators, red flags and mitigating measures, and are shared to all banks and SVF licensees, which facilitates them to enhance their system and control, and better mitigate financial crime risks.

Capacity Building

The FMLIT Secretariat also rolled out a pilot scheme to organise educational seminars and train-the-trainer workshops to personnel of banks with a view to promoting industry-wide awareness of latest financial crime trends, ML typologies, and enhancing detection and prevention of financial crime and ML activities by frontline bank staff, etc. FMLIT members are also actively discussing feasible and quantifiable measures of members' collective efforts on outreaching, capacity building and intelligence exchange, which paves way for developing a set of performance indicators to better reflect FMLIT's contributions in these aspects in the future.

Collaboration in Topical Subjects

FMLIT started a pilot project "AMLNet" to step up the intelligence exchange among all members against syndicated criminal networks involved in "Telephone Deception" crimes. Targeting money mules who set up bank accounts across different local retail banks for receiving and laundering crime proceeds of telephone and other deceptions, the FMLIT Secretariat took the lead in developing mule account networks based on an array of commonalities shared by these mule accounts.

To fully leverage the synergy created by the public-private partnership nature of FMLIT, member banks have played an active role in screening the involved money mules and mule accounts, identifying intra-bank level mule account networks using regulatory technology ("Regtech") or other analytics techniques, providing relevant intelligence to the FMLIT Secretariat and taking mitigating measures to impede the further use of mule accounts identified. Based on the intelligence received, the Secretariat threaded together the intra-bank level mule account networks provided by individual member banks into inter-bank level mule account networks, which enables coordinated enforcement and disruptive actions by law enforcement and FMLIT member banks and identification of over 400 bank accounts previously unknown to LEAs.

Following Regtech initiatives launched by the HKMA in 2019, increasing number of member banks have adopted more advanced AML/CFT Regtech for network analysis, as well as expanding the use of non-traditional data including digital footprints to identify hidden linkages and connected accounts. In this on-going process of co-developing large scale mule account networks, participating member banks proactively share the experience with one another in the identification and mitigation of mule account networks, such as during a sharing seminar organised by the HKMA on 2 December 2020 which has helped to accelerate adoption levels of Regtech across the industry and cultivate expertise on harnessing Regtech to identify syndicated ML activities.

3.45 Other mechanisms (regular or ad hoc) to ensure timely and effective cooperation in response to ML/TF threats and typologies include:

(a) The FSTB and the SB, with the FIIB, the financial and sectoral regulators or professional groups arrange outreach and capacity building programmes, such as seminars, for the financial sectors and DNFBPs on AML/CFT to share experience, information on risk and typologies and latest developments and promote CDD, record-keeping and STR, screening for TF and PF. For instance, the C&ED has launched a sector-wide outreach program for MSOs since May 2020. The outreach program aims to enhance MSOs' understanding of ML/TF risks and their AML/CFT obligations, in particular those related to TFS;

(b) The JFIU issues STR Quarterly Analysis to STR reporting entities to provide analysis and feedback on STRs and case typologies. Topical strategic analysis reports were also published by FIIB, for example on ML associated with email scams and SVF licensees, with a view to improving quality of information reported by entities, promoting intelligence exchange, triggering law enforcement actions and providing insights into formulation of AML/CFT regulations/policy. The HKPF also delivers seminars to FIs and DNFBPs, and liaises with financial regulators to share information about topical AML/CFT issues;

(c) The HKPF issues industry alerts and topical strategic analysis reports and meets regulators and sectoral stakeholders regularly to discuss the latest crime trends and provide updates on cases of interest and referrals via different platforms, for example, the FMLIT, the STR Working Group involving LEAs, regulators and major reporting entities and a Project e-GUARD launched by the CSTCB which aimed at protecting local small-and-medium-sized enterprises ("SMEs") against email scams through proactive prevention and investigations;

(d) The FSTB, financial regulators and LEAs have regular dialogue on policy and regulatory responses having regard the developments of VAs;

(e) As the supervisor of FMLIT member banks, the HKMA has undertaken a series of initiatives and thematic reviews to support FMLIT banks to share best practice, increase capacity and the use of technology, including network analytics and the use of external information and data, in order to strengthen intelligence being provided into the eco-system;

(f) On an on-going basis, the ICAC has been offering corruption prevention services and conducting ethics and anti-corruption training to local practitioners of high corruption/ ML risk sectors, including banks, insurance and listed companies, in addressing corruption/ ML threats;

Box 3.2 - ICAC: Focus on corruption prevention

The Community Relations Department ("CRD") of the ICAC has been offering corruption prevention services and conducting regular ethics and anti-corruption training for practitioners of high corruption/ML risk sectors including banks, insurance and listed companies through the arrangement of individual companies and professional organisations. To enhance the impact of AML messages, corruption risks related to ML were incorporated in regular training activities and other initiatives. In particular, the CRD has maintained a Corruption Prevention Network for Banks comprising about 230 managers from 85 banks/deposit taking companies. Regular e-newsletters were issued to Network members to provide up-to-date information pertaining to ethical and corruption risks. The CRD launched a two-year Ethics Promotion Campaign for the Insurance Industry in 2019, with the support of the IA and 12 industry bodies. Under the campaign, ICAC's corruption prevention services were offered to over 3 200 insurance-related companies in Hong Kong and more than 12 000 practitioners had attended ICAC's training.

The Corruption Prevention Department ("CPD") of the ICAC, inter alia, reviews the core work areas of regulators of the banking and insurance sectors as well as the securities market to ensure proper safeguards are in place in their regulatory and monitoring procedures. The CPD has developed various corruption prevention guides/toolkits illustrating the corruption risks and providing recommended safeguards for reference such as the "Bank on Integrity – A Practical Guide for Bank Managers", "Anti-corruption Programme – A Guide for Listed Companies" and "Corruption Prevention Guide for Insurance Companies". In addition, the CPD has established a designated group (Corruption Prevention Advisory Service) to provide free, tailor made and confidential corruption prevention services to private entities, including but not limited to individual banks, insurance-related companies and listed companies, upon their request, on their various operations and corruption prevention training to enhance their overall governance and corruption resistance in their operations.

(g) In view of the noticeable increase of deceptions and frauds as well as the associated ML risk, the HKPF established the Anti-Deception Coordination Centre ("ADCC") in July 2017 to step up actions against deception and enhance public awareness of various kinds of scams. Apart from the instant consultation telephone hotline service offered to the public and enhanced efforts in publicity and enforcement, the ADCC works together with the JFIU in strengthening cooperation with FIs, with a view to mitigating victims' loss and upholding the AML regime in Hong Kong. Specifically, the ADCC has been assuming the role of urgent liaison with local FIs on suspicious cases. Initial success has been noticed in the stop payment capacity of the ADCC. As at end 2021, the ADCC has intercepted HK$9.6 billion upon urgent liaisons with FIs in Hong Kong;

Box 3.3 - ADCC: Combating deception and frauds

24/7 Stop Payment Mechanism

Given the 24-hour nature of the online banking environment, the ADCC, with the

assistance of the HKMA and the HKAB, has established the round-the-clock contact channel with fourteen retail banks (including all eight VBs) for stop payment and intelligence exchange. The round-the-clock cooperation between banks and the ADCC addresses the changing landscape of payment services to an era of cross-platform instant e-payment. In 2021, the cooperation between the ADCC and the Hong Kong banking sector contributed to successful interception of funds involved in deception cases (included incoming request from Mainland and overseas proceed interception) of HK$2.21 billion.

International Stop Payment Mechanism

Regarding the ML threat arising from foreign crimes, the ADCC has established an International Stop Payment Mechanism with the support and collaboration of 12 jurisdictions and the Financial Crimes Unit ("FCU") of the International Criminal Police Organisation ("INTERPOL") in October 2019. The ADCC acts as the Force's focal point in engaging overseas LEAs for stop payment. Reciprocally, the INTERPOL and the overseas LEAs would also refer cases involving beneficiary accounts in Hong Kong to the ADCC for stopping the crime proceeds. The International Stop Payment Mechanism strengthens the capabilities of the ADCC to trace the illicit funds that dissipate to overseas bank accounts, at the same time, to stop the crime proceeds remitting from overseas to Hong Kong. As at end of 2021, the ADCC has processed the outgoing and incoming stop payment requests for over 1 300 cases, involving HK$6.3 billion crime proceeds. HK$2.9 billion out of HK$6.3 billion crime proceeds were being intercepted, with a successful rate of 45.7%.

Cryptocurrency Stop Payment Mechanism

In March 2021, ADCC and CSTCB jointly established a Cryptocurrency Stop Payment Mechanism in response to the increasing popularity of cryptocurrency trading and the potential risk that cryptocurrency might be exploited by criminals as a media to launder crime proceeds.

Capacity Building of the Stakeholders

The ADCC cooperates with all relevant stakeholders for formulating anti-deception and combating strategies with regard to the trend of topical scams. For example, the ADCC proactively has offered training to the frontline bank staff to introduce the modus operandi of latest prevalent scams, with a view to enhancing their capabilities of identifying the potential victims in bank branches. In 2021, there were 218 on-going deception cases, which were identified and halted by the frontline bank staff.

Publicity Outreach & Public Education

The ADCC oversees and coordinates all the publicity tasks of anti-deception in the HKPF. The ADCC closely monitors the deception trend, utilises all potential channels for anti-scam publicity and issues scam alerts. Looking forward, the ADCC will continuously monitor the crime trend and produce timely publicity materials to raise public awareness on scam and the topical financial crime risks.

Enhancement of coordination with compliance officers

The ADCC has been hosting meetings with the compliance officers of local retail banks including the eight VBs to share the situation of banks involved in scams and ML activities, to provide suggestions on AML measures and to encourage the better adoption of

Regtech solutions to prevent the banking services from being abused for illicit purposes and to support the risk management and compliance. Looking forward, the ADCC will continuously liaise with banks for the sharing of good practices.

(h) The CEDB convenes an inter-agency platform on implementation of UNSC sanctions against proliferation (including TFS), to share intelligence, discuss typologies, trends and cases, and coordinate government-wide actions and responses. Inter-agency meetings are attended by the FSTB, the SB, the HKPF, the C&ED, the CR, the Marine Department ("MD"), the TID and the HKMA on a regular basis and other co-opted members where needed. Follow-up actions, such as pursuing further investigation and enforcement, have been taken following the meetings, and alerts have been issued to the relevant trades to remind them of the need to comply with UNSC sanctions; and

(i) In response to reports about DPRK evading UNSC sanctions by allegedly using front companies based in Hong Kong, the HKPF and the CR collaborated closely in taking enforcement measures targeting the front companies and related company secretaries. In addition, CR has appointed a Police Liaison Officer to facilitate the liaison with the HKPF on ML/TF issues. With the intelligence shared by other agencies, the CR conducts enhanced checking and on-going monitoring of persons and entities involved. On a related note, the licensing regime for TCSPs came into operation on 1 March 2018 and the CR has established the Registry for Trust and Company Service Providers to administer the licensing regime and enforce the AML/CFT requirements of the AMLO for TCSPs (Details are found in Chapter 6).

Prosecution and Judicial Process

3.46 The Prosecutions Division of the DoJ provides legal advice to LEAs on their investigations, and generally exercises on behalf of the Secretary for Justice the discretion whether or not to bring criminal proceedings. Prosecution is initiated where the evidence demonstrates a reasonable prospect of conviction and that it is in the public interest to prosecute. ML offences can be tried summarily or on indictment.

3.47 All prosecutorial decisions are made strictly in accordance with the law, the Prosecution Code and admissible evidence. Prosecutors make decisions to prosecute or not independently. As noted in Chapter 1, the Basic Law guarantees the courts' exercise of judicial power independently, free from any interference.

3.48 The quality of prosecutions against ML/TF is backed by consistent and ongoing training for prosecutors. The DoJ continues to foster links with counterparts in other jurisdictions and participates in international conferences and events to keep prosecutors abreast of the latest developments in the AML/CFT regime.

Table 3.4: Number of ML Prosecutions (by case)

Year	2016	2017	2018	2019	2020
ML Prosecution	94	103	93	99	66

Table 3.5: Sentences of ML convictions (by person)

Year	2016	2017	2018	2019	2020
Non-custodial sentence	9	9	8	4	6
Custodial sentence : Under 24 months	62	50	33	51	32
Custodial sentence : 2 to 4 years	34	29	36	39	25
Custodial sentence : 4 to 6 years	2	5	7	7	2
Custodial sentence : Over 6 years	0	1	0	3	5

Table 3.6: Restraint and confiscation of crime proceeds

Year	2016	2017	2018	2019	2020
Number of restraint orders applied	29	31	47	32	29
Value of proceeds restrained (in HK$ million)	303	67	8,081	180	268
Number of confiscation orders applied	12	28	43	31	24
Value of proceeds confiscated (in HK$ million)	134	336	716	113	127

Note : One case in 2018 involved a restraint order for HK$7,300 million.

External and International Cooperation

3.49 Hong Kong has been assessed to have achieved a substantial level of effectiveness in the FATF 4th round ME in 2019. There have not been any substantial changes in the legal framework relating to international cooperation. Hong Kong recognises that effective international cooperation is essential in tracing crime proceeds, and uncovering the identity and background of criminals as ML often involves transnational crimes. As a member of the FATF, the APG, the INTERPOL, and the Egmont Group of Financial Intelligence Units ("FIUs") through the JFIU, Hong Kong participates in international efforts to combat ML and TF. Mechanisms are in place for providing assistance to other jurisdictions, including MLA, surrender of fugitive offenders, financial intelligence exchange, and cooperation among LEAs and financial regulators.

MLA and surrender of fugitive offenders

3.50 The Mutual Legal Assistance in Criminal Matters Ordinance ("MLAO")[67] provides a statutory framework for implementing bilateral agreements and multilateral conventions on MLA, enabling assistance to be provided to or obtained from foreign jurisdictions in the investigation and prosecution of criminal offences and ancillary criminal matters.

3.51 Hong Kong has signed bilateral MLA agreements with 33 jurisdictions[68], all of which contain provisions for tracing, restraining, confiscating and sharing proceeds of crime. In addition, 13 multilateral conventions targeting serious crimes which provide for mutual legal cooperation have been applied to Hong Kong, including the Palermo, Vienna and Merida Conventions. In the absence of applicable bilateral agreement or multilateral conventions, MLA may still be provided on the basis of a reciprocity undertaking provided by the requesting place.

3.52 Types of MLA that may be provided include taking of evidence and statements (including via a live television link), search and seizure, production of materials, facilitating travel of persons (in custody or otherwise) to provide assistance, confiscation of proceeds of crime (including freezing pending confiscation) and service of process.

3.53 Processing of incoming MLA requests involving non-urgent court applications was to some extent affected by the COVID-19 situation during end of January to May 2020 when the Judiciary generally adjourned court proceedings. Other aspects of request processing, which were conducted largely electronically remained unaffected during the said period. Further relevant details of the MLA requests in are shown below:

Table 3.7: MLA requests related to ML/TF and predicate offence

Year	2016	2017	2018	2019	2020
No. of MLA requests made	15	14	16	16	15
No. of MLA requests received[69]	339	342	377	414	301

3.54 The Fugitive Offenders Ordinance ("FOO")[70] permits the surrender from Hong Kong of persons wanted by foreign jurisdictions, either for prosecution or for the imposition or enforcement of a sentence, in respect of a broad range of offences against the laws of those places. Surrender is only permissible to places with which Hong Kong has an operative bilateral surrender of fugitive offenders agreement, or where there is a relevant multilateral convention applicable to Hong Kong, and subsidiary legislation is in place under the FOO to bring such an agreement into effect and to implement the extradition[71] provisions of such conventions. Hong Kong has signed bilateral surrender of fugitive

[67] Chapter 525 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap525

[68] Including agreements that are not yet in force or suspended. A current list of bilateral agreements in force can be found at http://www.doj.gov.hk/eng/laws/table3ti.html

[69] Some requests cannot be processed due to insufficient information provided in the request or a failure to meet minimum legal thresholds for processing etc.

[70] Chapter 503 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap503

[71] Extradition is known as "surrender of fugitive offenders" in the context of Hong Kong, China.

offender agreements with 20 jurisdictions and 14 multilateral conventions[72] which contain extradition provisions have been applied to Hong Kong.

MLA with other parts of PRC

3.55 The MLAO and the FOO do not apply to other parts of China, including the Mainland, Macao and Taiwan. Assistance for evidence-taking may be rendered to or sought from other parts of China on the basis of letters of request issued by the court and under Parts VIII and VIIIA of the Evidence Ordinance[73]. This is a court-to-court letter rogatory process and limited to the taking of evidence and production of documents. To date some requests from Hong Kong for taking of evidence in support of ML prosecutions have been successfully processed by the Mainland and Macao authorities, and Hong Kong has also processed requests from the Mainland and Macao. Hong Kong may also enforce external confiscation orders made in places designated under the Drug Trafficking (Recovery of Proceeds) (Designated Countries and Territories) Order[74] for recovery of proceeds of drug trafficking. One of the designated places listed in Schedule 1 to the Order is 'China (except Hong Kong)'.

Financial intelligence exchange

3.56 Under the OSCO, the DTROP and the UNATMO, the JFIU has the authority to exchange information with counterparts in other places without entering into MOUs. The signing of an MOU will be considered where the laws of a counterpart jurisdiction require an MOU for financial intelligence exchange. The JFIU has signed 16 bilateral agreements/MOUs with overseas FIUs and its Mainland and Macao counterparts[75].

[72] The abovementioned 13 multilateral conventions and the Convention on the Prevention and Punishment of the Crime of Genocide 1948.

[73] Chapter 8 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap8

[74] Chapter 405A of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap405A

[75] JFIU has signed 16 bilateral agreements/MOU with overseas FIUs and her mainland counterpart, including Australia (the Australian Transaction Report and Analysis Centre & the Australian Federal Police), Republic of Korea, Singapore, Cambodia, Canada, Japan, Malaysia, Poland, Panama, Russia, the Mainland China, Macao and the Republic of South Africa, to share financial intelligence.

Table 3.8: Financial intelligence exchanges by JFIU with Egmont Group and non-Egmont Group members

Year	2016	2017	2018	2019	2020
Incoming Requests & Spontaneous Exchanges (Egmont Group)	794	991	1 197	1 283	924
Incoming Requests & Spontaneous Exchanges (Non-Egmont Group)	43	154	123	209	177
Total Number of Correspondences	837	1 145	1 320	1 492	1 101
Outgoing Requests & Spontaneous Exchanges (Egmont Group)	866	990	1 036	1 135	933
Outgoing Requests & Spontaneous Exchanges (Non-Egmont Group)	293	358	290	243	330
Total Number of Correspondences	1 159	1 348	1 326	1 378	1 263

3.57 As a member of the Egmont Group, the JFIU works with FIUs worldwide to support cross- jurisdiction law enforcement and intelligence exchange. The number of information exchange by JFIU with over 160 FIU members in the Egmont Group have been on the rise. In addition, the JFIU provides assistance to overseas LEAs whenever appropriate. JFIU officers participate in the meetings and workshops of the FATF, the APG and the Egmont Group, with a view to exchanging financial intelligence and sharing experience. Despite the outbreak of the COVID-19 pandemic in 2020, representatives from the JFIU continued to extend its network and share insights with other jurisdictions into global ML/TF trend and ME preparation work through attending various conferences and meetings virtually.

External cooperation by LEAs

3.58 The HKPF is part of the INTERPOL. The Liaison Bureau ("LB") of HKPF, in its capacity as INTERPOL Hong Kong, a Sub-Bureau of INTERPOL Beijing, National Central Bureau China, is the point of communication between the HKPF and the other 194 member countries.

3.59 Intelligence exchanges occur regularly with the total number of requests made from overseas LEAs to LB being 6 105 between 2016 and 2020. LB makes extensive use of the round-the-clock e-mail system for secure communications to facilitate the fast and secure EOI. The rapid exchange of critical information in the case investigation enhances the effectiveness and efficiency of case enquiries in Hong Kong.

3.60 Each request is examined and indexed in LB, then the case is passed to the investigation team via the Electronic Liaison Information Timely Enquiry System ("ELITES").

Regular reviews are conducted by LB and replies are made as expediently as possible to the requesting overseas National Central Bureau. In urgent cases, the Electronic Liaison Information Timely Enquiry System referral is followed up with direct telephone conversation with the respective investigation team. In the most urgent cases, senior management from LB are involved in referring the case to the appropriate investigation team for immediate investigation. LB also maintains a close working relationship with overseas Liaison Officers posted to various consulates in Hong Kong as a conduit for the exchange of intelligence and information.

3.61 The C&ED participates in enforcement operations coordinated by the World Customs Organization and has entered into 27 Cooperative Arrangements/Agreements since May 1991 to promote international cooperation in the fight against contraventions of customs law. Under the above cooperation framework, the C&ED exchanges intelligence with counterparts for investigation of suspected customs crimes. The C&ED takes part in various international enforcement fora and participates in seminars and workshops on capacity-building, customs integrity, trade facilitation, AML, anti-drug trafficking, anti-piracy, environmental issues and global supply-chain security.

3.62 The ICAC has established direct liaison channels with a large number of overseas LEAs, and is a member of the Economic Crime Agencies Network (a global network of LEAs dealing with corruption and other economic crimes). The ICAC represents Hong Kong in the Law Enforcement Meeting of the Asian Development Bank - OECD Anti-Corruption Initiative for Asia and the Pacific, the International Association of Anti-Corruption Authorities ("IAACA"), and the Asia-Pacific Economic Cooperation Network of Anti-Corruption Authorities and Law Enforcement Agencies. In May 2019, the ICAC and the World Justice Project jointly hosted the 7th ICAC Symposium, which was attended by 500 eminent participants from over 50 jurisdictions. Following the symposium, the ICAC and IAACA jointly organised a training program, which included workshops on asset recovery, forensic accounting, computer forensics, corruption prevention and promoting/ upholding probity culture. The ICAC has established ties with about 60 countries for co-operation in anti-corruption capacity building and has provided training to about 1 000 graft fighters of different jurisdictions. The Commissioner of ICAC was elected the President of IAACA on 5 January 2022. ICAC is now playing a greater role in leading more than 140 anti-corruption agencies of signatory countries of the United Nations Convention Against Corruption to join efforts in fighting bribery and corruption which include related money laundering activities.

Regulators' external and international cooperation

3.63 The HKMA is a member of the Basel Committee on Banking Supervision and its AML/CFT Expert Group. The HKMA continues to participate actively in Hong Kong's representation at the FATF and the APG, co-chairing the Evaluations and Compliance Working Group of the FATF since February 2020. The HKMA also contributed three financial assessors for Mutual Evaluations, two reviewers for follow-up reviews and two experts for technical compliance re-rating reviews to the FATF and APG in the latest round of the peer review process.

3.64 The HKMA maintains close contacts with the People's Bank of China ("PBOC") and the China Banking and Insurance Regulatory Commission. Subsequent to the action plan set out in the 1st HRA, the HKMA has established a supervisory cooperation arrangement for prevention of ML/TF with the PBOC. MOUs or other formal arrangements

have been signed with 29 overseas banking supervisory authorities in 25 jurisdictions. These arrangements provide the formal framework, under which the HKMA and its counterparts agree to share and exchange, to the extent permitted by law, supervisory information (including AML/CFT matters) to assist in the supervision of banks, and to discuss matters of common interest. The HKMA continues to extend its cooperation with banking supervisors in other jurisdictions, including through college-of-supervisors meetings.

3.65 The SFC is a signatory to the IOSCO Multilateral Memorandum of Understanding, which is a global regulatory cooperation and information-sharing arrangement among securities regulators that facilitates cross-border enforcement against securities related misconduct. The SFC is also a signatory to the IOSCO Enhanced Multilateral Memorandum of Understanding, which provides additional cooperation tools to meet the challenges of combating financial misconduct in an increasingly complex, inter-connected and technology-driven global financial market[76]. IOSCO members regulate more than 95% of the world's securities markets in more than 115 jurisdictions[77]. In addition, the SFC has entered into bilateral arrangements with more than 50 overseas regulators for cooperation and EOI and participates in supervisory colleges in connection with the supervision and oversight of regulated entities that operate on a cross-border basis in Hong Kong and other jurisdictions.

3.66 The SFC collaborates closely with the China Securities Regulatory Commission, the PBOC, the State Administration of Foreign Exchange and China Banking and Insurance Regulatory Commission under bilateral agreements/arrangements for mutual regulatory assistance and the EOI.

3.67 The IA is a signatory to the International Association of Insurance Supervisors Multilateral Memorandum of Understanding, a global framework for cooperation and information exchange between insurance supervisors. It has also signed bilateral MOUs or other arrangements with insurance supervisors of 11 overseas jurisdictions for sharing of regulatory information. Cooperation and information exchange in respect of AML/CFT matters are covered under the aforesaid MOUs and arrangements.

3.68 The IA has signed a Cooperative Agreement on Insurance Supervision with the China Insurance Regulatory Commission to promote efficient, fair and stable insurance markets in Hong Kong and Mainland China, by providing a framework for cooperation, mutual understanding, EOI and assistance. The Trilateral Cooperative Agreement on Anti-insurance Fraud signed with the China Insurance Regulatory Commission and the Monetary Authority of Macao enables the provision of assistance and information sharing among the signatories.

3.69 To strengthen international supervisory cooperation in the insurance industry for effective group-wide supervision of multinational insurance groups, supervisory colleges

[76] Under the IOSCO Enhanced Multilateral Memorandum of Understanding's framework, securities regulators can obtain and share audit working papers, telephone and internet records, compel attendance at interviews and provide guidance on freezing of assets.

[77] The SFC also participated in the work of the IOSCO Asia-Pacific Regional Committee on monitoring extraterritorial rulemaking, strengthening regional enforcement and supervisory cooperation, and mapping regional regulatory frameworks for CISs.

are organised by relevant group-wide supervisors with the participation of other insurance supervisors of jurisdictions where such groups have operations. Supervisory colleges cover AML/CFT controls, which allow supervisors to share inspection findings and regulatory concerns, with a view to identifying and addressing group weaknesses. In the past years, the IA held group-wide as well as regional supervisory colleges in Hong Kong where involved overseas insurance supervisors participated. The IA also attended supervisory colleges hosted by various group-wide supervisors overseas. Meanwhile, AML/CFT matters are also discussed in the Joint Meeting of the Insurance Regulators of Guangdong, Hong Kong, Macao and Shenzhen held on a regular basis.

3.70 The C&ED liaises closely with financial regulators in other jurisdictions including the HM Revenue and Customs of the United Kingdom and Monetary Authority of Singapore in intelligence sharing, supervision of international MSO groups as well as to enhance mutual collaboration in combating ML/TF related activities.

Next Steps

3.71 Hong Kong's ability to combat ML and TF is high, characterised by a sound legal framework, high-level commitment, a multi-agency AML/CFT institutional framework, rigorous law enforcement with LEAs of high capability and integrity, a fair prosecution and judicial system, and effective external and international cooperation. That said, there is room for enhancement in some areas:

(a) **Enhancing the AML/CFT legal framework** under the AMLO through –

i. Introduction of a licensing regime for VASPs, whereby any person seeking to conduct the regulated business of VA trading platforms in Hong Kong will be required to apply for a licence from the SFC subject to the meeting of a fit-and-proper test, with licensed VASPs being subject to the AML/CFT requirements under Schedule 2 to the AMLO and other regulatory requirements for market integrity and investor protection purposes; and

ii. Introduction of a registration regime for DPMS, whereby any person seeking to conduct the business of dealing in precious metals, precious stones, precious products, or precious-asset-based instruments in Hong Kong will be required to

register with the CCE, with those seeking to engage in cash transactions at or above HK$120,000 during their course of business to be subject to the AML/CFT requirements under Schedule 2 to the AMLO, in addition to meeting a fit-and-proper test for registration.

(b) **Making use of technologies:** Our LEAs and regulators will make use of technologies to detect ML/TF risks and improve their supervisory or operational efficiency. For instance, the HKPF is developing a FDAP which will be equipped with data processing and analytic capabilities to employ advanced technologies such as data mining, machine learning and artificial intelligence to support the FIIB's analytical work and information dissemination.

Similarly, the HKMA is implementing an AML/CFT Surveillance Capability Enhancement Project to strengthen the use of data and supervisory technologies to enhance its monitoring and understanding of emerging risks so that AML/CFT supervision is more effectively targeted to high risk institutions and activities. Moreover, through a number of initiatives, the HKMA has been proactively supporting adoption of AML/CFT Regtech by banks and SVF licensees to enhance AML/CFT surveillance and analysis. The SFC has also launched a Market Intelligence Programme under which technologies were adopted to enhance the ability to identify key conduct risks in the Hong Kong financial markets.

Box 3.4 - Other examples of the use of technologies in enforcement

Bank Document Digitisation System ("BDDS")
In August 2019, the HKPF launched the pilot scheme of the BDDS with the three note-issuing banks. Under the BDDS, the participating bank will provide electronic bank records, upon receipt of search warrants or production orders in digital format from investigation units via the system. In addition, all eight VBs joined the BDDS in January 2021. With the support of the HKMA and the HKAB in promoting the use of BDDS in the banking sector, six additional banks have expressed their interest in joining and the HKPF is liaising with them on participation. The use of BDDS can enhance the efficiency of data collection and analysis.

Cryptocurrency stop-payment and fund flow analysis mechanism
Under the mechanism, once the crime proceeds are identified to have directed to the cryptocurrency exchange platform, request of stop-payment and subscriber check will be made to that platform regardless of the registered country where the platform is based. The subscriber details and stop-payment can be done even the exchange platforms are out of Hong Kong. By the end of 2021, 738 stop-payment requests were being processed with a total of HKD 29.3 million worth cryptocurrency frozen, thereby enabling the victims to liaise with respective platforms on the recovery of proceeds via civil proceedings.

(c) **Strengthening AML/CFT Partnerships including public-private partnership:** Further initiatives will be developed to enhance public-private partnerships. For example, the HKPF launched the Project e-GUARD to protect the local SMEs against email scams through proactive prevention and investigations. The University of Hong Kong was also engaged to jointly develop a software named "V@nguard" to assist local SMEs in screening out fraudster emails in their daily business activities. Adopting

a phased approach on expansion, FMLIT is committed to further expanding its membership to other local retail banks, LEAs and SVF licensees.

(d) **Capacity building:** Specialised training would continue to be provided to frontline officers and other LEAs with a view to boosting their knowledge of financial investigation, management of financial intelligence as well as asset recovery procedures. For instance, to keep pace with the emerging trends, the HKPF has incorporated cryptocurrency training into various existing capacity building programmes to develop officers' knowledge and technical capabilities to tackle the cryptocurrency-related crime effectively. In addition, topics on the formal MLA and surrender of fugitive offenders regimes have been included in the training programmes for staff of LEAs and DoJ (in particular the Prosecution Division) to enhance awareness and understanding on the general use of the formal regimes to pursue evidence, asset recovery and fugitive offenders overseas.

(e) **Outreaching, publicity and education:** The Government and all relevant agencies will continue to conduct theme-based outreach activities to enhance the capacities of reporting entities.

(f) **Strengthening external and international cooperation:** Our LEAs will continue to cooperate with LEAs of the Mainland China and other overseas jurisdictions to combat cross-boundary crime syndicate and the associated ML activities. We will continue to exchange experience and international best practices in investigation of financial crimes and asset recovery with our counterparts. Looking forward, the HKPF will continuously liaise with INTERPOL and the overseas LEAs for the better understanding of the asset recovery system and legal frameworks in different jurisdictions, with a view to optimizing the operation and development of International Stop Payment Mechanism.

CHAPTER 4

MONEY LAUNDERING THREAT

Overview

4.1 This Chapter provides an update on the major ML threats of Hong Kong, covering over 9 000 ML investigation, conviction, restraint and confiscation cases from all LEAs [78] in 2016-2020. The assessment takes into account updated statistics and information between 2016 and 2020, including the number of reports emanating from different predicate crimes; the magnitude of proceeds generated; the scope, complexity and sophistication of ML; and the impact of predicate crimes on the social, legal and economic development of Hong Kong.

4.2 A comprehensive scoping exercise was conducted as part of the assessment to identify the major predicate offences for in-depth analysis, taking into account four factors, namely (i) prevalence of the offence; (ii) likelihood to generate crime proceeds; (iii) magnitude of proceeds generated; and (iv) other relevant factors in the international/regional context. Fourteen types of crime were identified for in-depth analysis in the 2nd HRA.

4.3 In terms of the overall assessment, the local crime rate has remained at a low level since the last HRA report, though the forms in which predicate offences are committed have seen changes. In particular, it is observed that for both domestic and external crimes, predicate offences involving the use of the Internet, email, and social media are increasingly common due to the advancement of technology, the prevalence of electronic financial services, and social distancing measures arising from the COVID-19 pandemic. Further, given Hong Kong's status as an international financial centre and trading hub, it is observed that Hong Kong continues to be exposed to both external and internal ML threats, in particular transnational/cross-border ML syndicates, given its status as an international finance, trade and transportation centre. Moreover, transnational criminals are in general more sophisticated in the ML methods they employ. This Chapter analyses the different forms of predicate offences observed and the techniques deployed by domestic and transnational criminals.

[78] HKPF, C&ED, ICAC and IMMD.

Major Predicate Offences

Figure 4.1: Breakdown of ML Investigations initiated in 2016-2020 by predicate offences

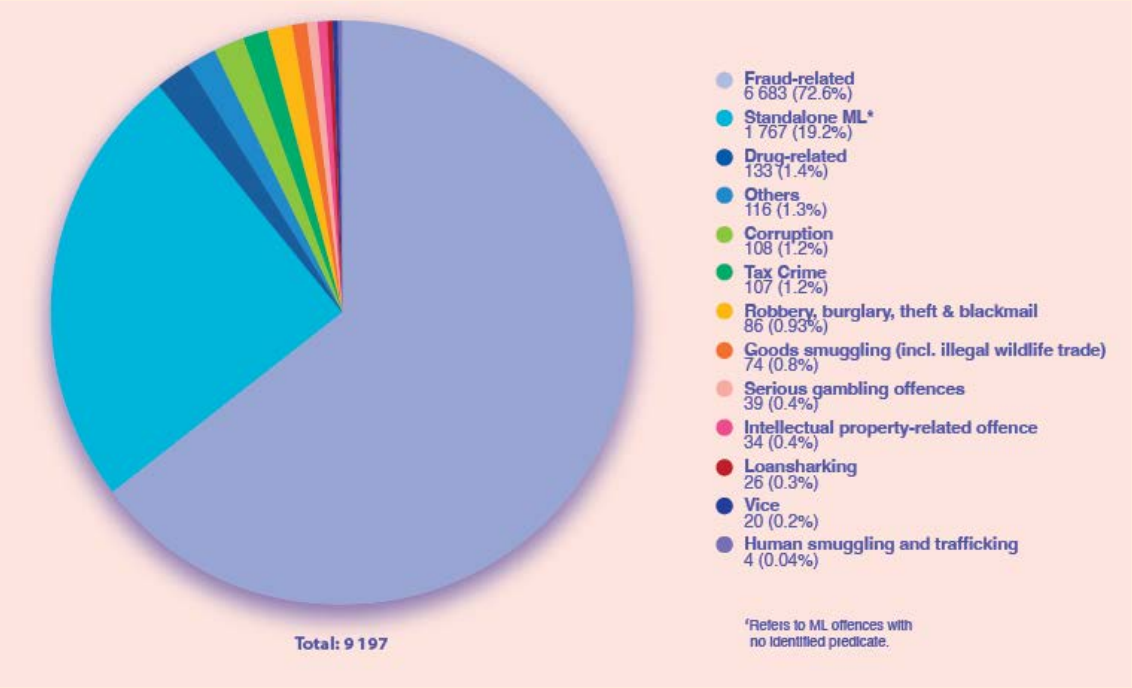


Figure 4.2: Breakdown of ML conviction initiated in 2016-2020 by predicate offences

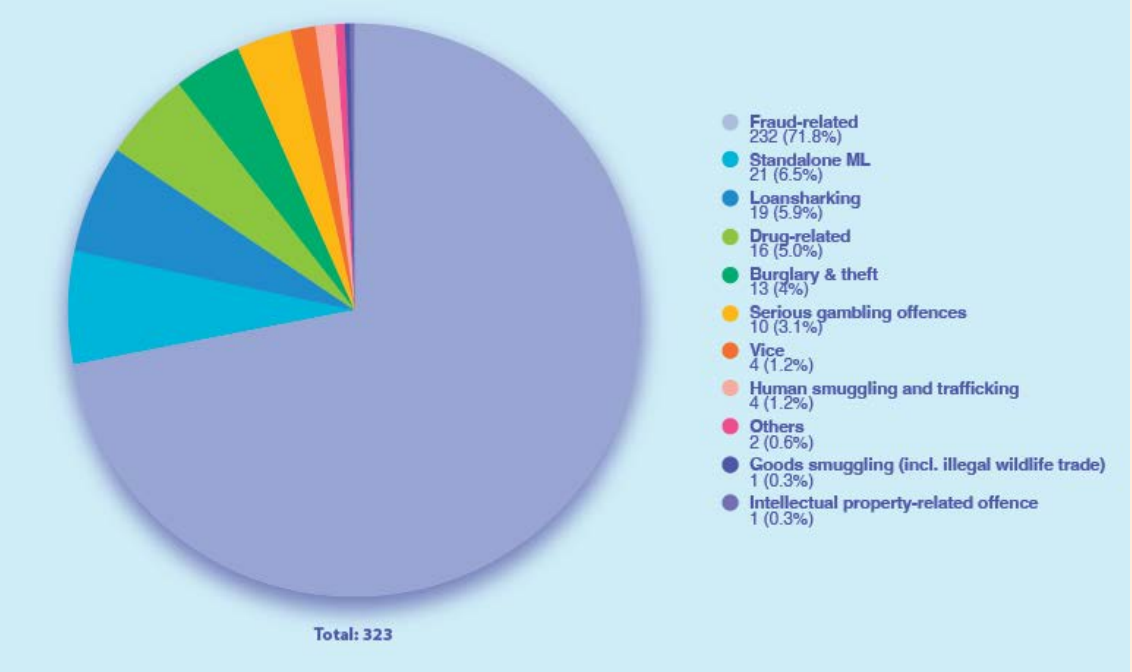


Figure 4.3: Breakdown of assets restrained in 2016-2020 by predicate offences (HK$ in million)

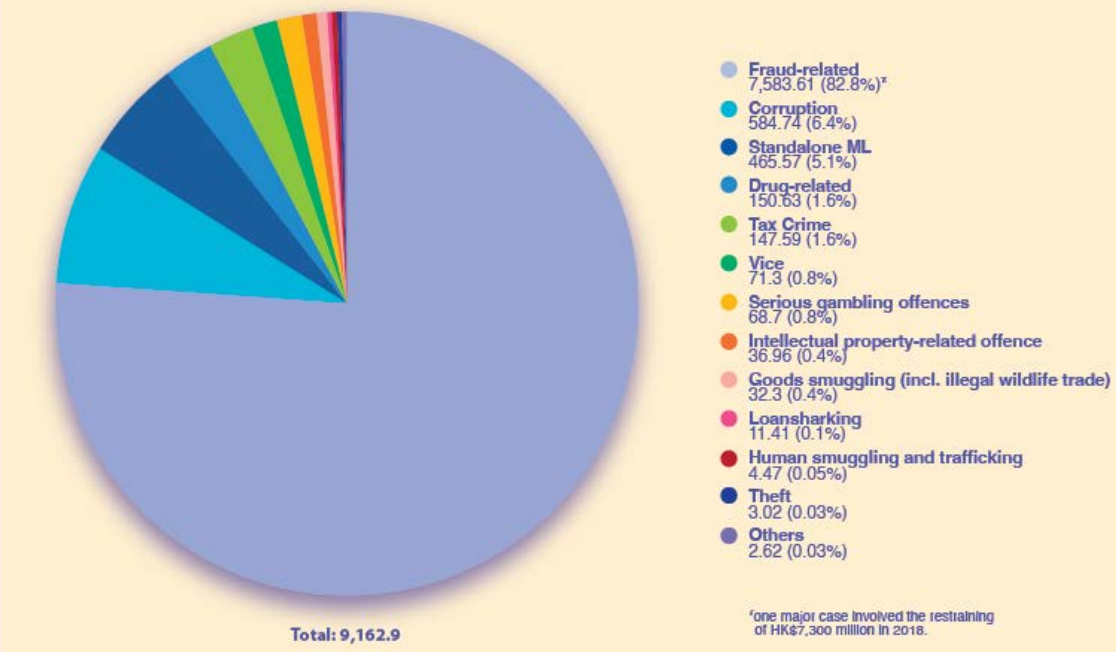
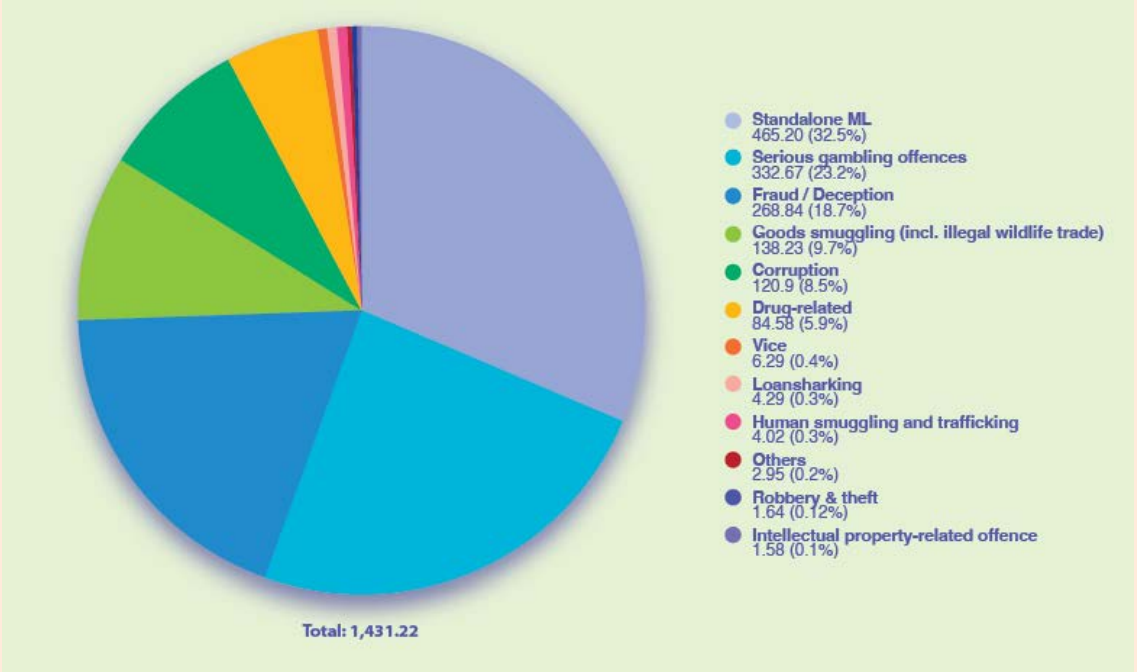


Figure 4.4: Breakdown of assets confiscated in 2016-2020 by predicate offences (HK$ in million)



4.4 Figures 4.1 - 4.4 provide a breakdown of identified predicate offences associated with the ML investigations, convicted ML cases, property subject to restraint and confiscation between 2016 and 2020. Around 47% were domestic predicate offences and 51% originated outside Hong Kong (other 2% with unknown sources) which corroborated with the cross-border elements often observed in certain predicate offences.

4.5 Based on the data in 2016 - 2020, there was no significant change observed in the ML threat portfolio of Hong Kong when compared with the 1st HRA. As presented in Figure 3.2 of Chapter 3, in terms of caseload, ML investigations showed a gradual increase from 2016 to 2018 as the LEAs strengthened their enforcement efforts. A brief drop in the number of ML investigations was observed in 2019, while the increased figure in 2020 could be partly attributed to the increased online transactions due to social distancing under COVID-19 pandemic coupled with the abuse of new financial services provided by VBs and SVF licensees as well as technological development in relation to VAs for committing ML. In terms of the typology of predicate offences, fraud-related crime continued to be most common both in terms of the number of investigations/convictions and, the crime proceeds involved. It was thus considered the most significant threat, followed by drug-related offences. Other predicate offences, including foreign tax and foreign corruption, which continued to be major global and regional concerns, were also assigned a higher threat rating, though our statistics indicated that the situation in Hong Kong has remained stable. Assessment on emerging regional threats such as human smuggling/trafficking and illegal wildlife trade have also been conducted, though the findings indicated that these offences posed only a limited threat to Hong Kong.

Fraud-related crime

4.6 Fraud-related crime encompasses a variety of criminal activities. Fraud-related crime accounts for almost 16% of total number of reported crime cases in Hong Kong from 2016 to 2020, the largest share of reported crime portfolio during the period. Study of cases between 2016 and 2020 revealed the following types of major fraud related-predicate crime –

(a) Online business fraud, e.g. e-shopping fraud and online commercial fraud;

(b) Email scam (both business and personal), e.g. hacking and pretence;

(c) Social media deception, e.g. romance scam, compensated dating scam;

(d) Online miscellaneous fraud, e.g. bogus investment plan, online employment scam; and

(e) Telephone deception, e.g. ‘Pretend Government Officials’, ‘Guess Who’ and ‘Detained Son’ scam.

4.7 It is observed that criminals have been taking advantage of the online platform to conduct fraud-related crimes, probably due to its ease of accessibility, broad coverage of users and anonymity. The COVID-19 has reinforced this trend as many businesses and individuals have shifted their daily activities to the online space. Given the high caseload and need for offenders to launder the proceeds, fraud cases accounted for a significant portion of Hong Kong’s ML risks. Analysis of ML investigations commenced between 2016 and 2020 revealed that fraud-related crimes took up the majority (about 70%) of the identified predicate crimes. Domestic fraud offences mainly encompass telephone deception, online business fraud, email scams and social media fraud, whereas external fraud offences mainly concern online fraud, telephone deception and investment fraud. The ratio of domestic fraud-related offences to external fraud-related offences account is about

40:60. The amount of proceeds involved in external foreign fraud-related crime is of much larger size. Among the convicted ML cases, fraud-related crime takes up a substantial percentage in the number of cases and proceeds involved from 2016 to 2020. For example, 80.6% of property restrained and 18.8% of property confiscated between 2016 and 2020 were proceeds connected to fraud-related offences. The ratio of convicted ML cases with domestic and foreign fraud cases was similar. Still, the amount involved in the domestic fraud-related predicate was more substantial than the foreign fraud-related predicate.

4.8 According to past experience, use of individual and corporate stooge accounts are in fraud-related crimes, with one hallmark sign being the deposit of large sums which is often quickly followed by withdrawals to overseas third parties which have no apparent relation with the depositor. For domestic fraud-related crimes, the principal offenders would either deal with the proceeds through stooges, associates or even family members. In external fraud cases, stooge accounts are used by cross-border syndicates to move money across the globe. The entry of new institutions such as SVF licensees and VBs in recent years, and technological advances such as the Faster Payment System ("FPS"), while facilitating faster and more convenient services for legitimate customers, have also attracted attempts to exploit these services for the transfer of illicit funds. Meanwhile, the emergence and more widespread adoption of VAs represent an emerging threat. As victims of fraud-related crimes usually became aware of and reported the scams only at a late stage, after the proceeds had been dissipated to other jurisdictions, a major consideration in combatting fraud case therefore lies with crime prevention and early intervention. Some of the measures taken by LEAs in fraud crime prevention has been described in Chapter 3, while risk-mitigating measures and the HKMA's supervision of the banking and SVF sectors are described in Chapter 5.

Drugs

4.9 Drugs are primarily manufactured outside Hong Kong and smuggled into Hong Kong by air, sea or mail. The criminal structure of drug trafficking varies from retail-level traffickers to syndicates with layers of management, such as brokerage, logistics, and drug couriers. Some of the drugs smuggled into Hong Kong are for re-export to other jurisdictions. The detected cases revealed that destination jurisdictions include Australia, Japan, New Zealand, Malaysia, Philippines, United States, etc. In combating drug trafficking activities, the HKPF and C&ED have coordinated with LEAs outside Hong Kong in interdicting the source of drugs. The effort has yielded significant results, leading to the seizure of a considerable amount of drugs and drug proceeds and the dismantling of a number of drug cartels in recent years.

4.10 Due to the COVID-19 pandemic, various jurisdictions have imposed travel restrictions, leading to a reduction in passenger travel. Given this development, drug traffickers have made more use of air and sea freight in larger quantities and postal parcels. With strengthened intelligence analysis and enhanced law enforcement action, LEAs successfully seized approximately 5 600 kg of drugs in 2020, an increase of 75% compared to 2019.

4.11 From ML convictions between 2016 and 2020, dangerous drug-related offences took up a relatively steady proportion of the identified predicate crimes. Such cases accounted for 5% in terms of case number and around 4% in terms of the amount involved. In terms of assets restrained and confiscated in 2016-2020, a moderate amount of restrained (1.7%) and confiscated (5.9%) assets were connected to dangerous drug-related offences. There were ten convicted cases on ML outside Hong Kong and six domestic convicted ML cases in the period. No significant change is observed in the ML techniques. Local drug syndicates' ML techniques are comparatively simple. They often deal with the proceeds by drug syndicates, their family members or associates, usually stored as cash or in family members' or associates' bank accounts, or used to acquire real estate. Proceeds were often deposited into bank accounts in batches of cash to conceal

the source of funds and break the audit trail. For international drug cartels, in addition to using local bank accounts opened by stooges and shell companies to launder proceeds, techniques like trade-based money laundering ("TBML") continued to be observed.

Tax crime

4.12 Hong Kong has a low and simple tax regime. Thus, tax evasion cases are limited, with most domestic tax-related offences involving late or non-submission of tax returns which pose negligible ML threat. In contrast, external tax evasion continues to pose a higher ML threat to Hong Kong.

4.13 Internationally, tax crime has long been an issue of concern and is a significant component of global illicit financial flows. A study of the OECD estimated that tax evasion has resulted in billions of annual revenue losses to different world economies. Various super-national organisations[79] have been conducting studies on various topics related to combating tax crimes and the related ML activities. Tax crime has also been frequently mentioned in APG Typologies Report 2016-2020 as a predicate offence in various jurisdictions in the Asia-Pacific Region. Transnational elements are often observed where proceeds of tax evasion were transferred to other jurisdictions through channels such as remittance and shell companies. In addition, many overseas' National RA/ME Reports of APG jurisdictions have identified tax crimes as primary proceeds/ML generating predicate offences with a relatively higher ML threat.

4.14 The contrast between domestic and external tax crimes can be seen from enforcement statistics. Between 2016 and 2020, the HKPF conducted 79 ML investigations associated with tax crimes, with over 98% of these cases related to tax crime occurring outside Hong Kong. Similarly, the C&ED undertook several tax crime-related ML investigations, with the majority being foreign cases and some involving considerable crime proceeds. Concerning property subject to restraint order, 1.6% of the property was connected to tax crime, which all related to foreign tax crime amounting to around HK$148 million.

4.15 MLA requests from overseas relating to tax crime are common. Between 2016 and 2020, 9.3% of incoming requests received were related to tax crime. The IRD is obliged to assist overseas tax authorities in obtaining information for their investigation of tax cases, including tax evasion cases, upon receipt of EOI requests under the relevant bilateral/multilateral tax arrangements. The tax purposes for which the incoming EOI requests were made included (i) determination, assessment and collection of taxes; (ii) recovery and enforcement of tax claims; and (iii) investigation or prosecution of tax matters. Examples of foreign tax evasion in the incoming EOI requests are non-reporting of offshore income and assets, deductions for unjustified payments and value-added tax fraud. Since 2018, the IRD has also conducted AEOI with tax authorities of appropriate partner jurisdictions annually to fight against cross-border tax evasion. In a case involving external tax evasion, nationals of a European jurisdiction were arrested for smuggling luxury items from Hong Kong in their homeland. The investigation by the HKPF revealed that the subjects exploited both corporate and personal bank accounts to receive and launder the proceeds.

[79] Including the FATF, OECD, the United Nations, the Europol, the Wolfsberg Group, etc.

Box 4.1 - Enhancing tax transparency and combating tax evasion

As an international financial centre and a responsible member of the international community, Hong Kong has all along been supportive of international efforts to enhance tax transparency and combat tax evasion. We have in recent years implemented a number of international tax initiatives, including a package of measures to counter Base Erosion and Profit Shifting ("BEPS") and AEOI. The Convention on Mutual Administrative Assistance in Tax Matters ("Convention") entered into force in Hong Kong on 1 September 2018. Since then, Hong Kong can ride on a multilateral platform under the Convention to implement various forms of administrative cooperation in assessing and collecting taxes, including EOI on request and AEOI.

In 2016, Hong Kong committed to implementing the four minimum standards of the BEPS package[80] promulgated by the OECD. The Inland Revenue Ordinance ("IRO") was amended in 2018 to implement specific measures under the BEPS package and codify transfer pricing principles into the tax law. To meet the international standards on countering BEPS, Hong Kong will implement the Multilateral Convention to Implement Tax Treaty Related Measures to Prevent Base Erosion and Profit Shifting for modifying the application of the comprehensive avoidance of double taxation agreements of Hong Kong in a swift and synchronised manner after completing the relevant legislative procedures.

Hong Kong is also committed to implementing the standard on AEOI promulgated by the OECD. The IRO was amended in 2016 to put in place a legal framework for Hong Kong to implement AEOI. Since the Convention came into force in Hong Kong on 1 September 2018, Hong Kong has taken a multilateral approach in implementing AEOI and exchanging information with a vast network of appropriate partner jurisdictions annually. Hong Kong smoothly conducted the first, second, third and fourth rounds of AEOI with other jurisdictions in 2018, 2019, 2020 and 2021.

Corruption

4.16 The domestic corruption situation in Hong Kong has remained stable. The number of corruption cases (excluding election-related complaints) in Hong Kong continues to decrease, sustaining the downward trend between 2011 and 2016. Corruption complaints against private sectors accounted for around two-thirds of the total complaints from 2016 to 2020. Annual community-wide opinion surveys conducted by ICAC revealed that, on average, 98.5% of the respondents had not come across corruption between 2016 and 2020.

4.17 Externally, corruption and associated ML activities have long been a global concern. According to some international and regional organisations' publications, Hong Kong faces an inherent ML threat posed by external corruption activities, particularly those occurring in neighbouring jurisdictions within the Asia-Pacific region[81]. These jurisdictions all highlighted corruption as a higher ML threat component. As an international financial

[80] The four minimum standards are countering harmful tax practices, preventing treaty abuse, imposing country-by-country reporting requirement and improving cross-border dispute resolution mechanism.

[81] APG Yearly Typologies Report (2016-2020). http://www.apgml.org/methods-and-trends/page.aspx?p=8d052c1c-b9b8-45e5-9380-29d5aa129f45

centre with a free and open economy, Hong Kong might also attract foreign business entities and officials seeking to launder the proceeds of corruption.

4.18 ML investigations initiated by HKPF and ICAC between 2016 and 2020 revealed that corruption-related offences accounted for a small percentage of the overall number of ML investigations during the same period. There has been no conviction associated with corruption-related ML cases between 2016 and 2020. The corruption-related MLA requests of ML/TF investigations accounted for 4.6% of all incoming requests . The high number of incoming requests indicates a coherence to the ML threat arising from external corruption in Hong Kong.

4.19 The complexity of corruption cases varied. Corrupt officials often use professional facilitators such as lawyers, accountants, real estate agents and TCSPs to launder illicit funds. In the study of ML cases arising from external corruption, exploitation of corporate structures was observed, which enabled corrupt officials to distance themselves from illicit funds. The use of multiple sectors such as banking and securities was also observed in some professional fraud and ML cases.

Box 4.2 - Foreign Corruption and Domestic ML

A merchant (Mr A) in Jurisdiction A, registered two shell companies in Hong Kong in 2007 and later obtained development rights to a Special Economic Zone in a South Asian jurisdiction. Mr A and his family were alleged to facilitate ML and bribery, among other offences. The financial investigation commenced against Mr A and his family and revealed that they had used over ten bank accounts to channel over HKD 120 million of crime proceeds. The company secretary of the shell companies and the nephew of Mr A's wife were arrested in Hong Kong.

Serious gambling offences

4.20 The number of reports related to serious gambling offences [82] remained constant from 2016 to 2020. Gambling seizure figures revealed that serious gambling offences had steadily generated substantial crime proceeds.

4.21 There has been a change in the operation of bookmaking activities in recent years. With the advancement of mobile technology and the Internet, illegal bookmaking in Hong Kong often takes the form of receiving bets locally and putting the actual operation base and servers outside the city. Bookmakers usually take bets for both horse racing and soccer matches. Soccer bookmaking activities are more prevalent when there are significant events held. The threat posed by illegal bookmaking on horse racing exists but is relatively minimal compared to soccer betting. Inter-bank transfers and personal bank accounts (typically stooge accounts) continued to be commonly used to receive proceeds. Proceeds integrated into stock trading accounts through banks or securities firms and cash seized from the arrest of suspects were also occasionally seen. In some recent cases, services of SVF licensees and VBs were exploited by bookmaking syndicates in the receipt/dissipation of proceeds, the characteristics of which were shared with banking and SVF sectors through a FMLIT alert developed by a VB. A cross-boundary element is also observed. From time to time, joint operations were conducted by the HKPF and the Mainland Public Security Bureau to combat cross-boundary bookmaking syndicates. For

[82] Serious gambling offences include bookmaking, operating or managing an unlawful gambling establishment, promotion of lotteries, providing money for unlawful gambling or an unlawful lottery, owner permitting/letting premises for use as an unlawful gambling establishment and cheating at gambling, under Cap.148 s5, s7, s9, s14-s16.

gambling activities without the mobile or Internet element, most gambling establishments are organised on a syndicated basis, which mainly operates unlawful mahjong gambling activities or gaming machines. Amongst the persons arrested for operating or managing / owner permitting/letting premises for use as an illegal gambling establishment, around 24% were found to have a triad background.

4.22 Serious gambling offences took up a small percentage of the identified predicate crimes in the analysed ML cases from 2016 to 2020. Though the majority (over 80%) of these crimes were committed domestically, the proceeds that stemmed from serious foreign gambling offences were much more considerable than domestic ones. In convicted ML cases, cases connected to serious gambling offences took up around 3.1% of all convicted cases between 2016 and 2020, with the majority belonging to domestic cases. However, in terms of funds involved, serious gambling offences took up a substantial share of proceeds involved in convicted ML cases in the same period, which amounted to around 9.49% of proceeds involved in all ML convicted cases. The amount in value of proceeds associated with external cases was about four times that of domestic cases. In the analysis on assets restrained between 2016 and 2020, the amount tied with serious gambling offences accounted for 0.75% (i.e. HKD 68.7 million), and all such cases are related to bookmaking. In contrast, the amount confiscated accounted for a relatively large proportion, about 23.24% (i.e. HKD 332.7 million) of the total amount, with over 90% being connected to external gambling offences.

Goods smuggling

4.23 Hong Kong has one of the world's busiest ports. According to the World Trade Organization, Hong Kong ranked 8th in terms of total trade in 2019 World Merchandise Trade (including imports, exports, domestic exports and re-exports). In Hong Kong, smuggled items detected include dutiable commodities, dangerous drugs, wildlife, firearms, infringing copyright articles, goods bearing forged trademarks, goods with false trade origin descriptions, and high-valued general merchandise. Between 2016 and 2021, the number of cases associated with unmanifested cargo ranged from 173 to 233, while the value of property seized varied from HKD 417 million to HKD 2,344 million per annum. The outbreak of the COVID-19 pandemic has had a significant impact on the logistics industry. The volume of cargo transportation by land reduced in 2020, and correspondingly most smuggling activities shifted from land to sea.

4.24 Given the differences in the tax and quarantine regimes between the Mainland and Hong Kong, most smuggling cases are related to items smuggled across the boundary between the two places. Commodities commonly involved include mobile phones and accessories, digital cameras and devices, computers and accessories, luxury goods, dried seafood and frozen meat, etc. Items smuggled to Hong Kong include dutiable cigarettes and counterfeit articles. In respect of maritime-based smuggling, the use of high-powered speedboats is a prevalent channel. To combat cross-boundary smuggling activities, the C&ED and the HKPF have been collaborating with the Mainland counterparts, including the Mainland Customs and China Coast Guard, and overseas LEAs in intelligence exchange and joint operations.

4.25 Between 2016 and 2020, 25.8% of the overall financial investigation cases conducted by the C&ED were related to goods smuggling identified as predicate crimes. As regards the convicted ML cases, there was one case related to goods smuggling offences, accounting for 0.3% of the convicted cases. The substantial proportion of convicted ML cases are on other predicate offences such as fraud. As to the analysis on assets being restrained or confiscated between 2016 and 2020, the amount restrained from goods smuggling-related crimes accounted for 0.35% of the total amount restrained, while the amount confiscated from the related offences accounted for 9.7% of the total amount confiscated.

Illegal wildlife trade

4.26 The United Nations identify illegal wildlife trade as a "global threat" that has links with other organised crimes such as modern slavery, drug trafficking and arms trade. According to the United Nations Environment Program-INTERPOL Report, the trade is estimated to generate revenues of up to US$23 billion a year[83].

4.27 Hong Kong is rarely the source or destination for illegal wildlife trade. However, the city is sometimes chosen as an intermediate transit given its status as a trade hub. The Agriculture, Fisheries and Conservation Department ("AFCD") is the principal law enforcement agency for the Protection of Endangered Species of Animals and Plants Ordinance (Cap.586) ("PESAPO") [84] that gives effect to the Convention on International Trade in Endangered Species of Wild Fauna and Flora. On the other hand, the C&ED is responsible for investigating large-scale smuggling cases of endangered species under the IEO. An in-depth investigation would be conducted in parallel against each smuggling case should there be suspected ML elements or a large sum of suspected crime proceeds involved.

4.28 The C&ED has stepped up enforcement actions against smuggling of endangered species, and the annual number of cases ranged from 276 to 745 between 2016 and 2021. The main endangered species seized were wood logs, ivory tusks, American ginseng, dried shark fins, and pangolin scales. Most of these cases involved individual travellers who brought small amounts of such goods into Hong Kong for personal use without a licence. The remaining small portions of cases involved the use of sea container shipments carrying huge hauls of endangered species. In 2020, Hong Kong saw a decline of 276 smuggling cases of endangered species due to the drop of cross-boundary travellers under the COVID-19 pandemic. However, it has been observed that some criminals are switching to the use of cargo traffic to smuggle high-valued endangered items. The C&ED has been working closely with its international counterparts on intelligence exchange and sharing of information to combat this illegal trade. On domestic enforcement, the C&ED has also emphasised the collaboration with other LEAs. For instance, various platforms include the Inter-departmental Task Force on Wildlife Crime and the C&ED's Marine Joint Task Force for combating smuggling activities, etc. Furthermore, LEAs may form an ad-hoc task force to deal with specific illegal wildlife trade cases where and when necessary.

4.29 There is no convicted ML case related to illegal wildlife trade between 2016 and 2020. And with the low number of ML investigations related to illegal wildlife trade indicated a low level of ML threat for this predicate offence. It is observed that many fraudulent shipments involving endangered species were imported to Hong Kong solely for the purpose of being transshipped to other places. Most of the local arrestees are so-called "mules" or "couriers" without involvement in the associated ML activities. Nevertheless, in response to the escalating global ML threat of illegal wildlife trade as discerned by the FATF, the C&ED will continue to work closely with the AFCD and international parties to monitor such illegal activities and collaborate with the banking sector on suspicious bank transactions relating to illegal wildlife trade-related ML activities.

[83] United Nations Environment Programme. (2016). The Rise of Environmental Crime: A Growing Threat to Natural Resources Peace, Development and Security. https://wedocs.unep.org/handle/20.500.11822/7662

[84] Chapter 586 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap586

Box 4.3 - Enhancement of combating smuggling of endangered species

Hong Kong attaches significant commitment and determination in fighting against the smuggling of endangered species. In 2018, the maximum penalty under the Protection of Endangered Species of Animals and Plants Ordinance ("PESAPO") (Cap. 586) was increased to a fine of HKD10,000,000 and imprisonment for ten years. In addition, with effect from 27 August 2021, certain offences under the PESAPO were included in Schedule 1 to the OSCO to make OSCO provisions applicable to those offences. The legislative amendment provides additional powers for investigating certain offences and proceeds of crimes in relation to wildlife crimes and the confiscation of such proceeds and related matters. It is a significant step forward in facilitating the combating of wildlife crimes.

Loansharking

4.30 Loansharking refers to the criminal act of lending money at an excess interest rate[85] and adopting aggressive or illegal means to compel loan settlements. In 2020, the number of money lending-related offences reported in Hong Kong slightly increased and was assessed to be possibly related to the economic downturn of Hong Kong under the influence of COVID-19. Nevertheless, the number of loansharking reports in Hong Kong remained low and stable from 2016 to 2020.

4.31 Loansharking-related offences accounted for only 0.3% among all identified predicate crimes in the ML cases examined from 2016 to 2020. The majority (over 70%) of the cases were domestic cases. The ML activities usually involved persons who were stooges recruited by a loansharking syndicate; some were debtors who, upon failure to settle the debt, were instructed to open bank accounts for collecting debts for creditors. Some individuals may have also sold their accounts to loansharking syndicates. In convicted ML cases, 5.9% of the convicted cases between 2016 and 2020 are related to loansharking-related offences, with almost 80% connected to domestic cases. As to the analysis on assets restrained or confiscated between 2016 and 2020, the amount restrained from loansharking-related crimes accounted for 0.1% (i.e. HKD 11.4 million) of the total value of restrained assets, while the amount confiscated accounted for 0.3% (i.e. HKD 4.3 million) of the overall total. Globally, loansharking has been recognised as a source of income for organised criminal groups. Yet, it is not commonly mentioned as a major threat in the national risk assessment reports/ME reports of jurisdictions in the Asia-Pacific Region[86].

Vice

4.32 Jurisdictions around the globe take very different approaches to prostitution. In Hong Kong, vice activities are usually operated in a low-profiled and small-scale system. The number of vice-related reports remained low compared to the total number of reported crimes.

4.33 The ML cases between 2016 and 2020 revealed that vice-related offences account for 0.23% of all identified predicate crimes and only 1.2% of convicted case. Most of these cases were detected locally. It was not uncommon to see misuse of personal bank

[85] Under section 24 of the Money Lenders Ordinance, Cap.163, any person who lends or offers to lend money at an effective rate of interest which exceeds 60% per annum commits an offence and shall be liable to a fine of HKD 5 million and imprisonment for 10 years.

[86] Only a few jurisdictions have mentioned loansharking as one of the major ML threats, including Japan, Papua New Guinea, Macao and Singapore

accounts held by syndicate members to launder the proceeds from the convicted cases. Only a small percentage of assets restrained and confiscated between 2016 and 2020 were connected to vice-related offences.

Intellectual property-related offences

4.34 In Hong Kong, enforcement actions against retail sales of pirated goods fall under the purview of C&ED. Over the years, there has been a continuous drop in the caseload and property seizure relating to piracy cases. However, the inclusion of online elements has become an emerging trend for piracy case. Therefore, the C&ED deployed a Big Data Analytics System in 2017 to perform automatic cross-platform cyber patrol, analyse mass information on different Internet platforms and identify prevailing and emerging trends of intellectual property rights (IPR) crimes. In addition, with an aim to effectively enhance enforcement against transnational IPR infringement, the C&ED has collaborated with the Mainland Customs (Guangdong Sub-Administration of Customs) and Macao Customs to conduct regular joint operations to combat cross-boundary smuggling of counterfeit goods between the Mainland, Macao and Hong Kong as well as to suppress exportation and transshipment of pirated consignments destined for overseas countries. Between 2016 and 2021, a total of 20 joint operations had been conducted with the detection of 258 cases and seizure of HKD 75.39 million of counterfeit goods.

4.35 Between 2016 and 2020, intellectual property-related cases identified as the predicate crimes behind the ML cases accounted for about 0.4% of all ML investigations and 0.3% of the convicted cases. The amount restrained and confiscated from intellectual property-related offences accounted for 0.4% and 0.1% of the total amount restrained and confiscated respectively. The seized goods were mainly electrical and electronic products, leather goods, watches, parts and accessories, clothing and pharmaceutical products, accounting for about 68% of the total value of seizures during the period. There was only one incoming MLA request related to piracy received between 2016 and 2020.

4.36 Internationally, the trading of fake goods is recognised as transnational organised crime. The production and distribution of counterfeit goods present a low-risk/high-profit opportunity for criminals, and the corresponding ML activities and methods are often linked with corruption, drug trafficking and other serious crimes[87]. Moreover, copyright infringement and trademark counterfeit activities continued to exist, with emerging threats observed in those using the Internet platform.

Others

4.37 Other proceeds generating offences include:

(a) Blackmail – accounted for 0.7% to 2.2% of total annual report crimes throughout 2016 to 2020 with the modus operandi of naked chat[88] and internet-based blackmail[89] comprising most of the cases under this predicate offence. While the traditional blackmail cases, such as extortion, has shown a decreasing sign, it is observed that there is a transition to internet-based blackmail cases (including ransomware cases[90]). Crypto-ransomware, one

---

87 United Nations (2014). *Counterfeit: 'Don't buy into organized crime'*. https://www.unodc.org/unodc/en/frontpage/2014/January/counterfeit-dont-buy-into-organized-crime---unodc-launches-new-outreach-campaign-on-250-billion-a-year-counterfeit-business.html

88 Victims get acquainted with the opposite sex on the Internet through social networking platforms/ instant messaging software. They are subsequently tempted to go naked or perform lewd acts before web cameras are blackmailed for the taken images or videos.

89 Other Internet blackmail include the modus operandi of email ransom and ransomware-related cases

90 Ransomware is malicious software that prevents/ restricts a user from accessing a computer system by

of the most common ransomware in recent years, encrypts computer files on infected systems and files stored on external storage devices or the same network. Users are then demanded to pay a ransom in cryptocurrency in the hope of obtaining a decryption key. In 2020, the internet-based blackmail cases (online naked chat) observed a significant increase from 171 cases to 1 009 cases. Another type of Blackmail offence is associated with distributed denial-of-service attacks where culprits paralyze computers or websites by releasing enormous data. Commercial organizations are usually the target, and culprits often demand the attacked companies for VAs as ransom. Asia and other parts of the world face the threat of distributed denial-of-service.

(b) Theft – theft-related cases decreased, dropping from 42% to 32% of the total reported crimes from 2016 to 2020. The majority of the theft cases are opportunity theft, with miscellaneous theft[91] and shop theft[92] being the two major offences. Theft-related cases identified as the predicate crimes behind the ML cases accounted for only about 0.8% of the overall ML investigation profile. 55% of theft-related ML investigations were related to theft originating outside Hong Kong, which took up over 80% of the amount involved in theft-related cases, suggesting the possible external threat. ML investigation of domestic theft-related cases often involved employees' embezzling employers' properties. With the advancement in technology, the exploitation of electronic payment methods is also observed in recent cases (e.g. transfer of monies from the company's account to the employees' account).

(c) Human smuggling and trafficking - Hong Kong is neither a destination for human trafficking nor a place of origin for exporting illegal migrants, and there is no sign that transnational syndicates actively use Hong Kong as a destination or transit point for Trafficking in Persons[93]. In terms of Illegal immigrants, the number of arrests related to overstaying and illegal entry has remained stable in 2016-2020. In particular, non-ethnic Chinese ("NEC") Illegal immigrants was under control, with figures remaining at low levels in recent years. The majority of them came to HK for economic reasons, with many choosing to enter the Mainland by legal means and then sneak into Hong Kong by sea or on land. Some then abused the non-refoulment claim system to extend their stay in Hong Kong. The use of forged travel documents, though on the decline, has been commonplace. Following the closure of land boundary crossing points during the COVID-19 pandemic in 2020, an increase in Mainland Chinese sea-crossers was observed. The ML cases investigated between 2016 and 2020 revealed that human trafficking/smuggling offences accounted for only 0.04% of all identified predicate crimes and 1.3% of the convicted cases. Proceeds involved were often laundered by personal bank accounts of syndicate members or remitted out of Hong Kong through MSOs. The amount involved was

freezing the computer's screen or encrypting the computer files unless a ransom is paid.

91 Mainly related to scenarios where victims left their properties unattended and then got stolen.

92 Most shop theft cases took place in supermarkets, chained retail stores and convenience shops with a small value of the stolen property.

93 SB. (2020). *Trafficking in Persons*. https://www.sb.gov.hk/eng/special/bound/iimm.htm

insignificant, accounting for 0.05% of the total amount restrained, and 0.3% of the total amount confiscated.

(d) Burglary – the number of burglary reports took up only 3% - 4% of total annual reported crime throughout 2016 to 2020. Among those identified predicate crimes behind the analysed ML cases, burglary only accounted for a tiny percentage (0.05%) between 2016 and 2020. Monetary loss from burglary is low when compared to other proceeds generating offences.

(e) Robbery – robbery-related offence in Hong Kong ranges from opportunistic street robberies to organised robberies of jewellery shops or banks. The number of robbery-related crime cases has remained low between 2016 and 2020, comprising less than 0.36% of the total reported crimes.

Typologies Analysis and ML Trends

4.38 This part analyses the common methods and sectors involved and the latest ML trend observed.

Third-party ML

4.39 The use of third parties to launder proceeds generated domestically or outside Hong Kong is prevalent. Over half of the 323 ML cases leading to convictions between 2016 and 2020 were identified as third-party ML involving money mules. Third-party ML commonly involves non-residents, students and low-paid stooges who are recruited to open bank accounts for a small monetary reward. In some cases, the recruitment of stooges was found to be an employment fraud. In recent cases, domestic helpers are being recruited as stooges.

Use of bank accounts

4.40 Bank accounts are still one of the most common tools exploited by money launderers for both domestic and external predicate offences via cash deposits, cash withdrawals or wire transfers. Misuse of both corporate and personal bank accounts have been observed. From detected ML cases, individual accounts were opened by the criminals themselves, family members or associates, or stooges, who may or may not be Hong Kong residents. Corporate accounts of legitimate businesses may be exploited or accounts set up by shell companies to hide beneficial ownership.

4.41 Among all the ML cases involving bank accounts, most of the accounts were used for a "temporary repository of funds", i.e., the funds transferred into the account would be transferred away within a short period, and usually to somewhere outside of Hong Kong. This method suggested that Hong Kong was often involved mainly in the early stage of the ML process, i.e. placement and layering. In some cases, criminals would use a small deposit as "test money" to make sure that the account was in operation before they arranged for the transfer of the crime proceeds. More information than ever before on these characteristics has been identified and shared among LEAs, and banks, allowing some banks to deploy innovate approaches and technologies to increase the effectiveness of their response. In some cases, criminals would conduct cash kiting[94] through different bank accounts to either manipulate the turnover of a corporate entity or the payroll of an individual to obtain additional loans or credit that was not authorised. The money used during the cash kiting might not necessarily be crime proceeds. Still, the money generated

[94] Cash kiting is referred as a circular flow of fund among a number of entities, being individual or corporate body, which are under the control of the same party.

from the additional loan or credit resulting from the cash kiting would be considered as crime proceeds.

Box 4.4 - Use of overseas shell company corporate account

Between October 2008 and August 2009, 95 victims in France and Belgium were lured into investing a purported Forex investment and remitted a total of EUR 1.29 million (approximately HKD 10.92 million) to one United Kingdom bank account and then further dissipated to the corporate bank accounts in Hong Kong belonging to an offshore shell company with a foreign national as signatory and director. In February 2020, the foreign national was arrested when he entered Hong Kong. He admitted that he operated the bank account to deal with the crime proceeds that originated from other predicate offences in France. In November 2020, he was convicted of ML and sentenced to 28 months' imprisonment.

Use of securities accounts

4.42 Securities accounts were found used in the layering and integration stages of the ML process. Criminals would conduct frequent trade in the account to layer the crime proceeds, believing that each transaction would help make it more difficult for LEAs to trace back to its origin. On rare occasions, criminals would withdraw the shares in certificate form and hide them away for an extensive period. Between 2016 and 2020, HKD2.23 billion valued securities-related products have been restrained due to the ML investigation.

4.43 Use of securities account for ML activities was also popular for investment fraud cases. Criminals would use a small proportion of the deceived fund to invest in the stock market and pretend that the scam was genuine and legitimate.

Use of remittance services

4.44 While the banking system remains one of the primary conduits for cross-border transfer of crime proceeds, MSOs have been another avenue for fund transfer. The very well developed business network between Hong Kong and Mainland China has led to widespread usage of MSO services. Frequent cross-border transfers have exposed MSO services to the risk of being misused for ML purposes. There were 32 ML conviction cases that involved the use or complicit involvement of MSO from 2016 to 2020.

Box 4.5 - Case Example – Use of MSO

In early 2013, Hong Kong Customs conducted a joint investigation with the Customs authority of the Mainland against a syndicate involved in exporting luxury left-hand drive vehicles from Hong Kong to Vietnam and then smuggling them into the Mainland, as well as laundering the criminal proceeds from the Mainland into Hong Kong in indirect ways. The buyers made the payments for the vehicles into bank accounts in the Mainland held by the mastermind, who then arranged the transfer of the funds to bank accounts in the Mainland held by a Hong Kong MSO. The mastermind ultimately arranged to collect the monies from the MSO, mainly in cash, in Hong Kong (i.e. the criminal proceeds generated from the smuggling activities). The total amount laundered was HKD 59 million. The mastermind was eventually convicted of ML in 2018 and sentenced to 5 years' imprisonment. The assets valued at HKD 14.2 million under the control of the mastermind was confiscated in April 2019.

Purchase of insurance products

4.45 According to the FATF, the purchase of insurance products is a known international typology used in the layering and the integration stage of the ML process. Criminals would purchase insurance products with crime proceeds and subsequently withdraw them to get a "clean" cheque from the insurance company as a layering process. For the integration stage, criminals would purchase products with variable annuities or specific life insurance policies and keep the insurance products for a more extended period (or lifelong).

4.46 As analysed in greater detail in Chapter 5, purchase of insurance products during the layering stage is not typical in Hong Kong. However, more cases are being observed for purchasing insurance products during the integration stage. Between 2016 and 2020, HKD 10.81 million valued insurance products have been restrained due to the ML investigation.

ML involving professionals

4.47 Professionals such as accountants and lawyers can be used by criminals who need expert advice to devise complicated ML schemes. Cases of complicit involvement of professionals in ML in Hong Kong are relatively rare.

4.48 In most ML cases involving accountants, they were often found to be innocent agents used by criminals to conduct auditing work based on forged documents for various purposes such as tax evasion, loan fraud and listing fraud, etc. In some cases, accountants were employed by corporate entities to oversee the books and accounts of the company. They were instructed to do certain illicit acts for the company, such as false accounting or concealment of information. There were two cases in 2016 with accountants being convicted and sentenced to imprisonment for eight months and nine years.

4.49 Criminals can use lawyers as escrow agents to facilitate their ML activities by handling funds purporting to be from a legitimate business or investment. The fund originated from the investors could be a legitimate source, but it would become proceeds of crime when or if an illegal activity has been unveiled. Two cases involved lawyers whom the court convicted and sentenced them to imprisonment for 26 months and 36 months in 2016 and 2018, respectively.

4.50 Purchase of properties during the placement and layering stage of the ML process is unusual because it requires a lengthy time and various costs to complete the transaction. However, criminals are seen using the crime proceeds (after layering) to purchase properties in Hong Kong. In Hong Kong, DTROP and OSCO empowered the Court to make a restraint order for the restraint of "realisable property[95]". The property that the Secretary for Justice seeks to restrain needs not be connected to the offences. Between 2016 and 2020, HKD 2.91 billion valued properties have been restrained due to the ML investigation.

4.51 In Hong Kong, TCSPs, many owned or managed by solicitors or accountants, provide services such as forming companies, acting as company secretary, or handling funds as a trustee, assisting in opening bank accounts. In 2020, 19 out of 55 ML cases leading to convictions involved the use of TCSP services.

[95] Realisable Property: (a) any property held by the defendant;(b) any property held by a person to whom the defendant has directly or indirectly made a gift caught by this Ordinance; and (c) any property that is subject to the effective control of the defendant.

Misuse of legal persons and arrangements

4.52 Exploitation of corporates in ML cases continued to be observed. The use of layering has increased the difficulty and time required to trace crime proceeds. The use of shell companies, either in Hong Kong or offshore, remain a common conduit for ML. However, the use of offshore companies to facilitate ML activities has become less popular as FIs continued to enhance their CDD requirements to gather information on the beneficiary owner of all types of companies. Misuse of domestic trust in ML has been rare in the past few years.

Complex ML techniques

4.53 Use of complex financial transactions to obscure audit trails is common, and detection requires cooperation by multiple stakeholders. Camouflaging commercial activities by employing tactics of commingling, front companies and TBML are frequently identified in the analysed ML cases.

Use of front companies

4.54 Use of front companies continued to be expected in ML cases involving more sophisticated ML techniques. Front companies were often established to transfer crime proceeds from one country to another under commingled payments resulting from legitimate business activities, such as imports and exports or other business activities. The cross-jurisdictional camouflage of commercial activities, or commingling of funds with those stemming from legitimate businesses, can create numerous layers of funds by disguise.

Box 4.6 - Case Example – Use of Front Companies for email scam

In June 2017, the Chief Executive Officer ("CEO")'s secretary of a UK based Co. (company A) received emails purportedly to be sent from the CEO directing her to wire a total of USD 2.87M to six companies' bank accounts for buying cocoa. The secretary believed the email was genuine and followed the instruction accordingly. Later, the CEO found out those emails were fraudulent. The case was then reported to the HKPF. A Mainland male (D) was the director and bank account signatory of one of the suspect companies receiving the deceived proceeds. D admitted that he was a stooge recruited by a Mainland secretary firm to attend Hong Kong to incorporate companies and open bank accounts. Apart from the bank account used to launder the crime proceeds deceived from company A, D had also opened three other bank accounts which were then exploited for ML purposes. Altogether D had laundered USD 1.26M using the four bank accounts in Hong Kong. D was charged with four counts of ML offences and was sentenced to 45 months of imprisonment.

ML involving cross-boundary movement of CBNIs

4.55 Since the commencement of the R32 Ordinance till the end of 2021, a total of 39 343 declarations were received from the traveller channel. Whereas for the cargo channel, 24 107 electronic declarations for CBNI consignments were submitted through the Currency and Bearer Negotiable Instruments Declaration System. The C&ED makes use of its database and those of JFIU as well as other sources of information such as intelligence and looks into both declarations and non-compliance cases for ML activities. After the grace period of three months[96] since the commencement of the R32 Ordinance, from 16 October 2018 till the end of 2021, a total of 275 non-compliance cases were detected from the traveller channel involving CBNIs of around HK$128 million. The cash concerned was not suspected to be crime proceeds. For the cargo front, 16 non-

[96] A three-month grace period was introduced between 16 July 2018 and 15 October 2018.

compliance cases were detected with the value of CBNIs amounting to around HK$371 million. Most of the non-compliance cases on the cargo front involved importers who breached the declaration requirements inadvertently, and were not suspected to be related to ML or TF activities.

Table 4.5: Declaration figures and non-compliance statistics

Year	2018 (16.7.2018-31.12.2018)	2019	2020*	2021	Total
Passenger					
No. of CBNI declarations	10 186	25 557	3 104	496	39 343
Declared amount (HK$ in billion)	113	307	44	15	479
Non-compliance cases	32	144	25	74	275
Cargo					
No. of CBNI declarations	4 862	10 757	4 930	3 558	24 107
Declared amount (HK$ in billion)	621	1,302	548	312	2,783
Non-compliance cases	1	7	4	4	16

*Since 2020, the numbers of declarations made by passengers and in respect of cargo have significantly declined, possibly attributable to the effect of COVID-19 pandemic to passenger flow and the demand for physical cash

4.56 As cross-boundary movements of physical CBNIs were predominantly attributable to banks, the ML risk for such CBNIs is minimal. However, there is a comparatively higher risk when individual cash couriers repeatedly carry cash without full knowledge of the sources from nearby jurisdictions/other jurisdictions into Hong Kong for currency exchange at MSOs. Meanwhile, there had been three ML cases under investigation arising from cash transported by travellers. Overall, in spite of the significant amount of cash physically transported into and out of Hong Kong, the threat is considered limited having regard to the limited number of ML cases established through investigation and different layers of intelligence gathered under the R32 system and via other sources and channels. The significant reduction in cross-boundary travellers in 2020 and 2021 due to the COVID-19 pandemic has led to a drop in the ML threat level regarding cross-boundary cash transportation.

Trade-based money laundering

4.57 TBML requires intermingling of the trade and finance sectors, and practices vary in complexity. Given the large volumes of financial transactions with trading partners, Hong Kong faces an inherent threat of TBML.

4.58 According to the FATF, the most basic schemes are fraudulent trade practices (e.g. under- or over-invoicing, multiple invoicing of goods and services, under- or over-shipment of goods or services, etc.). In some extreme cases, fraudulent invoices were

created to support non-existent trade or vice versa, and phantom shipping was arranged to justify certain transactions. A typical example of TBML would be using crime proceeds as payment to settle genuine or purported sales of products.

4.59 Considering the complexity of international trade and the absence of any system cross-referencing trade and trade finance data globally, TBML is difficult to detect. Nevertheless, the C&ED adopts an intelligence-based approach to initiate proactive investigation against TBML, which involves predicate offences under Customs purview. The C&ED also collaborates with the banking sector on TBML intelligence and typologies during its outreach activities. Advanced information technology systems are also applied to enhance C&ED's capabilities of cargo selection for clearance and post-clearance analysis on cargo data to identify suspicious shipments and traders. Besides, information exchange among LEAs of different jurisdictions is essential to detect and suppress TBML. Local LEAs coordinated with overseas counterparts to take joint enforcement actions have resulted in successfully detecting TBML cases. There was also financial intelligence from the JFIU suggesting possible TBML activities overseas.

4.60 Hong Kong implements an import and export declaration system whereby any person who imports or exports any article other than an exempted article must make an accurate and complete declaration within 14 days after the importation or exportation of the article. Being the enforcement authority of the import/export declaration regime, the C&ED adopts a risk management approach to verify the declaration data, including the declared quantity and value of goods, to identify suspicious shipments for follow up action.

Assets restrained or confiscated in ML cases

4.61 Criminals continue to disguise their sources of crime proceeds by converting them into complex forms to retrace. The following tables show the amounts restrained or confiscated as realisable assets of persons convicted of ML, their family members or associates between 2016 and 2020. The most common restrained and confiscated assets in Hong Kong are cash in bank accounts, real estate and securities held with licensed corporations ("LCs") or banks. Other assets include precious metals, stones, jewellery or wristwatches and physical cash. Around 60% of the assets were held in the name of other persons or co-owned by a company.

Table 4.6: Breakdown of realizable assets in Restraint and Confiscation Orders (2016-2020)

Type of Assets			Amount (HK$ in million)	%
Breakdown of Realizable Assets in Restraint Orders (2016-2020)	**Categorised Assets**	Assets placed in banks[97]	3,886	42.44%
		Securities[98]	2,233.2	24.39%
		Insurance policies/products	10.81	0.12%
		Real Estate	2,908.6	31.77%[99]
		Precious metals and stones, jewellery or wristwatches	12.36	0.14%
		Cash[100]	62.47	0.68%
		Vehicles	8.37	0.09%
		Others[101]	34.2	0.37%
		Sub-total	9,156.01	100%
	Uncategorised Assets	Uncategorised company assets	0	0%
		Total	9,156.0	100.00%
Note: Total amount of assets owned by third parties (HK$ in million)			7,729.84	84.42%

97 Includes cash, securities products, trust (unit trust) and insurance products.

98 Securities include physical shares and shares in securities firm accounts.

99 Including 0.02% identified property outside Hong Kong.

100 Cash include physical cash (banknotes) and bail money.

101 Others include vehicle registration marks, trading licenses, luxury bags and pens, Hong Kong Jockey Club betting account and stamp duty held by IRD.

Type of Assets			Amount (HK$ in million)	%
Breakdown of Realizable Assets in Confiscation Orders (2016-2020)	**Categorised Assets**	Assets placed in banks [102]	780.3	54.52%
		Securities[103]	2.8	0.20%
		Insurance policies/products	12.18	0.85%
		Real Estate[104]	216.11	15.10% [105]
		Precious metals and stones, jewellery or wristwatches	3.26	0.23%
		Cash[106]	75.92	5.30%
		Vehicles	1.38	0.10%
		Vessels	1.24	0.09%
		Sub-total	1,093.19	76.38%
	Uncategorised Assets	Uncategorised company assets	338	23.62%
		Total	1,431.19	100.00%
Note: Total amount of assets owned by third parties (HK$ in million)			628.35	43.90%

[102] Includes cash, securities products, trusts (unit trust) and insurance products.
[103] Securities include physical shares and shares in securities firm accounts.
[104] Real Estate Includes Property, Land and Car park space.
[105] Including 0.52% identified property outside Hong Kong.
[106] Cash includes Physical cash in banknotes and Bail money.

Typologies Revealed by STRs and Intelligence Exchange

4.62 STRs filed locally by entities and intelligence exchanges with other jurisdictions show a general increase in recent years. Both internal and external intelligence shows that fraud cases, particularly email scams, telephone deception and COVID-19 e-shopping fraud, dominate the predicate crimes.

4.63 Examination and analysis of STRs reveal certain common modus operandi employed in pursuing ML activities including:

(a) Change of directorship or shareholding of the corporate customers in question soon after the opening of bank accounts;

(b) Use of the bank accounts concerned is ceased upon receipt of one or a few fraudulent payments; and

(c) Change of Device identity/ internet protocol ("IP") address shortly after account opening;

(d) Common Device identity/ IP address shared by suspicious customers;

(e) Dissemination of fund mainly involved FPS or other online payment platforms instead of traditional transactions means;

(f) Use of cryptocurrency as an alternative to dispose suspected crime proceeds; and

(g) The misuse of accounts in "traditional" banks is still the dominant pattern in overseas fraud cases.

4.64 "Temporary Repository of Fund", "Large Transaction", and "Transaction Incommensurate with the Customer Background" were the most reported suspicious indicators, followed by "Large Cash Transaction", "Non-resident Personal Account" and "Transaction with no Business Purpose".

Box 4.7 - Case Example – Use of STR for Detection of Crime

STR suggested that Company A's bank accounts had numerous credit card transactions, incommensurate with its purported business as a party room. Between January 2019 and July 2020, Company A's accounts in local banks received thousands of payments from hundreds of credit cards amounting to over HKD 85 Million. Further investigation by the HKPF revealed that most of the credit cards were issued to a syndicate of more than 20 persons suspected of making credit card applications by submitting fake employment records. Funds were further dissipated to the other accomplice accounts. The HKPF later neutralised the syndicate.

Other Observation and Emerging Challenges

Organised crime or triad groups

4.65 In Hong Kong, organized crime in the form of triad gangs activities are mainly territorial. Triad members commonly committed unlawful society offences, wounding and

serious assault, criminal intimidation, criminal damage, possession of offensive weapons, and involvement in the proceeds generating crimes such as fraud, drug trafficking, gambling, vice and blackmail represent an ML threat.

4.66 Not all syndicates operating in Hong Kong are triads. Triads groups are usually involved in fraud, drug trafficking, bookmaking, vice, smuggling of counterfeit goods and payment card fraud. Transnational organised crime groups are generally more sophisticated, with the knowledge and network to perpetrate predicate crimes and ML across multiple jurisdictions. There is no evidence supporting any strong network between local and transnational organised crime groups in the facilitation of ML.

Use of SVF

4.67 The COVID-19 pandemic has stimulated the use of non-face-to-face and contactless (non-cash payment) transactions to facilitate payment worldwide. In Hong Kong, there has been a significant increase in the use of SVFs to enable payment, given its ability to provide instantaneous transactions and the option of anonymity for small-value services with limited functionalities[107]. In some cases, it was found that, through LEAs' investigations into alerts raised by SVF licensees in STR filing, operators of illegal gambling activities had been exploiting SVF services for receiving payments from gamblers.

Virtual banks

4.68 Another change in the banking sector landscape has been the rapid emergence of remote onboarding processes. This phenomenon has been accelerated by COVID-19 social-distancing requirements and the development of VBs. Remote onboarding is now a standard feature offered by almost all retail banks, and the vulnerabilities are the same. However, it should be mindful that the innovation involving remote onboarding makes it attractive to criminals, i.e., ease of access to banking service regardless of time and location, making multiple applications without incurring extra cost, and the speed of electronic transactions. As a new segment of the banking sector, VBs have been targeted to test vulnerabilities and launder crime proceeds derived from deception cases and illegal gambling activities. VBs have responded swiftly to the emerging threats, as reflected by their STR filing and contributions to platforms such as FMLIT. Further details on risk-mitigating measures and supervision on VBs are set out in Chapter 5.

Virtual assets / virtual asset services provider

4.69 Criminals easily abuse VAs with its borderless nature. VAs are often conducted with hidden beneficiary ownership with many of the transactions capitalising on jurisdictional arbitrage, making it extremely attractive for ML purposes. In Hong Kong, most of the VA-related crimes were fraud-related (e.g. romance scam) and mainly perpetrated through social media platforms. Fraudsters mainly convinced victims to invest in VA investment plan or transfer VA to them with nothing in return.

Environmental crime

4.70 According to the FATF, environmental crime covers a wide range of activities, from illegal extraction and trade of forestry and minerals to criminal land clearance and

[107] Taking into account the lower level of ML/TF risks of some SVF products as determined by limitations to value stored and functionality and predominant use for low-value retail transactions, a tiered approach to customer due diligence is allowed which permits certain due diligence measures to be performed in a particular manner or not performed under certain scenarios. Please refer to the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Stored Value Facility Licensees) for details. https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/infrastructure/svf/Guideline_on_AMLCFT_for_SVF_eng_Sep2020.pdf

waste trafficking, which harm the environment. In Hong Kong, the Protection of Endangered Species of Animals and Plants (Amendment) Ordinance 2018 (Cap. 586), which came into effect in May 2018, stipulates the importing, exporting or re-exporting of scheduled endangered species as indictable offences otherwise than under the Ordinance. In addition, illegal logging and wildlife smuggling can also be prosecuted through other applicable indictable offences (such as theft, smuggling, etc.). In Hong Kong, statistics of various environmental crimes remained stable. There were no ML investigations, convictions, restraints and confiscations related to environmental crime between 2016 and 2020. Very few environmental crimes-related STRs and MLA requests were received during the period, which mainly pertained to persons/companies suspected of involving international illegal logging and wildlife trading. Still, none of them occurred within Hong Kong. The ML threat level for environmental crimes in Hong Kong is assessed as low. With the increasing global concern, these activities would be closely monitored and evaluated.

Overall ML Threat

4.71 The overall ML threat of Hong Kong remains as medium-high. As an international financial centre, Hong Kong continues to be exposed to both internal and external ML threats. Transnational criminals exploiting Hong Kong's financial and telecommunication infrastructure and free-trade system to channel crime proceeds persists. Based on relevant quantitative and qualitative data, it is noticed that domestic ML threat and external ML threat have posed a similar threat level in the 2nd HRA. While the portfolio of predicate offences did not show a significant change compared with the 1st HRA, evolvement in the modus operandi, ML typologies and techniques deployed by criminals have been observed, partly attributed to the accelerated and wide-spread application of technology during the pandemic.

CHAPTER 5

SECTORAL RISK ASSESSMENT - FINANCIAL INSTITUTIONS

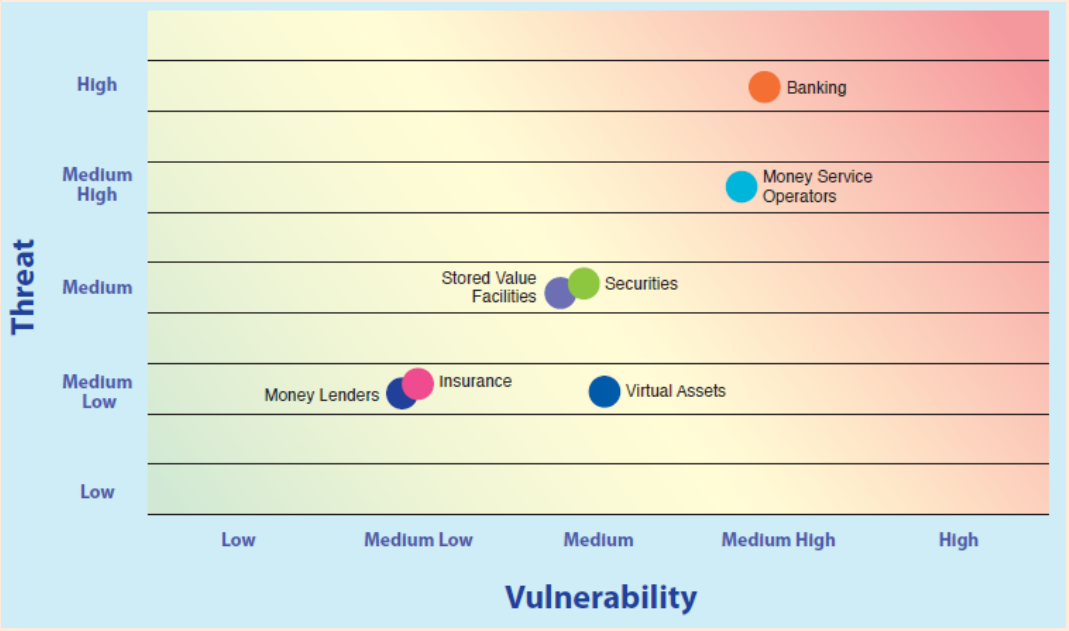
5.1 OVERVIEW

5.1.1 This Chapter sets out an updated assessment of the banking, securities, insurance, MSO, SVF, VASP and money lender sectors and an account of the assessment of financing lease businesses, non-bank credit card provider and credit unions. The first five are the major financial sectors covered by the AMLO and relevant regulatory frameworks, and supervised by the relevant authorities. They are subject to AML/CFT requirements prescribed in the AMLO and the guidelines issued by the regulators. In addition to the CDD and record-keeping requirements, overarching statutory obligations exist in primary legislation for regulated FIs to establish AML/CFT controls, ensuring proper safeguards to prevent contravention of CDD and record-keeping provisions, and more generally to take all reasonable measures to mitigate ML/TF risks. The money lender sector is regulated under the MLO and subject to a rigorous regulatory regime. The VASP sector is already subject to multi-disciplinary oversight of regulators in accordance with the nature and function of the VA activities. The Government plans to enhance further its regulatory efforts on this front by including licensed VASP in the AMLO similar to other FIs.

Table 5.1: Size – Financial institutions

	Number of institutions or practitioners	Asset size as at Dec 2021, unless otherwise specified (USD billion)
Banking	Licensed banks: 160 Restricted licence banks: 16 Deposit-taking companies: 12 Local representative offices of foreign banks in HKC: 39	3,383
Securities	LCs: 3 210	250.2
Insurance	Aurhorised Insurers carrying on long term business: 73 Insurance intermediaries carrying on regulated activities in respect of long term business: Licensed Insurance broker companies: 733 Licensed Insurance agencies:380 Licensed Individual insurance agents: 116 237	2021 total long term in force premiums: 69.3
Money Service Operators	805 licensees	1.98
Money Lenders	Licensed money lenders: 2 490	Total customer loan amount: 28
Stored Value Facilities	12 SVF licensees; and 3 licensed banks currently issuing or facilitating the issue of SVF	Total SVF float and deposits: 2
Virtual Assets	VA trading platform operator: 1	76.3 million

Figure 5.2: Overview of risk levels of major financial institutions



5.2 BANKING

5.2.1 Hong Kong continues to be one of the world's leading banking centres. Seventy-eight of the world's top 100 banks operate in Hong Kong, including all 30 global systemically important banks identified by the Financial Stability Board. At the end of 2021, there were 188 authorized institutions[108] with total assets of HK$26.4 trillion, an increase of 16% from HK$22.7 trillion in 2017, and equivalent to 916% of Hong Kong's GDP.

5.2.2 Since the 1st HRA, fintech has brought about significant changes in the banking sector in terms of service offerings, customer relationships and client behaviour, especially during the COVID-19 pandemic. Digital payment channels and remote customer onboarding now play more important roles than ever. The FPS, launched in September 2018, allows the public to transfer money and make payments safely and conveniently and has achieved widespread adoption. The introduction of VBs[109] has also increased the diversity and inclusiveness of the banking sector and helps provide customers with innovative banking services and experience. While bringing greater customer choice and convenience, these changes are accompanied by different degrees of ML risk to banks at institutional and sectoral levels. The following analysis examines the impact of these changes on the ML risk landscape of the banking sector and how banks, the HKMA and LEAs have strengthened management and mitigation of common and emerging ML risks.

ML Threats in the Banking Sector

5.2.3 In line with the 1st HRA, ML threats to the banking sector remain high. Between 2016 and 2020, 87% of ML cases leading to convictions affected the banking sector to varying degrees, with approximately HK$11 billion in crime proceeds involved in these cases laundered through abuse of the banking system. Bank accounts are the most common vehicles exploited for ML. Close to 70% of ML-related realisable assets in restraint and confiscation orders between 2016 and 2020 were found to be held in bank accounts.

Fraud

5.2.4 With the widespread adoption of information technology, online fraud involving cross-border activities is on the rise globally. With an accelerated rise in online commerce and financial service activities in Hong Kong, especially during the COVID-19 pandemic, both online fraud and related ML have also increased. As highlighted in Chapter 4, fraud[110] continues to be the major proceed-generating crime posing the most significant ML threat to Hong Kong and the local banking sector. Over 19 000 deception cases were reported to the HKPF in 2021, an increase of around 24% compared with 2020. Bank accounts opened by money mules or stooges remain a common means of laundering fraud-related funds through the banking sector.

5.2.5 Criminals have adapted their operations to exploit vulnerabilities that emerged in the wake of COVID-19. At the pandemic outbreak, COVID-19-related cases typically involved fraudulent offers to supply personal protective equipment, especially face masks,

---

[108] In this report, the terms "Authorized Institutions or AIs" and "banks" are used interchangeably. As at end-2021, there were 160 licensed banks, 16 restricted licence banks and 12 deposit-taking companies.

[109] See Box 5.2 for details of VBs.

[110] According to the HKPF statistics, email scams, lottery fraud and telephone deception are the most prevalent predicates for ML cases affecting the banking sector.

and deception related to government subsidies designed to provide relief during the epidemic. Banks also saw increases in other types of fraud, such as email scams, telephone deception and theft of account information. It was possibly due to businesses adopting work-from-home arrangements and individuals subject to travel restrictions or social distancing making greater use of online financial services, with which they may be unfamiliar.

5.2.6 The HKMA, the banking industry and other financial regulators, working closely with the HKPF have cooperated to minimise risks resulting from the COVID-19 pandemic through a timely, risk-based and whole-of-system response. Information on COVID-19 related financial crime and threats (e.g. typologies) has been developed and shared through the FMLIT, which in early 2020 designated COVID-19 related deception as one of its operational priorities. In May 2020, the HKPF broadcasted a video clip on television to alert the public to COVID-19 related fraud and shared good practices on fraud prevention and detection with the industry. Case-based intelligence to mitigate displacement risk across banks and an alert to all banks and SVF licensees on surgical mask scams were disseminated to raise industry awareness.

5.2.7 Riding on the international good practices promoted by the FATF, the HKMA issued guidance to banks in April, July and December 2020 to reiterate existing risk-based flexibility in AML/CFT requirements while reminding banks of vigilance regarding COVID-related financial crime risks. The HKMA hosted a discussion by video-conferencing with other financial regulators and the CR in May 2020 to share experience and information on sectoral responses and developments observed, which strengthened coordination on ML/TF risk management in relation to COVID-19. An industry sharing session was also held by the HKAB, with the HKMA's support, in September 2020 covering financial crime trends observed and challenges encountered during COVID-19 and good practices by banks in managing and mitigating ML/TF risks. These concerted efforts led to enhanced controls and improvements in the sector's ability to detect and report accounts potentially used for COVID-related financial crime activities.

Box 5.1 - Case study on personal protective equipment fraud using bank accounts

In January 2020, an individual posted an advertisement on various e-commerce platforms claiming to have a large stock of surgical masks and alcohol sanitisers for sale. Between January and March 2020, more than 200 victims attempted to purchase the goods from the individual and paid for them by depositing cash or making electronic fund transfers. However, only partial delivery, and in some cases no delivery at all, of the goods has been completed. HKD 1.4 million was deposited into three local bank accounts and four SVF e-wallets held by the individual's spouse and associates. Investigations revealed that the money was quickly withdrawn after victims deposited it into the designated bank accounts and e-wallets. Four individuals were arrested in April 2020. The investigation is ongoing.

Corruption and tax crimes

5.2.8 As noted in the 1st HRA, Hong Kong's status as an international financial centre with a free and open economy, proximity to the Mainland and simple tax regime make it

vulnerable to ML related to overseas corruption and tax crimes. The observations in Chapter 4 reinforce this assessment. Tax crimes and corruption originating outside Hong Kong accounted for about 1.4% of all ML investigations between 2016 and 2020[111]. While this figure is dwarfed by the 72.6% for investigations related to fraud (both foreign and domestic), it is comparable to the 1.4% for drugs-related investigations (both foreign and domestic). In addition, foreign tax crime and corruption accounted for 4.4% (HK$404.86 million) of the funds covered by Restraint Orders over the same period[112] and 13.9% of incoming MLA requests. These observations suggest that corruption and tax-related offences, while not the most serious ML threats to the banking sector, are not insignificant and should be viewed seriously. The importance attached globally to these offences as proceeds-generating crimes, particularly in the Asia Pacific region[113], supports this view.

5.2.9 In the light of these observations, the HKMA has accorded priority to assessing and identifying how such predicates and related ML activities materialise in the context of Hong Kong's banking sector and the level of resilience of the sector. Thematic examinations on private banks, together with analysis of cases provided by major banks, revealed that the banking sector, particularly the private banking segment, has good awareness of the threat and applies appropriate preventive measures with related STRs submitted being generally of high standard. Regarding tax crime, there were some sample cases involving overseas tax amnesty programmes or triggered by Common Reporting Standard or AEOI arrangements, suggesting that these initiatives have the intended effect. Also, while private banks are often regarded as being more vulnerable to corruption and tax crime-related ML, case examples indicate that risks also exist in current account / savings account and retail wealth management services. These retail services have been used as intermediary channels for the movement of funds related to these predicates, including through automatic teller machine ("ATM") and credit card withdrawals.

Other ML threats

5.2.10 Other proceed-generating crimes such as drug trafficking, serious gambling offences, goods smuggling (including wildlife trafficking) and human trafficking continue to pose ML threats to which the banking sector remains vigilant (see Chapter 4). Illegal wildlife trade is a major transnational organised crime that generates billions of criminal proceeds each year[114], and has received global attention led by the FATF. It is envisaged that the amendments being made to OSCO in August 2021 to include wildlife crime offences will further raise awareness and drive more effective risk understanding and mitigation by banks through existing risk-based AML/CFT controls. As to human trafficking, the Government has put in place a legislative and institutional framework to address the threat posed by human trafficking activities. The HKMA noted some banks conducted in-depth analysis on human trafficking, which helped raise awareness and mitigate controls.

[111] See Table 4.1. Foreign tax crime represented 1.1% of investigations and foreign corruption 0.3%. Domestic tax crime accounted for 0.02% and domestic corruption 0.9% of cases.

[112] See Table 4.3. A further 3.6% (HK$327.47 million) was related to domestic corruption, while the figure for domestic tax crime was zero. Note that there were no Confiscation Orders relating to foreign tax crime or corruption in the period (Table 4.4).

[113] See Chapter 4, in particular paragraphs 4.13 and 4.17.

[114] FATF Report on Money Laundering and the Illegal Wildlife Trade (June 2020).

ML Vulnerabilities of the Banking Sector

5.2.11 Hong Kong remains a major international financial and trading hub and leading wealth management centre in Asia-Pacific, making the banking sector inherently vulnerable to ML. The 1st HRA analysed how different banking products and services, e.g. private banking, trade finance, international fund transfer, retail and corporate banking, were vulnerable to ML activities. This HRA focuses on significant developments which affect the local banking sector in recent years. The previous considerations are still relevant and continue to present a medium-high level of ML vulnerability[115], albeit the banking sector continues to apply adequate and effective controls to mitigate these vulnerabilities.

Remote customer on-boarding

5.2.12 To date, more than 90% of retail banks[116] in Hong Kong have either launched or are planning to launch remote customer onboarding services through non-face-to-face channels. More than 970 000 personal accounts were opened remotely in 2021, compared with about 18 000 in 2019. The increase was mainly attributable to the launch of VBs in 2019 and the changes in customer behaviour due to COVID-19, with shorter bank branch opening hours and social distancing measures.

Box 5.2 - Launch of VBs in Hong Kong

A VB primarily delivers retail banking services via the internet or other electronic channels rather than physical branches. In May 2018, the HKMA issued a "Guideline on Authorization of Virtual Banks" to encourage the development of VBs[117] in Hong Kong to promote fintech development, improve customer experience, and spur financial inclusion. In the first half of 2019, the HKMA granted banking licences to eight VBs with a mix of backgrounds[118]. All eight VBs commenced business in 2020 following pilot trials through the HKMA's Fintech Supervisory Sandbox and comprehensive independent regulatory compliance assessments, including AML/CFT requirements. By 2021, the VBs collectively had onboarded a total of 1.25 million individual customers with deposits totalling HK$24 billion. Products and services offered by VBs include savings, time deposits, personal loans, local funds transfers, credit cards, physical and virtual debit cards, and loan products for small and medium enterprises.

5.2.13 In the past, impersonation risk [119] was generally considered an area of vulnerability for remote customer onboarding. However, with the introduction of reliable and cutting-edge technology such as digital identity systems (e.g. iAM Smart[120]) and facial

[115] Banks should read this banking section in conjunction with the 1st HRA, available at: https://www.fstb.gov.hk/fsb/aml/en/doc/hk-risk-assessment-report_e.pdf

[116] As at end-2021, there were 28 retail banks in Hong Kong, including eight VBs.

[117] In Hong Kong, a VB denotes an authorized institution that operates primarily online without physical branches. However, all VBs must have a principal physical place of business.

[118] Two are joint ventures set up by established banking groups, one is formed by a local fintech firm, two are backed by Mainland insurance firm, and the remaining three are established by Mainland technology firms.

[119] Impersonation or impersonation fraud refers to a fraudster deceiving someone by pretending to be another person. In the context of account opening, this includes identity theft and the use of stolen or lost identification documents.

[120] iAM Smart was launched in December 2020 by the Office of the Government Chief Information Officer as one of the key infrastructure projects for smart city development announced in the 2017 Policy Address. It provides all Hong Kong residents with a single digital identify and authentication to conduct government and

recognition technology, the channel risk of remote onboarding can be mitigated to a level commensurate with that of traditional face-to-face onboarding. The HKMA has issued several circulars between 2019 and 2021, setting out the guiding principles for remote onboarding. In particular, technology solutions should be able to perform identity authentication and identity matching[121] when individuals onboard remotely to meet the identification and verification requirements in CDD processes. Individual banks also apply other risk mitigation measures (e.g. further reviews of customer identification documents in higher-risk situations, limiting the functionalities of certain accounts).

5.2.14 AML/CFT thematic examinations on remote customer onboarding conducted in 2020 showed that banks generally had a sufficient understanding of vulnerabilities in this area and adopted additional control measures to mitigate impersonation risks further. The HKMA has shared key observations and good practices for remote customer onboarding initiatives with the banking industry, and also through its ongoing engagement with banks through the Fintech Supervisory Chatroom and Fintech Supervisory Sandbox. Furthermore, targeted outreach and capacity building work have also been undertaken against mule account networks as detailed in paragraphs 5.2.18 and 5.2.20 below.

5.2.15 Remote onboarding enhances the efficiency of banks' CDD processes (e.g. by reducing paper documentation). It improves customer experience by sparing them from physical attendance at the branch and allowing flexibility to access services around the clock. However, remote onboarding can be exploited by criminals for ML through the recruitment of stooges to open bank accounts (see Box 5.3) and increases the scalability of potential abuse with little extra risk for the stooge or network. Stooge accounts are a long-established ML typology affecting conventional banks using face-to-face channels to onboard customers.

5.2.16 This vulnerability is not limited to VBs, but applies to any bank, locally or globally, using remote onboarding channels. Banks in Hong Kong mainly offer remote onboarding services to Hong Kong Identity Card holders (i.e. local individual customers[122]). This operation makes it difficult for foreign criminals to directly abuse the remote customer onboarding for ML purposes, generally lowering residual vulnerabilities.

Box 5.3 - Case study on telephone deception using stooge accounts in VBs

A telephone deception syndicate recruited young people to open stooge accounts, seeking to exploit vulnerabilities in remote banking services.

Multiple banks were targeted with accounts at conventional banks mainly used as the first layer and VB accounts as the second and subsequent layers for receiving crime proceeds.

commercial transactions online. Details could be found in the HKMA circular "Launch of iAM Smart" dated 29 December 2020. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20201229e1.pdf

[121] See HKMA's circular on "Remote on-boarding of individual customers" published on 1 February 2019 for the definitions.

[122] The total number of corporate customers on-boarded remotely by banks in Hong Kong so far is relatively small at around 2,000, where all corporate customers are locally incorporated.

The Fraud and AML teams of a VB identified a network of stooge accounts after its fraud monitoring system flagged suspicious behaviour of an account, where a review had shown linkage to other accounts. The VB was able to apply controls to prevent the account from being operated without further customer verification. STRs were filed against 15 individual retail accounts.

Further intelligence from law enforcement indicated that four of these accounts were suspected of being used to receive proceeds of telephone deception. Analysis by the VB found that funds had been disbursed to other accounts among the original 15 and then to accounts at different VBs. STRs were subsequently filed against a further 12 accounts. In total, the 27 accounts had recorded transactions of HKD 70 million.

Mule account networks

5.2.17 Criminals continue to use mule accounts to launder illicit proceeds, distancing themselves from the criminal act and making the funds more difficult to trace. During the pandemic, there has been a shift in the profiles of suspected money mules opening accounts, from individuals of various nationalities on short-term stays in Hong Kong to Hong Kong residents, including domestic helpers and persons with vulnerable backgrounds. In particular, banks have observed (i) dormant accounts receiving surges in deposits marked as pandemic-related fundraising or donations; (ii) surges in transaction volume, temporary deposits via cash, FPS and online banking platforms, which were not consistent with the customer's stated purpose of the account and/or nature of business; and (iii) multiple mule accounts opened by one beneficial owner within one year with initial transactions related to sales of personal protective equipment to other jurisdictions, which were not consistent with the customer's stated business.

5.2.18 The ability of LEAs to crack down on mule account networks is in part dependent on data and intelligence provided by the banking sector, which has been progressively improving its capabilities to identify such networks using Regtech and innovation. These capabilities are not just restricted to large global banks; positive outcomes have been achieved and valuable intelligence derived from banks' network analytics shared through FMLIT, leading to targeted actions by law enforcement. To scale up the use of these capabilities across the retail banking segment, the HKMA has undertaken a number of initiatives, including thematic work on network analytics, the sharing of good practices in the use of external information and data in AML/CFT systems, as well as hosting a sharing session on "Adoption of Regtech for Network Analytics" for FMLIT member banks in December 2020, and invited some banks to share experience and good practices on network analytics with the banking and SVF sectors in the AML webinar in September 2021.

Figure 5.3: Insights from an HKMA thematic review on banks' AML/CFT systems

Key observations and good practices in the use of external information and data in AML/CFT systems

5.2.19 The HKPF also launched an AML-themed cross-sector publicity campaign named "Project AccFencers" in November 2021, which engaged stakeholders from the public and private sectors in stepping up the preventive, enforcement as well as publicity efforts in combating mule accounts in the spirit of public-private-partnership. In collaboration with the HKPF, the HKMA set up a new educational page on its website in December 2021 to remind the public not to sell or lend their accounts to third parties as these may be used as mule accounts for unlawful purposes. The industry has also disseminated similar messages through various channels.

Box 5.4 - Case study on mule network analysis

A retail bank noted a significant increase in fraud-related referrals between March and June 2020, over 50% of which involved suspected fraudulent proceeds being credited to the accounts of non-local individual customers. The bank conducted a special review and identified several commonalities in the concerned customers' demographics, profiles and transaction patterns, suggesting these were possibly mule accounts opened by a fraud syndicate(s). The bank's analysis of the digital footprints of the suspicious accounts further revealed that the account holders were mainly using online banking to operate their accounts and attempted to access online banking shortly after opening the accounts. This suspicion led to an FMLIT alert to share observed risk indicators, the investigative technique used to identify potential mule networks and possible risk mitigation measures with other banks.

Payment systems and new payment methods

5.2.20 As a regional payment and settlement hub with an extensive correspondent banking network, Hong Kong remains exposed to ML vulnerabilities posed by international fund transfers[123]. In recent years, traditional payments, both domestic and cross-border, have been undergoing transformation. During the COVID-19 pandemic, electronic payment channels became widely adopted. Locally, 9.6 million accounts were registered with the FPS between its inception in September 2018 and the end of 2021. The average daily turnover of FPS reached over 673 000 real-time transactions (worth HK$5.4 billion and RMB136 million) in 2021, 90% higher than that in 2020. While FPS allows users to transfer

[123] 1st HRA recognised vulnerabilities of correspondent banking and cross-border wire transfers.

money more safely and conveniently, its speed and efficiency inevitably led to it being exploited to move illicit funds, albeit usually in small amounts. As with similar systems globally, a stronger public-private partnership through the FMLIT and ADCC, together with other effective preventive measures like CDD and transaction monitoring imposed by banks, help mitigate the increased vulnerabilities. As described in Box 3.3, the ADCC has established a round-the-clock contact channel with fourteen retail banks (including all eight VBs) for "stop payment" and intelligence exchange.

Box 5.5 - Case study on stooge accounts for illegal gambling

Illegal gambling is a long-standing issue, with syndicates targeting banks and SVF licensees to open mule accounts and move funds using FPS. In 2020 a syndicate recruited unemployed persons to open stooge accounts with a VB for a small financial reward, with control of the accounts immediately passed to syndicate members. These accounts were used to receive bets and top-up funds from gamblers recruited to open online gambling accounts via social media. Funds were then passed to an operating centre for illegal bookmaking using VB accounts, the FPS and prepaid cards issued by an SVF licensee.

The VB's AML team identified specific characteristics shared by the stooge accounts from monitoring the VB's data and conducted manual reviews, which identified further similarities. This review led to a network of accounts identified with a distinctive pattern in account opening and transaction activity.

The VB filed STRs, which, together with STRs filed by another VB, led to Police action against the syndicate. Twenty-two persons were arrested, and HK$10 million in assets, including HK$3.4 million in cash, luxury watches and a Porsche sport utility vehicle, were restrained. HKPF believed the city's first bookmaking and ML racket that had taken advantage of fintech collected more than HK$500 million in bets on international gambling websites. A FMLIT alert was issued to banks and SVF licensees to share intelligence on this case, including characteristics and indicators of potential stooge accounts.

5.2.21 NPM providers[124], which provide alternatives to traditional payment methods, have emerged and gained popularity globally, including in Hong Kong. While NPM providers often provide genuine economic benefits by offering faster and more efficient payments at lower cost, they generally utilise bank accounts to conduct payment transactions on behalf of their customers and may increase ML/TF risk by inserting additional intermediaries into payment chains, making it harder to "see through" to the originator and final beneficiary. As NPM providers mainly operate through online platforms, it may be difficult for the "host jurisdiction" to confirm their principal place of business due to their transnational nature and dynamic business models. Given their easy accessibility and sometimes unclear regulatory status, NPMs may become attractive to criminals for ML/TF, which poses challenges to banks in assessing and mitigating risks. There has been little evidence that abuse of NPMs for illicit purposes is prevalent in Hong Kong, although the use of some NPMs, including the use of VAs, was observed in some ML cases (see

[124] While there is no widely adopted definition, NPM providers usually refer to electronic wallet (e-wallet) issuers (see section 5.6 on ML risk associated with SVF licensees), money transfer providers, payment aggregators, payment gateways and the use of VAs like digital payment tokens or "cryptocurrencies" for payment.

section 5.7 on ML risk associated with VASPs). Banks have become increasingly aware of the ML risks posed by NPMs and have conducted reviews where appropriate to identify and assess their exposure to threats arising from NPMs and understand fund flows of accounts that potentially use NPMs for ML/TF purposes. Some banks have already implemented or amended controls (e.g. targeted CDD measures) to address any identified risks. Donation-based or crowdfunding platforms, often operating in conjunction with NPM providers, are another development that may present risks, including for TF and other illegal activities. In this connection, the Government has conducted a preliminary study on legislation related to crowdfunding, and is planning to conduct a public consultation in 2022.

5.2.22 In December 2019, the HKMA provided updated guidance to banks, in line with guidance issued by the FATF, on managing ML/TF risks associated with VAs and VASPs when establishing and maintaining business relationships with VASPs or offering VA-related products, including guidance on conducting appropriate risk assessments. In the light of international and local developments and in response to industry enquiries, the HKMA issued a circular in January 2022 to articulate its regulatory approaches regarding AIs' business dealing with VAs and VASPs and provide updated guidance in AML/CFT and financial crime risk, in line with the latest guidance issued by the FATF. The HKMA will continue to monitor ML/TF risks posed by NPMs, including VAs, to the banking sector and the effectiveness of banks' controls in addressing these risks as they evolve.

Private banking and wealth management

5.2.23 Hong Kong remains a major private wealth management centre in the Asia-Pacific region, ranking third in the world[125], and with stable growth in the last four years[126]. To date, around 41 banks are providing private banking and wealth management services to local and international customers with combined assets under management of around HK$9 trillion.

5.2.24 As highlighted in the 1st HRA, the client attributes, large size of assets under management, complexity of products and services, highly personalised services and close relationship between the customer and relationship manager of private banking continue to make it vulnerable to ML, particularly in the areas of foreign tax evasion and corruption (see paragraphs 5.2.8 and 5.2.9 above). Relationship managers may unknowingly help criminals to invest in complex and often opaque investment products where the legitimate investment returns act to launder significant illicit funds.

5.2.25 Thematic examinations conducted in 2019 and 2020 indicated that private banks generally understood the threat of high-end ML and applied preventive measures effectively. However, there was also room for improvement in certain areas, such as the frequency of customer reviews and the effective application of enhanced due diligence under higher risk situation. The sector's exposure to the proceeds of political corruption will be more comprehensively monitored by changes to the definition of politically exposed person ("PEP") in the upcoming amendments to the AMLO[127].

[125] Reference: "The Deloitte International Wealth Management Centre Ranking 2021".

[126] Number of private banking customers increased by 2.9% between 2018 and 2021.

[127] The definition of PEP will be amended from "an individual who is or has been entrusted with a prominent public function in a place outside the PRC" to "an individual who is or has been entrusted with a prominent public function in a place outside Hong Kong", while risk-based flexibility will be provided for the treatment of former PEPs.

AML/CFT Supervision of the Banking Sector

Risk-based supervision

5.2.26 The 2019 ME Report notes that the HKMA applies a RBA for AML/CFT supervision and has a good understanding of risks in the banking sector. Over the past years, the HKMA has continued to develop and enhance its risk-based supervision of banks' AML/CFT systems and controls. Supervisory engagements with banks through on-site examination, off-site reviews or other means are graduated according to the ML/TF risks presented by different segments of the banking sector and by individual institutions.

5.2.27 Provision of guidance and feedback, particularly on current and emerging risks and the effectiveness of controls in mitigating those risks, remains a key supervisory priority for the HKMA. A Supervisory Policy Manual "Supervisory Approach on Anti-Money Laundering and Counter-Financing of Terrorism" was published in October 2018 to articulate the HKMA's overall policy and risk-based supervisory approach in a single document for greater transparency, with a focus on effectiveness and better outcomes in AML/CFT work. To provide stronger encouragement for banks to adopt the RBA, the Anti-Money Laundering and Counter-Financing of Terrorism Guideline was updated in 2018 to give greater clarity on legal requirements as well as the HKMA's expectations in terms of how efforts should target the high risk areas and consistently across the sector.

5.2.28 The HKAB and the HKMA has also worked together closely in the last few years to develop a more detailed set of FAQs to help banks understand AML/CFT requirements especially in relation to operational issues. So far, around 80 FAQs have been published since 2018 and updated from time to time in the light of market development. The HKMA also uses other means such as regulatory circulars, seminars and webinars to provide timely guidance and feedback to the banking sector, making materials available on the dedicated AML/CFT page of the HKMA public website. A dedicated online training platform was launched in September 2021 to make various presentation materials available for capacity building of staff of banks with AML/CFT responsibilities.

5.2.29 Since the publication of the 1st HRA, the HKMA has continued to increase its specialist AML/CFT resources, including the capability to respond to the increasingly complex AML/CFT environment and the use of supervisory technology ("Suptech"). In particular, part of the supervisory focus was devoted to supervising the eight VBs that commenced business in 2020. VBs have undertaken extensive preparatory work before commencing business which included establishing robust ML/TF risk management controls and comprehensive independent assessments of their AML/CFT systems. The HKMA also launched a supervisory programme, referencing to the same standards as for conventional banks, to regularly review VBs' ML/TF risk profiles and the effectiveness of their AML/CFT systems and controls after business commencement. The HKMA also collects data and information from VBs and other stakeholders in the ecosystem regarding emerging ML/TF risks faced by VBs in the light of their business models and has shared good practices adopted by VBs to address these risks.

5.2.30 The HKMA continues to apply effective, proportionate and dissuasive enforcement actions on control deficiencies and breaches of AML/CFT legal and regulatory requirements. For example, the HKMA took disciplinary actions in November 2021,

including pecuniary penalties totalled HK$44.2 million and remedial orders to rectify the shortcomings, against four banks for infringements of the AMLO, mainly in the areas of ongoing monitoring of customer relationships and conducting enhanced customer due diligence ("EDD") in high-risk situations.

Box 5.6 - De-risking

As indicated in the recent FATF publication, de-risking remains a challenge for many sectors globally and is contrary to the core philosophy of the RBA promoted by the FATF and international regulators. As an international financial centre, Hong Kong cannot be immune to this phenomenon. The HKMA aims to maintain a robust AML/CFT regime, which does not restrict access by legitimate businesses and ordinary residents to essential banking services. Since 2016, the HKMA has been working closely with the banking industry and the business community to tackle issues associated with opening and maintaining bank accounts. In addition to the guidance issued in 2016, the HKMA has encouraged banks to launch the Simple Bank Account service[128] and set up a dedicated email account and hotline to deal with relevant inquiries and follow up. Following these initiatives, the average rate of unsuccessful account-opening applications has fallen from around 10% in early 2016 to less than 4% of total applications in 2021.

Use of data and technology

5.2.31 The HKMA has significantly strengthened the use of data and technology in its own risk-based AML/CFT supervision as well as proactively encouraging greater industry adoption to help more effectively identify, understand and mitigate risk. For example, in 2018, a more proactive and targeted approach to evaluating the effectiveness of banks' screening systems was introduced, involving thematic reviews supported by a leading global Suptech provider and enabling the HKMA to target risks in banks' systems at a level of detail that had not been possible previously. This was followed in 2019 by the implementation of the AML/CFT Surveillance Capability Enhancement Project[129] under the HKMA's Digitalisation Programme, with the aim of strengthening the use of data and technology in its risk-based AML/CFT supervision, central to which are the enhancement of its data driven supervision capability as well as the development of a macro analytics capability. In addition to managing and improving data governance, Suptech-enabled process enhancements are strengthening the forward-looking assessment of risks. Automation has allowed more data to be ingested efficiently and frequently, providing more up to date, enhanced analysis of key risk areas through visualization tools.

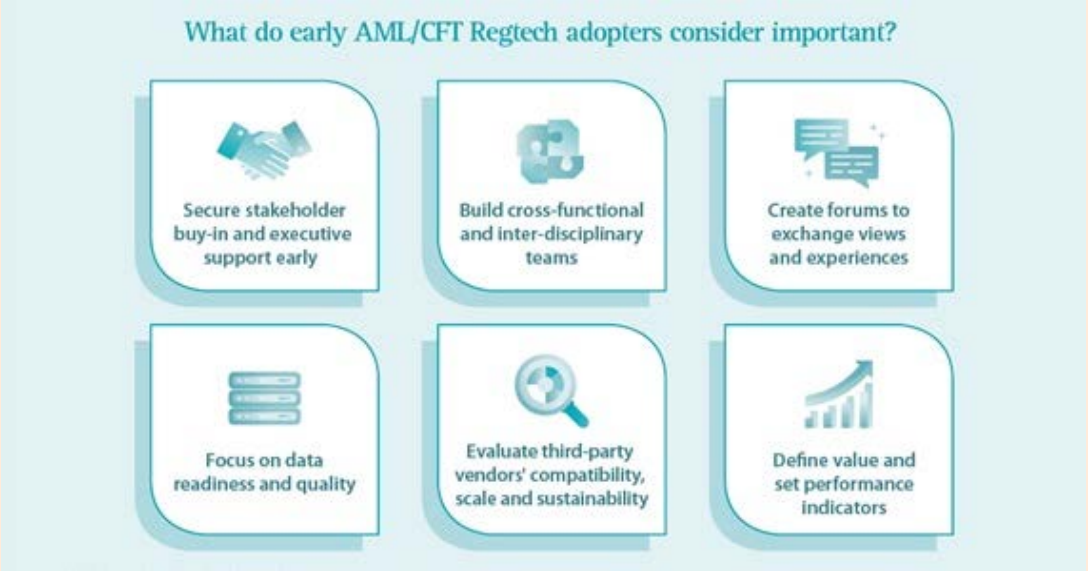
5.2.32 The HKMA also recognises the importance of banks being able to use Regtech and continues to encourage and enable banks' responsible innovation and Regtech adoption for AML/CFT as a core part of its supervision. Since the AML/CFT Regtech Forum

[128] Introduced in April 2019, Simple Bank Account services are, in essence, a tier of accounts derived from traditional accounts focusing on the provision of essential banking services such as deposits, withdrawals, local and cross-border remittances. With narrower service scope and transaction volume compared to traditional accounts, the risks involved in Simple Bank Accounts would be relatively lower and hence less extensive CDD measures required.

[129] Details of the AML/CFT Surveillance Capability Enhancement Project can be found in the report "AML/CFT Supervision in the Age of Digital Innovation", published in September 2020.

in 2019, the HKMA has undertaken a variety of initiatives, including, for example, a knowledge and experience-sharing workshop on network analytics with FMLIT member banks and issuance of "AML/CFT Regtech: Case Studies and Insights", which shared practical hands-on experience and use cases of banks that have implemented AML/CFT Regtech to address a number of themes.

Figure 5.4: Publishing AML/CFT Regtech: Case Studies and Insight for Experience Sharing



5.2.33 Pursuant to the next phase of the work under the HKMA's "Fintech 2025" strategy which aims to encourage the financial sector to adopt technology comprehensively, the HKMA launched the AMLab series in November 2021 to strengthen banks' capabilities to protect customers from fraud and financial crime losses, with the first AMLab focusing on using network analytics to address the risks of fraud-related mule accounts and enhancing data and information sharing through public-private partnership efforts in AML.[130] Some of these techniques are already delivering improved outcomes (see Chapter 3), such as neutralising mule account networks, filing of proactive STRs and sharing more FMLIT alerts, which have greatly aided the wider sector's assessment and understanding of specific ML/TF risks. The collective ability of the banking sector to reduce the risk of ML networks using data, analytics, information-sharing and collaboration[131] has been improved as a result.

International cooperation and engagement

5.2.34 Subsequent to the action plan set out in the 1st HRA, the HKMA has established an AML/CFT supervisory cooperation arrangement with the PBOC. The HKMA conducted an on-site examination of a Mainland subsidiary of a Hong Kong-incorporated bank in 2019. As part of home-host cooperation, the HKMA met with the PBOC during the visit and exchanged views on examination findings on the institution being examined.

[130] Details of the AMLab can be found in: "HKMA launches AML Regtech Lab", published on 5 November 2021.

[131] A circular "Supporting the Use of New Technologies for AML/CFT: Suggested Actions for the Hong Kong Banking Sector", which sets out the next steps that will be taking as part of the HKMA's broader "Fintech 2025" strategy, was published on 11 August 2021. These initiatives are part of the HKMA's ongoing response to the work of the FATF and, in particular, its recent report "Opportunities and Challenges of New Technologies for AML/CFT".

5.2.35 The HKMA also maintains good relationships with AML/CFT supervisors globally and participates actively in AML/CFT international work. In addition to the AML/CFT Expert Group of the Basel Committee on Banking Supervision, the HKMA continues to participate in the FATF and the APG on ML and draw banks' attention to the latest international regulatory developments. In particular, the HKMA is co-chairing the Evaluations and Compliance Working Group of the FATF since February 2020, and also contributed three financial assessors for Mutual Evaluations, two reviewers for follow-up reviews and two experts for technical compliance re-rating reviews to the FATF and APG in the latest round of the peer review process.

ML Risks

5.2.36 Taking into account the ML threat and vulnerability levels for the banking sector, which are assessed to be high and medium-high, respectively, the ML risk level for the sector is assessed to be high. These ratings are the same as those in the 1st HRA.

Next Steps

5.2.37 The HKMA will continue to work closely with banks and other competent authorities to mitigate the high ML risks in the banking sector and has identified a number of areas for action:

(a) **Understanding of risk**: Continuing to strengthen the understanding of ML/TF risks, including new and emerging risks to enable proactive responses;

(b) **Supervision**: Staying vigilant to changing threats and vulnerabilities faced in the age of digital innovation and making efficient use of HKMA resources with wider adoption of Suptech tools and a more data-driven approach, to enhance our ability to take supervisory actions quickly and effectively;

(c) **Innovation**: Continuing to support innovation and the adoption of Regtech by banks to deliver improved outcomes in AML/CFT work and further reduce regulatory compliance burden;

(d) **Collaboration**: Scaling-up and enhancing public-private information sharing through the FMLIT and other initiatives, particularly for mitigating threats such as fraud and mule account networks; and

(e) **Sustainability**: Building sector-wide resilience through more timely and responsive education, outreach and awareness programmes that support a more holistic and sustainable response to ML/TF and other financial crimes.

5.3 SECURITIES

5.3.1 Despite heightened volatility as a result of the COVID-19 pandemic, Hong Kong has continued to be one of the world's most active and liquid securities and futures markets[132] and a top listing venue[133]. Hong Kong has also continued to be a leading asset and wealth management centre in Asia, with HK$ 34.9 trillion assets under management by the end of 2020[134].

5.3.2 Hong Kong is one of the leading international financial centres with strong economic ties with the Mainland. Through Mainland-Hong Kong Stock Connect and other mutual market access schemes such as Bond Connect[135] and Wealth Management Connect[136], Hong Kong plays a unique role in facilitating capital flows between the Mainland and the rest of the world.

5.3.3 By the end of 2021, there were 3 210 LCs and 111 registered institutions ("RIs") conducting securities business in Hong Kong[137], including one VA trading platform operator licensed under the SFC's regulatory framework for VA trading platforms announced in November 2019.

5.3.4 In conducting this assessment, quantitative and qualitative information from internal and external sources[138] for the period from 2016 to 2020 has been gathered and analysed on a sub-sector[139] level to the extent possible. To achieve a more thorough assessment of the ML threats and vulnerabilities in the securities sector, the SFC engaged closely with the private sector by conducting a perception survey and focus group discussions with selected LCs to gather their views and perceptions of ML/TF risks of the securities sector and individual sub-sectors, followed by conducting a fact-finding survey on a larger group of LCs to understand the inherent ML/TF risks arising from their business operations and the AML/CFT measures they have put in place to mitigate these risks.

5.3.5 Participants in this engagement exercise were selected to ensure appropriate

---

[132] Hong Kong's securities and futures markets respectively ranked eighth and fourteenth in the world in terms of value of share trading (US$3.3 trillion) and notional turnover (US$13.2 trillion) in 2020.

[133] Hong Kong ranks the fourth globally in terms of equity funds raised through initial public offering activities in 2021. See the 2021 Annual Market Statistics published by the Hong Kong Exchanges and Clearing Limited ("HKEX").
https://www.hkex.com.hk/-/media/HKEX-Market/Market-Data/Statistics/Consolidated-Reports/Annual-Market-Statistics/2021-Market-Statistics_e.pdf

[134] See the Asset and Wealth Management Activities Survey 2020 published by the SFC.
https://www.sfc.hk/-/media/EN/files/COM/Reports-and-surveys/AWMAS2020_e.pdf

[135] Bond Connect allows Mainland and overseas investors to trade in each other's bond markets through a linkage between financial infrastructure services institutions in the Mainland and Hong Kong. Northbound Bond Connect, which allows Hong Kong and other overseas investors to invest in the China Interbank Bond Market, was launched in 2017.

[136] Wealth Management Connect allows eligible Mainland, Hong Kong and Macao residents in the Guangdong-Hong Kong-Macao Greater Bay Area to invest in wealth management products distributed by banks in each other's market through channel established between their respective banking systems.

[137] Securities business in Hong Kong is conducted by non-bank intermediaries which must be licensed by the SFC as an LC and licensed banks which must be registered with the SFC as an RI.

[138] Including supervisory findings, regulatory filings with the SFC by LCs, typology studies on ML in the securities sector, etc.

[139] In line with the 1st HRA, LCs' business activities are classified into four business sub-sectors for the ML risk assessment: brokerages, asset managers, advisers on investments, and advisers on corporate finance.

coverage of major players and some smaller ones from each sub-sector of the securities sector. A total of 127 LCs participated in this exercise upon the SFC's invitation. These firms accounted for 62% of the aggregate securities transaction value for brokerages, 53% of the aggregate assets under management for asset managers, 42% of the total fee income for advisers on investment and 31% of the total fee income for advisers on corporate finance in 2019. Upon completing the whole engagement exercise, the SFC held a debriefing session for all LC participants to share the key findings from the exercise, thereby raising their awareness of the ML risks faced by the securities sector and individual sub-sectors.

ML Threats in the Securities Sector

5.3.6 ML threat level of the securities sector remains at medium level. The level of STRs filed by the securities sector[140] and the number of ML investigation and conviction cases related to the securities sector[141] remains low. Although the value of restrained property in the form of securities was notable[142], it was primarily related to one single ML case under investigation. The ML threat level is in line with the demographics of the Hong Kong stock market whereby institutional investors[143] dominated trading activities, including AML/CFT regulated FIs in and outside Hong Kong, which lower the ML threats of the securities sector.

Transnational and cross-border ML threats

5.3.7 In light of the preponderance of non-Hong Kong investors[144] in the Hong Kong securities market, the securities sector continues to be exposed to transnational and cross-border ML threats in addition to domestic ML threats.

5.3.8 Given Hong Kong's strong economic ties with the Mainland and its status as a global equities trading centre, it is common among LCs which engage in brokerage activities to execute trades for FIs that operate outside Hong Kong and act for their underlying investors to whom the LCs may have limited information about. In the latest amendments to its AML/CFT Guideline issued in September 2021, the SFC provides guidance to LCs in assessing and mitigating the risks of cross-border correspondent relationships, which aligns with the FATF's latest standards[145].

ML threats from non-securities-related offence

5.3.9 The securities sector continues to be exposed to ML threats of being used to launder illicit proceeds derived from predicate offences conducted outside the sector. Criminally derived funds are usually first introduced to the financial system through the

[140] STRs filed by LCs accounted for 1.2% - 2.3% of STRs received by the JFIU each year between 2016 and 2020.

[141] Less than 1% of the ML investigation and conviction cases between 2016 and 2020 involved the use of the securities sector.

[142] More than 24% of the value of property restrained between 2016 and 2020 was in the form of securities.

[143] Survey conducted by the HKEX showed that around 85% of the 2020 Hong Kong stock market turnover came from institutional investors (including exchange participants' principal trading, which accounted for 28% of the market turnover).

[144] According to surveys conducted by the HKEX and the SFC respectively, non-Hong Kong investors contributed 41% of market turnover on the Hong Kong securities market in 2020 and 64% of assets under management of the asset and wealth management business in Hong Kong in 2020.

[145] Namely the FATF Recommendation 13 as amplified by the FATF's Guidance for a RBA for the Securities Sector published in October 2018.

banking sector before being transferred to the securities sector.

5.3.10 As mentioned in Chapter 4, fraud-related offences remain the key source of domestic and external ML threats in Hong Kong. The SFC has seen a surge of investment fraud cases involving ramp and dump schemes conducted in the securities market in Hong Kong (see paragraph 5.3.14 below). Use of securities accounts to launder crime proceeds from drug offences was also observed (see Box 5.7).

Box 5.7 - Use of securities accounts to launder crime proceeds generated from domestic drug trafficking

In 2017, the HKPF raided establishments in rural areas of Hong Kong with a total of 1 635 pots of cannabis plants (approximately 114.5 kg) and 450 grams of cannabis were seized (with retail value amounted to approximately HK$36.7 million in Hong Kong). Three suspects were arrested for the cultivation of cannabis plants. The HKPF conducted a financial investigation against the suspects and their family members. In-depth analysis revealed that one of the suspects (Mr A) engaged his wife to launder crime proceeds, whereby some of the proceeds were layered into securities accounts. A sum of about HK$7.2 million worth of assets, in cash, gold, securities, credit balance of banks and luxury cars, were seized or prevented from further dissipation.

In 2019, all these suspects were convicted of cultivating cannabis plants and trafficking in dangerous drugs. Mr A was also convicted of an ML offence and was sentenced to an extra 32 months' imprisonment with HK$5.5 million confiscated.

5.3.11 Hong Kong is exposed to ML threats posed by corruption and tax crimes committed in neighbouring and other jurisdictions. 46% of the LC respondents in the SFC's fact-finding survey indicated that they maintained clients who are PEPs or associated with a PEP during 2020. This type of clients poses higher risk of ML associated with corruption and tax crimes. Nonetheless, it only accounted for less than 5% of the clientele for a majority of the LC respondents having exposure to this type of clients.

ML threats from securities-related offence

5.3.12 The securities market continues to be exploited to generate illicit proceeds through predicate offences perpetrated in the securities markets, such as insider dealing, market manipulation and other forms of securities fraud. Ramp and dump schemes (which usually involved the use of social media) now account for a significant percentage of the SFC market manipulation investigations (see paragraph 5.3.14 below).

5.3.13 As part of the ongoing effort to combat market misconduct, the SFC has deployed rigorous market surveillance and leveraged the latest technology to detect unusual activities in the securities market. The SFC takes proportionate and dissuasive enforcement actions to punish and deter market misconduct perpetrated from Hong Kong and prevent the dissipation of unlawful proceeds of financial crime or misconduct.

Box 5.8 - SFC's initiatives to strengthen its market surveillance and data analytic capacities

The SFC has launched a Market Intelligence Programme under which advanced technologies were adopted to enhance the ability to identify key conduct risks in the Hong Kong financial markets. New data analytic tools were developed to manage and analyse data collected from the SFC's operations and public sources to isolate patterns and connections among individuals, companies and transactions which may indicate conduct risks.

The SFC implemented an investor identification regime for southbound trading under Mainland-Hong Kong Stock Connect in January 2020. The SFC is currently working with the HKEX to implement an investor identification regime for the Hong Kong securities market which would speed up the identification of the originators of the trade orders and therefore enhance the detection of potential market misconduct in a more timely and efficient manner.

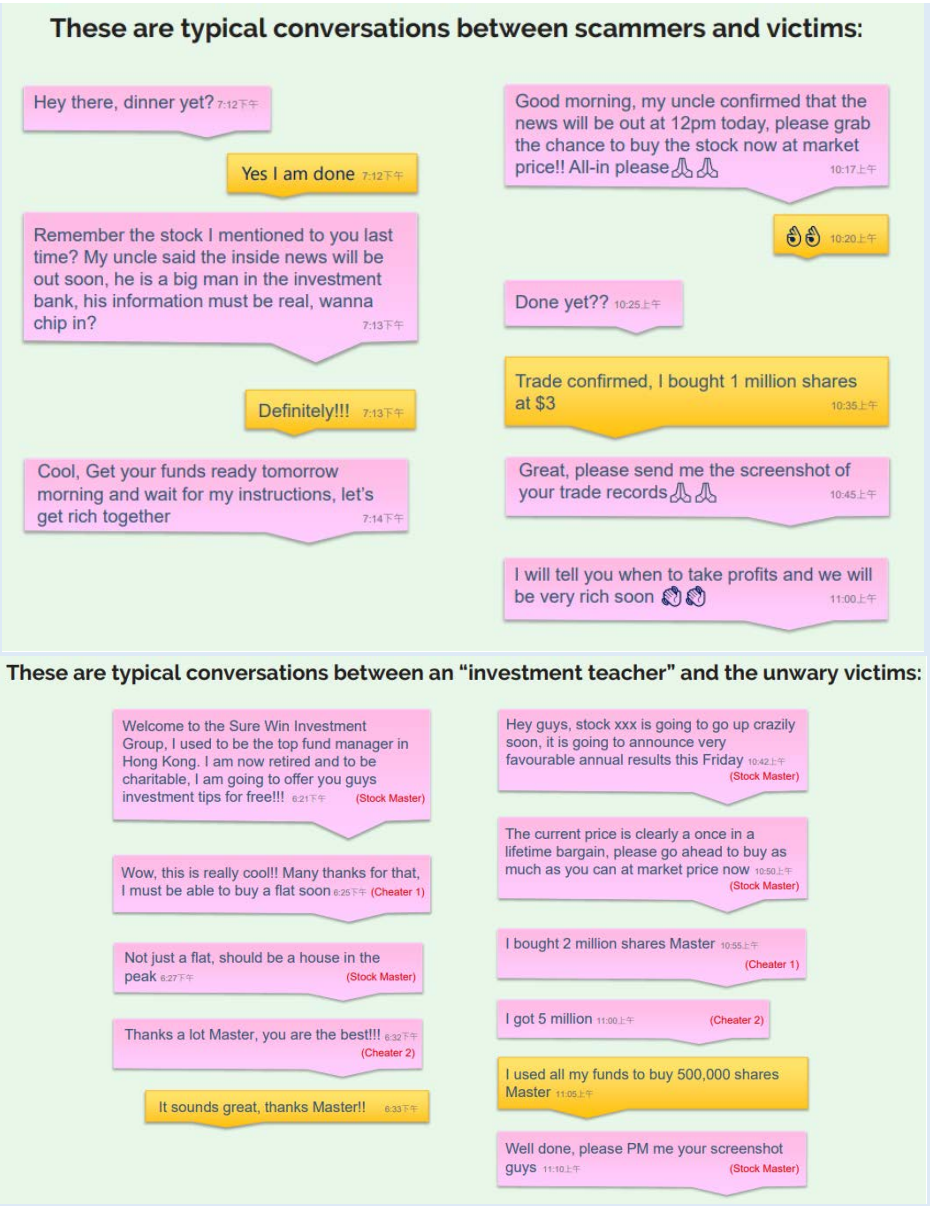
ML threats from social media investment scams

5.3.14 In line with the growth of digitalisation and the use of social media in recent years, the SFC has observed a surge of social media investment scams by way of "ramp and dump" schemes, a form of stock market manipulation whereby fraudsters "ramp" up the share price of a listed company before "dumping" onto unwary investors lured to buy the shares at artificially high price via popular social media platforms. The SFC works closely with the HKPF and/or the ICAC in some of the investigations of these scams and related ML, fraud and/or corruption offences that these cases involved. Where possible, the SFC takes action to freeze the securities accounts suspected of being part of these schemes. In addition, the SFC worked closely with the Investor and Financial Education Council and the HKPF's ADCC to raise public awareness about social media investment scams through various means, including websites, social media and community outreach events.

Box 5.9 - Typology and case example for social media investment scams

In a typical scheme, the scammers choose a thinly-traded, small-cap stock, often with a small group of shareholders holding most of the shares, and use their own securities accounts or other nominee accounts to buy a large quantity of the target stock at low prices and push up the share prices.

Investors are then approached on popular social media platforms. To convince unwary investors to buy the shares at an inflated price, scammers or their accomplices would establish relationships with them by making frequent contact on the pretext of friendship or romance; or set up investment chat groups on social media and claim to offer investment tips or inside information by identifying themselves as "investment masters" or "investment teachers" to induce investors to join.



(Source: SFC's Enforcement Reporter (September 2020 edition))

After enough unwary investors buy the stock, the scammers "dump" their own shares, causing the price to collapse. The victims will not be able to contact the fraudsters after the crash and most of the time will not know the true identities of the people who lured them into the trap.

In March 2021, the SFC and the HKPF conducted a joint operation against an active and sophisticated syndicate suspected of operating multiple ramp and dump schemes. Twelve people, including those believed to be the ringleaders of the syndicate and their associates were arrested.

Cash and valuables amounting to HK$8.1 million were seized, and a total of HK$85.5 million was either withheld by Restraint Order or prevented from dissipation by the financial institutions concerned. Prior to the joint operation, the SFC issued 16 restriction notices and froze 63 securities accounts which it believed to hold proceeds of the ramp and dump schemes belonging to syndicate members, freezing around HK$860 million worth assets.

ML Vulnerabilities of the Securities Sector

5.3.15 The overall ML vulnerability level of the securities sector remains unchanged as medium after considering the assessments of ML vulnerability of the four business sub-sectors below:

Table 5.5: ML vulnerability and number of LCs under each business sub-sector

Business sub-sector	ML vulnerability [146]	Number of LCs as at the end of 2020 [147]
Brokerages	Medium	1 538
Asset managers	Medium-low	1 813
Advisers on investments	Medium-low	1 704
Advisers on corporate finance	Low	320

5.3.16 The ML vulnerabilities of the four business sub-sectors remain largely the same as those detailed in the 1st HRA report. Notwithstanding this, there have been some significant developments in the brokerages and asset managers sub-sectors as discussed in the following paragraphs, though these developments are found to have not increased the overall ML vulnerabilities of these two sub-sectors considering the nature of and degree and extent of investor participation in these market developments, and risk-mitigating measures implemented.

VA trading, fund management and distribution activities

5.3.17 In light of the growing investor interest in VAs in Hong Kong and the ML and other risks associated with investing in VA, the SFC has, since 2017, published a number of statements and circulars to clarify how VA and some specific activities involving these assets would fall under the SFC's existing regulatory regime, stepped up investor education and taken regulatory action against those who may have breached its rules and regulations when carrying out activities related to VAs.

5.3.18 In November 2018, the SFC decided to bring VA trading, fund management and distribution services under its regulatory net and power to protect investor interests. To this end, the SFC has implemented a new approach to ensure that licensed fund managers intending to invest in VAs are subject to the SFC's oversight even when managing portfolios invested solely in VAs which fall outside the definition of "securities" or "futures contracts" in the SFO. These fund managers are required to comply with a proforma set of terms and conditions, which the SFC published in October 2019, through the imposition of licensing conditions. The licensing conditions capture the essence of the existing legal and regulatory requirements (including AML/CFT requirements) applicable to LCs, adopted as needed to better address the risks associated with VAs. For example, these fund managers are required to ensure that proper safeguards exist to mitigate ML/TF risks, especially for subscriptions made by fund investors using VAs.

[146] The ML vulnerability of each business sub-sector remain unchanged as compared to the 1st HRA.

[147] Under the SFO "single licence" regime, an LC may fall into one or more sub-sectors depending on the number and types of regulated activity it is licensed for.

5.3.19 The SFC also reminded firms that distribute funds investing in VAs that they should be licensed by or registered with the SFC[148], comply with AML/CFT and other regulatory requirements, and provide further guidance on the expected standards and practices when distributing VA funds in a circular issued on 1 November 2018.

5.3.20 In November 2019, the SFC introduced a new regulatory framework for centralised VA trading platforms, allowing platforms that operate in Hong Kong and offer trading of at least one security token apply to be licensed and regulated by the SFC. In January 2022, the SFC and the HKMA issued a joint circular to provide guidance to intermediaries on the distribution of VA-related products and provision of VA dealing and advisory services. In particular, intermediaries which provide VA dealing services are expected to comply with a set of robust standards, which include but are not limited to AML/CFT requirements, to address the risks associated with VA trading activities. The ML risk of centralised VA trading platforms and other VA service operators is assessed under the VA sector in section 5.7.

Deepening market connectivity with the Mainland

5.3.21 Wealth Management Connect and southbound trading under Bond Connect were launched in September 2021, under which eligible Mainland investors are allowed to invest in wealth management products distributed by banks in Hong Kong and trade offshore bonds through the Hong Kong bond market. To mitigate the ML/TF risks, a Mainland investor can invest under Wealth Management Connect only after he/she has opened a dedicated investment account with a bank in Hong Kong, which is obliged to conduct CDD on the investor. As for Bond Connect, only Mainland institutional investors, generally AML-obliged entities and of lower ML risk, are eligible to participate in southbound trading under the scheme.

5.3.22 Similar to Mainland-Hong Kong Stock Connect, fund flows under the two schemes are conducted and managed on a "closed-loop" basis, ensuring that funds remitted offshore by a Mainland investor will only be used to invest in eligible products. Proceeds from redemption or sales of the eligible products must be remitted back to the Mainland for the account of the Mainland investor. With the risk-mitigating factors mentioned above, this feature has significantly reduced the cross-border ML risks that may arise from the two schemes.

Introduction of open-ended fund company ("OFC") regime

5.3.23 The OFC regime was introduced in July 2018, providing a corporate fund structure in addition to the existing available unit trust structure to establish public or private investment funds domiciled in Hong Kong. The SFC is the primary regulator responsible for registering and regulating OFCs under the SFO. By the end of 2021, 48 OFCs have been set up.

[148] Under the SFO, any person who carries on a business in the distribution of interests in a CIS (which includes a fund which invests in VAs regardless of whether or not these assets constitute "securities" or "futures contracts" in the SFO) in Hong Kong or to the Hong Kong public is required to be licensed or registered for Type 1 regulated activity (dealing in securities) unless an exemption applies.

5.3.24 The introduction of the OFC regime in itself should not increase the vulnerabilities of the securities sector as the investment manager of an OFC and intermediaries involved in the sale of OFC shares in Hong Kong must be persons licensed or registered with the SFC who are subject to AML/CFT requirements. That said, the SFC has taken steps to enhance and ensure that the AML/CFT measures regarding OFCs align with the FATF standards on transparency and beneficial ownership of legal persons. In particular, AML/CFT obligations will be explicitly imposed on OFCs and they are required to appoint a responsible person (who must be AML/CFT obliged person in Hong Kong) to carry out AML/CFT functions as stipulated in the AMLO.

Key ML vulnerabilities

5.3.25 Apart from the key vulnerabilities identified in the last HRA[149], the SFC observes that "nominee" and dubious investment arrangements have been exploited for use in schemes of market misconduct or in concealing the actual beneficial ownership for other illegal purposes. The increased use of online trading and remote office arrangement due to the COVID-19 pandemic also provide new opportunities for criminals to abuse the sector for online fraud and theft and related ML activities.

"Nominee" and dubious investment arrangements

5.3.26 The SFC notes the prevalent use of "nominee" arrangements to facilitate market misconduct in brokerages sub-sector where nominee clients took instructions from "masterminds" and participated in activities to manipulate share prices or conceal actual shareholding in a listed company.

5.3.27 In the SFC's supervision of asset managers, dubious investment arrangements and transactions involving private funds or discretionary accounts were also observed where the investors gave instructions on how to structure the private funds or discretionary accounts, what investments to make and when to make them. These arrangements and transactions were not commensurate with the intended nature and purpose of the business relationship, and in some cases raised red flags of "nominee" arrangements or concealing the actual beneficial ownership for other illegal activity which may present a higher ML risk.

5.3.28 Industry respondents to the SFC's perception survey also perceived "nominee" arrangement and the use of legal persons or arrangements to obscure the source of funds as the main methods of ML in the brokerages and asset managers sub-sectors.

5.3.29 The SFC issued advisory circulars in October 2018 and November 2019 respectively to remind brokerages and asset managers to be vigilant in looking out for red flags that may indicate the existence of such arrangements or transactions and caution LCs not to disregard these arrangements or transactions which may facilitate their clients or other entities for conducting illegal activities or avoiding or contravening laws, rules or regulations. Relevant illustrative risk indicators or indicators of suspicious transactions have also been incorporated into the SFC's revised AML/CFT Guideline published in September 2021 to assist LCs in conducting their ML risk assessments and identifying suspicious transactions.

[149] The key ML vulnerabilities identified in the last HRA were in the areas of third-party deposits and payments, use of technology for online onboarding, and cybersecurity associated with internet trading.

Box 5.10 - Examples of red flags that may indicate "nominee" and dubious investment arrangements

- Business relationships established in unusual circumstances. For instance, an investor instructed a fund manager to set up multiple funds which invested in a single stock, but these funds were only subscribed by persons who were related to the investor or with funds provided by the investor.

- Use of legal persons or arrangements as personal asset-holding vehicles without any commercial or other valid reasons. For instance, a private fund was set up for an investor, but apart from a transfer of shares owned by the investor into the fund, no other transactions, or only minimal transactions, were carried out by the asset manager for the fund.

- Multiple new customers are referred by the same individual to open accounts for trading in the same security within a short period of time.

- A customer's legal or mailing address is associated with other apparently unrelated accounts; or does not seem connected to the customer.

5.3.30 The SFC's fact-finding survey indicated that industry participants have generally taken heed of the SFC's advice to put in place measures to detect and prevent suspicious "nominee" arrangements to mitigate their risks.

Remote onboarding

5.3.31 With the advancement in fintech and the need for social distancing during the COVID-19 pandemic, there is a notable increase for clients to open and operate trading account online[150]. Similar to the banking sector, remote client onboarding without adequate controls for client identification and verification poses a higher risk of impersonation. The ML risks may be aggravated by the speed of electronic transactions, multiple fictitious accounts and the use of stolen identities.

5.3.32 To address these risks, the SFC issued advisory circulars in October 2016, July 2018 and June 2019 to provide guidance on acceptable approaches to comply with client identity verification requirements for non-face-to-face account opening, which specify alternative procedures that provide safeguards to contain the risks while enabling LCs to onboard clients online. The SFC also conducted a thematic review on online brokers in 2021, emphasising AML/CFT procedures in onboarding new clients.

Cybersecurity – Online and mobile trading

5.3.33 With online trading applications now more easily accessible and spurred by the COVID-19 pandemic and social distancing measures, people are spending more time on social media and conducting various activities online, including banking and investing. The

[150] 27% of the fact-finding survey respondents (which were primarily brokerages) noted increase in number of clients onboarded via non-face-to-face channels during the COVID-19 pandemic.

growing volume of online trading activities provides opportunities for criminals to exploit the cybersecurity vulnerability of online brokerages to conduct unauthorised securities trading transactions in clients' internet trading accounts.

5.3.34 To ensure the proper management of hacking risks associated with internet trading, the SFC issued guidelines requiring all LCs engaged in internet trading to implement 20 baseline requirements to enhance their cybersecurity resilience in October 2017, followed by a thematic review of online brokerages to assess their compliance with the baseline requirements in 2019. A report on the thematic review which summarised the key findings and observations was published in September 2020. The report noted that there were no reports of hacking of client accounts after the baseline requirements became effective, and most LCs complied with the SFC's key regulatory requirements. The report elaborated on the regulatory expectation in relation to the baseline requirements and also provided guidance on the SFC's expected standards in relation to mobile trading applications which assist LCs in managing associated risks.

Cybersecurity – Remote office arrangements

5.3.35 The increased use of remote office arrangements[151] during and following the COVID-19 pandemic provides opportunities for criminals to exploit vulnerabilities in remote access applications and processes to derive illicit gains from online fraud and theft. Some industry participants involved in the risk assessment exercise reported to have observed a rise in cybercrimes during the COVID-19 pandemic. The SFC also received reports by some LCs falling victim to cybercrimes such as ransomware attacks or business email scams whereby the LCs were tricked into transferring funds to the bank accounts controlled by the scammers.

5.3.36 In April 2020, the SFC issued a circular to remind LCs to assess their operational capabilities and implement appropriate measures to manage the cybersecurity risks associated with remote working arrangements during the pandemic. This message was reinforced in a report published by the SFC on 4 October 2021, which set out regulatory standards to promote the operational resilience of LCs and discuss in particular measures related to information, communication and technology to manage the major possible risks of remote working arrangements.

Third-party deposits and payments

5.3.37 Third-party deposits and payments continue to be a key ML vulnerability, particularly in the brokerages sub-sector, as criminals may exploit the arrangement and use a third party to pay for or receive proceeds of investment transactions in order to obscure the identity of the beneficial owner or the source of illicit funds. During the period from 2018 to 2020, four brokerages were publicly reprimanded and fined by the SFC for failure to comply with AML/CFT requirements when handling third-party fund deposits and/or transfers. Around one-third of the brokerage respondents in the SFC's fact-finding survey indicated that they handled third-party deposits and payments in 2020.

5.3.38 The SFC issued an advisory circular in May 2019 to reiterate the importance of mitigating the risks associated with third-party deposits and payments and provide LCs with

[151] When staff work remotely, they may access the LC's internal network and systems from outside the office and hold meetings through videoconferencing platforms.

guidance on the policies, procedures and controls to mitigate these risks, such as the due diligence process for assessing third-party deposits and payments[152]. This guidance has been incorporated into the SFC's revised AML/CFT Guideline published in September 2021.

AML/CFT Supervision of the Securities Sector

Risk-based supervision

5.3.39 The SFC adopts a RBA to monitor LCs' AML/CFT compliance and maintains a good understanding of the securities sector's ML/TF risks, building on its ongoing supervision activities, which comprise on-site inspection and off-site monitoring with intensity and frequency vary according to the ML/TF risk profiling of individual LCs.

5.3.40 The SFC has further strengthened its risk-based AML/CFT supervision by implementing the Manager-In-Charge regime for eight-core functions including AML/CFT in October 2017 and launching a revamped Business and Risk Management Questionnaire for completion by all LCs for each of their financial years ending on or after 31 March 2019. The revamped Business and Risk Management Questionnaire collects more information about LCs' business operations and AML/CFT controls, enabling the SFC to conduct off-site monitoring of LCs' AML/CFT compliance in a more risk-sensitive and effective manner.

Updates on AML/CFT Guideline

5.3.41 The SFC reviews and revises its AML/CFT Guideline from time to time to align with the latest international standards as part of its continuous efforts to keep the guidance provided to LCs and their senior management in designing and implementing policies, procedures and controls for meeting their AML/CFT obligations useful and up-to-date.

5.3.42 In the latest amendments to its AML/CFT Guideline issued in September 2021, the SFC provides guidance on applying AML/CFT measures in a more risk-sensitive manner and addresses some areas for enhancement identified in the September 2019 ME Report of Hong Kong published by the FATF which are relevant to LCs[153]. The SFC also updated the FAQs from time to time to assist LCs in designing and implementing policies, procedures and controls for meeting their AML/CFT obligations.

Capacity building and outreach programmes

5.3.43 LCs generally have a good understanding of ML/TF risks and their obligations relating to ML, TF and PF, and apply appropriate preventive measures. The majority of larger-sized LCs performed AML/CFT systems review and ongoing compliance checking to ensure the effectiveness of their systems and compliance with regulatory requirements and internal policies and procedures in relation to CDD, transaction monitoring and screening controls. The SFC will continue to step up capacity building and outreach programmes, in particular among smaller-sized LCs, with a view to improving their understanding of ML/TF

[152] Third-party deposits and payments should be accepted only under exceptional and legitimate circumstances and when they are reasonably in line with the customer's profile and normal commercial practices. LCs should critically evaluate the reasons and the need for third-party deposits and payments; take reasonable measures to verify the identities of the third parties and ascertain the relationship between the third parties and the customers; and obtain approval from senior management for the acceptance of a third-party deposit or payment.

[153] For example, by expanding the list of examples of risk indicators to facilitate risk assessments and enhancing the list of red-flag indicators for suspicious transactions.

risks, implementation of AML/CFT measures and sanctions screening controls for compliance with their statutory obligations on TF and PF, and suspicious transaction monitoring and reporting.

5.3.44 As part of its ongoing effort to improve LCs' AML/CFT compliance, the SFC shares key observations identified from inspections, provide feedback and further guidance on LCs on areas where deficiencies and inadequacies were identified in some LCs' application of AML/CFT measures through advisory circulars and regular AML/CFT seminars hosted by the SFC and various industry associations for licensed persons. For instance, the SFC issued an advisory circular in December 2020 and conducted eight AML/CFT seminars for LCs and industry associations to share findings from inspections carried out in 2019 and 2020.

5.3.45 The SFC also updates LCs on the latest regulatory developments and risk issues to assist the industry in identifying suspicious transactions and remaining vigilant on risk trends. For instance, the SFC issued an advisory circular in July 2021 to inform LCs of the FATF's adoption of guidance on PF risk assessment and mitigation. In light of the rising number of suspected ramp and dump scams, the SFC issued an advisory circular in June 2021 to provide securities intermediaries with guidance on red flags which may arouse the reasonable suspicion of intermediaries or their staff about the suspected ramp and dump scams and warrant an assessment of whether the associated trading activities should be reported to the SFC.

5.3.46 In addition, the SFC discussed the latest AML/CFT regulatory developments in the compliance forums for industry participants in 2019 and 2020 and ongoing dialogue with industry associations from time to time. Presentation materials for AML/CFT seminars and other SFC's publications relating to AML/CFT are made available on a designated AML/CFT webpage of the SFC's website for ready access by industry participants.

Use of technology

5.3.47 It is also observed that there is a higher level of use of technology to support AML/CFT compliance[154] among larger-sized LCs, particularly brokerages that have larger client bases and process a high volume of transactions. The securities sector is expected to adopt more advanced technologies to improve their AML/CFT compliance while achieving cost-effectiveness with the use of Regtech.

5.3.48 In recognition of the potential of new technologies to make AML/CFT faster, cheaper and more effective, the FATF recently published a report on "Opportunities and Challenges of New Technologies for AML/CFT" to raise awareness of relevant progress in innovation and specific emerging and available technology-based solutions for AML/CFT, and examine the challenges and obstacles to their implementation and how to mitigate them. In its circular issued on 7 July 2021 and an AML/CFT seminar held in December 2021, the SFC drew to the attention of LCs of the above FATF report so as to raise their awareness of how they may use new technologies to improve the efficiency and effectiveness of their AML/CFT measures.

[154] Mainly in the areas of screening, CDD and transaction monitoring.

Mainland and international cooperation

5.3.49 The SFC has strengthened supervisory cooperation with the China Banking and Insurance Regulatory Commission and the China Securities Regulatory Commission by entering into a MoU with each of them in 2018. The MoUs facilitate cooperation and exchanges of information in the supervision of FIs operating on a cross-border basis in the Mainland and Hong Kong.

5.3.50 The SFC has also strengthened supervisory cooperation with the German Federal Financial Supervisory Authority by entering into MoU in June 2018. The MoU facilitates cooperation and information exchanges in the supervision of FIs operating on a cross-border basis in Hong Kong and Germany.

Enforcement

5.3.51 The SFC continues to take effective, proportionate, and dissuasive enforcement actions for violation of AML/CFT requirements to prevent LCs from being used as conduits for transferring suspicious funds into the capital markets in Hong Kong. In its focused investigations into suspected AML/CFT regulatory breaches and related internal control failures by LCs, the SFC's investigations also hone in on the firms' senior management and other individuals who are accountable for the violation. During the period from 2018 to 2020, disciplinary actions taken by the SFC on these cases resulted in public reprimands and fines totalling more than HK$2,783 million against seven LCs and two licensed representatives and licence suspension / prohibition from re-entering the industry of four responsible officers / former responsible officers.

ML Risks

5.3.52 Taking into account the ML threat and vulnerability levels for the securities sector discussed above, which are both assessed to be medium, the ML risk level for the sector is assessed to be medium.

Next Steps

5.3.53 The SFC will continue to enhance its risk-based AML/CFT supervision and LCs' AML/CFT compliance capability to mitigate the ML risks in the securities sector and has identified the following areas for further action:

(a) The SFC is in the process of reviewing the data available and considering further enhancements to the data collection and the use of data analytics to enhance its risk-based AML/CFT supervision of LCs; and

(b) The SFC will continue to monitor the development and adoption of new technologies for AML/CFT and share relevant information and provide guidance where appropriate to help the industry to overcome challenges and realise the promise of responsible use of new technologies to strengthen the effectiveness of AML/CFT measures in the securities sector.

5.4 MONEY SERVICE OPERATORS

5.4.1 In Hong Kong, any person who wishes to operate a money service (i.e. money-changing or remittance service) must have a licence granted by the CCE unless an exemption applies under the AMLO. Since the 1st HRA, the total number of MSOs has decreased from 1 309 to 805 in 2021. This is mainly attributable to the tightened entry control and decrease of market activities due to the COVID-19 pandemic. Among the 805 licensed MSOs, 621 licensees (77%) operated in particular premises, and 184 licensees (23%) were MSOs providing money service without particular premises but maintaining personnel of their business/corporation in a local management office set up in Hong Kong.

5.4.2 As regards the profiles, the MSOs operating at particular premises could be broadly sub-divided into four categories, namely traditional MSOs operating at street level or within shopping arcades (53% of the total number of MSOs), MSOs which are serving FDHs (12%), MSOs running other side businesses (9%) as well as MSOs only serving corporate customers which are not open to the public (3%). The majority of the licensed MSOs carried on both money changing and remittance businesses. For MSOs operating without particular premises, they are mainly service providers of point-of-sale ("POS") payment platforms, partners of third-party payment licensees in the Mainland, and web-based platforms or mobile applications providing remittance service.

5.4.3 With technological advancement reinforced by the COVID-19 pandemic, the business model of the MSO sector has undergone significant changes in recent years. Nevertheless, cross-border fraud remains the largest ML threat to the MSO sector. With an increase of MSOs operating on POS payment platforms and web-based platforms or mobile applications providing remittance service, cybercrime may become another emerging threat to the MSO sector.

ML Threats in the MSO sector

5.4.4 The MSO sector remains exposed to medium-high ML threats arising from domestic and foreign criminal activities. Between 2016 and 2020, the sector was involved in 9.9% of ML convicted cases and 3.6% of crime proceeds laundered via MSO or unlicensed money service operation ("UMSO"). MSOs are observed to be used in the placement and layering stages of ML. Between 2016 and 2020, MSOs filed 0.98% to 3.56% of all STRs, third to banks and SVF licensees.

Fraud

5.4.5 Similar to the findings of the FATF's study[155] and APG's Typologies Reports[156], the MSOs sector is prone to be used as a conduit for criminals to place illicit fund into the financial system and transfer it to other jurisdictions/regions. Typologies study on ML cases involved the use of MSO between 2016 and 2020 revealed that fraud, including telephone deception, email scam and lottery fraud, posed the most prevalent threat to the MSO sector, followed by other predicate offences such as drug trafficking, smuggling, and theft. Use of

[155] Money Laundering through Money Remittance and Currency Exchange Providers published by the FATF. https://www.fatf-gafi.org/media/fatf/ML%20through%20Remittance%20and%20Currency%20Exchange%20Providers.pdf

[156] 2020 APG Yearly Typologies Report. http://www.apgml.org/includes/handlers/get-document.ashx?d=e2e2d9c7-47f7-4864-8689-556c11c02e27

money mules, who were recruited to receive crime proceeds and facilitate remittance for remuneration, was observed to be a common ML method for fraud cases.

Box 5.11 - Case study on telephone deception using money mules

This case stemmed from a telephone deception case in Hong Kong. Between March and April 2017, an old lady victim, upon receiving phone calls from persons purporting to be officials of Hong Kong and the Mainland authorities, was deceived into paying a total of HK$3.95 million (via three cheques) for exoneration of her suspected crime in dealing with crime proceeds. Upon investigation, a person D was found to be helping with the laundering of the crime proceeds by first collecting the three cheques from the victim, then depositing the cheques into her bank account and remitting an equivalent amount in RMB to the Mainland via a licensed MSO.

D was convicted of "Dealing with property known or believed to represent proceeds of indictable offence" and was sentenced to 25 months' imprisonment.

5.4.6 In light of the susceptible ML risk as well as for the purpose of crime prevention, since May 2017, the C&ED has conducted ten joint publicity operations codenamed "APPLESHINER" with the HKPF to raise the MSOs' alertness to suspicious remittance transactions, particularly those involving the clients suspected to be victims of telephone deception cases. In general, the sector is aware of the threat posed by fraud cases and maintains a high level of vigilance in preventing the occurrence of fraud by intercepting the suspicious remittance in the course of their business. As a result, MSOs have successfully intercepted 62 telephone deception cases up to 2020 and prevented HK$29.18 million from being defrauded. As MSOs may act as the last stop to send money from victims of local deception cases out of Hong Kong, the C&ED highlighted relevant threats arising from the emerging phone/cyber scams in the educational outreach, seminars and small group workshops with a view to updating the MSOs on crime prevention awareness and the latest threats posed to the sector.

Cybercrime

5.4.7 The C&ED notes in recent years an upward trend of the number of MSO licensees operating online money service platforms without particular premises leading to a larger amount of online transactions. With the increasing proportion of online transactions, cybercrime may become an emerging ML threat to the sector. To this end, the C&ED has imposed strict entry requirements for the MSO sector, and at the same time MSO licensees are required to put in place effective policies, procedures and internal controls to address the ML/TF risks involved. For example, when considering their proposed business plan, the C&ED will consider whether there are sufficient risk-mitigating measures on identifying and verifying non-face-to-face customers.

Hawala

5.4.8 Hawala is an alternative remittance system outside of the traditional banking system. Unlike the conventional method of actually moving money across borders through bank wire transfers, money transfer in hawala is arranged through a network of hawala brokers who operate based mainly on trust and communication. Transactions between

hawala dealers can be settled in cash, property or services.

5.4.9 Hawala is not common in the MSO sector, and the C&ED seldom receives intelligence or complaints of hawala. However, to have a comprehensive understanding of the FDHs' preference in remittance and the potential risks posed by the niche market, starting from 2020, the C&ED has conducted a thematic study on the remittance behaviour of FDHs and the delivery channels of MSOs who mainly provided services to FDHs. The study found that FDHs predominantly made their remittances through licensed MSOs and the actual transfer of money, in particular overseas remittances to the recipients in the Philippines and Indonesia, was generally completed by way of bank transfer instead of relying on the trust-based network of hawala. As part of the ongoing efforts to enhance supervision of the MSO sector, the C&ED will continue to encourage the public, including NEC, to utilise licensed MSOs for money services, and take enforcement action against UMSO activities, whether involving hawala or not.

5.4.10 To conclude, hawala is not a prevalent practice in the FDH group to transfer funds to their homelands. No information or intelligence indicates that the MSO sector is adopting hawala as a way for money remittance. Therefore, it is assessed that such an alternative remittance system still poses no obvious threat to the sector.

ML Vulnerabilities of the MSO sector

5.4.11 The threats and vulnerabilities affecting MSOs are not uniform because of variations in their size and business models. As elaborated in paragraph 5.4.2 above, the MSO sector is diverse in terms of the business nature, scale and mode, of which the MSOs range from local small-scale brick and mortar stores for providing traditional money service to international corporations with global money transfer networks. With its cash-intensive nature with global exposure, the MSO sector is inherently vulnerable to higher ML threats.

5.4.12 It is recognised that transactions involving personal and trade-based funds, frequent and cross-border transactions, large-amount transactions by walk-in and one-off customers pose medium-high ML vulnerability to the MSO sector. The use of online platform through MSOs operating without particular premises, widespread use of cash and transactions below customer identification and verification thresholds also pose relatively higher ML vulnerability. MSOs, particularly the smaller sized ones with fewer resources to build up their ML/TF risk understanding and set up an effective compliance control system to properly implement CDD and ongoing transaction monitoring, leave themselves vulnerable to exploitation by criminals seeking to launder funds.

5.4.13 To mitigate the ML vulnerability to the MSO sector, the C&ED has enhanced the regulatory regime to implement more proper and proportionate licensing requirements. Since 2020, MSO licence applicants have been required to clearly disclose their fund flow and delivery channels in their business plan and to demonstrate that effective and proportionate AML/CFT measures are put in place. For existing MSO licensees, the C&ED launched a sector-wide outreach programme in which improving the MSO's awareness and understanding of institutional risks were one of the key priorities of the exercise. For the marginal MSOs identified in the outreach, the C&ED would take necessary follow-up supervisory actions such as providing the MSOs with relevant AML/CFT guidance or tailor-made training to make up the deficiencies concerned.

AML/CFT Supervision of the MSO Sector

Supervision and Enforcement

5.4.14 Since the 1st HRA, the C&ED has stepped up efforts in implementing a robust licensing regime for the MSO sector. The entry requirements have been reviewed and strengthened to ensure that qualified MSOs meet their AML/CFT obligations effectively. In addition, the C&ED has revamped its RBA supervision, supplemented by on-site supervision and off-site monitoring according to the risk level of the MSO. The C&ED will also carry out theme-based inspections targeting areas of non-compliance.

Risk-based approach

5.4.15 To establish a robust basis for implementing risk-based supervision, the C&ED has launched a revamped risk profiling methodology with a systematic and comprehensive set of risk parameters. Under the enhanced risk model, each MSO will be given an overall risk rating and an impact rating reflecting its annual turnover which will be combined into a matrix to determine the appropriate supervisory extent and priority. Coupled with ongoing off-site monitoring, a high, medium-high, medium or low supervision priority category is assigned to all MSOs, which will then be subject to a proportionate supervisory engagement.

5.4.16 The C&ED has been actively adopting the enhanced risk model to determine the ML/TF risk level of individual MSOs in the targeted outreach exercises. Ongoing risk assessment has been conducted by making use of a wide range of avenues, for example, periodic risk profiling, examination of the business plan and AML/CFT policy submitted by the applicants/licensees, analysis of regular business returns, feedbacks collected from on-site interviews, etc. to ensure that the risk ratings of individual MSOs are up-to-date. The outreach exercises' outcomes have contributed significantly to formulating the supervision priority categories and refining our risk-based supervisory strategies.

Entry control

5.4.17 The C&ED applies strict entry controls for the MSO sector. Before granting or renewing an MSO licence, the C&ED will go through the background due diligence of the applicants to ensure that they are fit and proper. Between 2016 and 2021, the C&ED suspended 67 MSO licences, revoked 137 MSO licences, and refused to grant MSO licences to 430 applicants on fit-and-proper grounds.

Ongoing risk-based supervision

5.4.18 The C&ED conducts compliance inspections on MSOs using an RBA and will initiate dissuasive and proportionate sanctions in the event of non-compliance. MSOs are required to lodge quarterly returns to report transaction volumes, STR reporting figures, etc. for monitoring purposes. Between 2016 and 2020, the C&ED conducted on-site and off-site inspections of 903 high-risk MSOs. In addition to the compliance on CDD and record-keeping requirements, the C&ED will also consider whether the MSO has properly implemented sanction screening and transaction monitoring regarding PEPs, terrorists and TFS implementation against the relevant sanction lists.

5.4.19 The C&ED has deployed a broader range of disciplinary sanctions proportionate and dissuasive to deal with various non-compliances, including all the three available sanctioning tools under the AMLO, i.e. public reprimand, pecuniary penalty and

taking of remedial actions. Between 2016 and 2020, the C&ED completed 13 disciplinary actions against non-compliant MSOs. These MSOs were publicly reprimanded and/or ordered to pay a pecuniary fine involving a total of HK$29,000. Among them, five MSOs were additionally ordered to take remedial actions to rectify their AML/CFT system deficiencies. The C&ED also served written warnings to seven MSOs for non-compliance with statutory obligations. For the four cases involving serious contraventions in CDD and record-keeping requirements, the C&ED took prosecution against these non-compliant MSOs who were convicted with total fines of HK$210,000.

5.4.20 Meanwhile, to enhance the MSO supervisory regime, off-site monitoring is strategically deployed to complement on-site inspections targeting MSOs of varying risk profiles under the overall risk-based operation mode. It can be used as a reliable control measure for reviewing and evaluating non-high-risk MSOs for routine check-ups or a prelude to a later on-site inspection for collecting advance information and making preliminary assessment. Those MSOs selected for off-site monitoring are required to attend interviews in the C&ED's office and provide the requisite documents for scrutiny by the C&ED within a specified period. Such a risk-focused monitoring approach serves as an effective reinforcement measure to enhance the comprehensiveness of the compliance programme and increase the overall operational flexibility in deploying supervisory actions.
5.4.21

Sanction screening and transaction monitoring system

5.4.22 Implementation of TF/PF TFS is another focus in the AML/CFT regime for the MSO sector. In submitting their licence applications, MSOs must demonstrate their capabilities in applying sanction screening and transaction monitoring mechanisms. As in paragraph 5.4.18 above, the C&ED will also consider whether the MSO has made use of the prerequisite database and screening tool to implement TFS screening during the on-site inspection.

Unlicensed money service operation

5.4.23 The C&ED maintains an up-to-date MSO licensee register, which is publicly accessible on the Internet. This public register helps distinguish licensed and unlicensed MSOs and facilitate the identification of false or inaccurate information about MSOs. To combat unlicensed MSOs, the C&ED monitors higher-risk areas through street-level patrols, cyber monitoring, surveillance of suspected unlicensed MSOs, analysis of STR referrals and intelligence as well as other sources such as complaints from the public. Between 2016 and 2020, there were 30 convictions involving UMSO. Suspended imprisonment sentences and disqualification from holding an MSO licence for a specified period were also imposed on some convicted unlicensed MSOs.

5.4.24 With a view to strengthening the enforcement capability against UMSO, a designated division for the investigation of suspected cases involving UMSO has been newly established in 2020 to conduct patrols, carry out cyber monitoring, investigate UMSO cases and further any potential ML investigations. With the extensive efforts exerted on the investigation of UMSO, in 2021, 24 cases were effected, which has increased by 50% compared to 2020. Among the cases detected, four cases were involved in unlicensed money changing transactions and 20 cases were involved in unlicensed remittance transactions, including ten UMSO operating at the social media platforms.

5.4.25 Looking ahead, the Government has proposed to amend the AMLO and increased the deterrent effect for UMSO by increasing the sentencing level to a fine of HK$1,000,000 and imprisonment for two years.

Box 5.12 - Cases

Case No.1
In 2018, the C&ED detected a UMSO case during a street-level patrol. The sole proprietor and the manager of the target precious stone shop provided unlicensed money changing service to C&ED officers disguised as walk-in customers. Both the proprietor and the manager were arrested for UMSO activities and subsequently convicted by the Court in 2019. Each of the defendants was fined HK$15,000 and disqualified from holding an MSO licence for 12 months. The Court also ordered the forfeiture of some of the seized assets, including funds involved in the illegal activities.

Case No.2
In 2019, the C&ED detected a UMSO case during a street-level patrol. The sole proprietor of the money exchange shop provided unlicensed money changing services to C&ED officers disguised as walk-in customers. During the operation, C&ED officers seized the transaction records of the shop's unlicensed money changing and remittance activities. The owner was subsequently convicted in 2020 and sentenced to two months' imprisonment suspended for two years.

Case No.3
In 2020, the C&ED initiated enforcement action against a discussion group of a social media platform offering unlicensed remittance service. C&ED officers disguised as online customers to trace the unlicensed MSOs and subsequent investigation revealed that a couple had been acting as the administrator of the discussion group and using their bank accounts to provide remittance services, involving a total of nine outward remittance transactions from Hong Kong to Thailand from December 2019 to January 2021, with a total transaction value of HK$15,360. A Thai female and a Chinese male were subsequently convicted by the Court in February 2022 and fined HK$30,600 in total.

Capacity building and outreach

5.4.26 The C&ED regularly conducts capacity building and outreach activities to strengthen the sector's understanding of emerging trends and to address their shortcomings. From 2016 to 2021, a total of 25 seminars and 27 small group workshops were organised. Through these capacity building and outreach programmes, the MSO sector has improved its understanding of AML/CFT risks and obligations, particularly on PF/TF risks and TFS implementation, and has enhanced the quantity and quality of STRs. Besides, the C&ED established a closer cooperative relationship with the InvestHK to jointly organise the webinars for local and overseas-based MSOs. The C&ED also collaborates with the Hong Kong Money Service Operators Association to exchange views on industry best practices and disseminate the latest regulatory requirements to the sector.

5.4.27 In May 2020, the C&ED launched a new round of territory-wide outreach programme. Apart from raising MSO's awareness of ML/TF risks and addressing their shortcomings to dovetail the implementation of risk-based monitoring mentioned in

paragraph 5.4.18 and 5.4.20, the outreach programme also seeks to facilitate the C&ED's assessment and determination of the risk profiles of individual MSOs as well as to assist the MSOs in formulating their own AML/CFT policies and address concerns and difficulties in adapting to the regulatory regime.

Guideline and best practice

5.4.28 The C&ED regularly reviews and updates its licensing and AML/CFT guidelines for the MSO sector. A "Supplementary Guideline on the Criteria to Determine Fitness and Propriety" was published in January 2020 to provide additional guidance to MSOs on the C&ED's latest assessment criteria on the fit-and-proper requirement. Our "Licensing Guide" was revised in August 2021 to detail the enhanced regulatory measures on MSO's licensing and compliance requirements. In addition, the C&ED issues sectoral and thematic guidance via circulars to MSOs such as guidance on conducting institutional risk assessments, filing STR, reminding MSOs of the latest licensing requirements, and keeping them abreast of information on areas of concern such as the UNSC Sanction Lists and FATF Public Statements.

ML Risks

5.4.29 The overall ML risk is therefore assessed to be medium-high, given that both the ML threat and vulnerability level of the sector is medium-high.

Next Steps

5.4.30 Looking ahead, the C&ED will –

(a) strengthen its understanding of MSOs' risk profiles, by completing the territory-wide outreach programme and conducting thematic studies, in order to form a solid foundation for effective risk-based supervision;

(b) enhance MSOs' capability in particular in ML/TF/PF risk understanding, STR reporting obligations, and TF/PF TFS screening;

(c) encourage the adoption of innovation and new technology to enhance MSOs' efficiency in AML/CFT compliance;

(d) further study the emerging ML/TF/PF threats arising from cybercrime to formulate supervisory measures and provide guidance to the MSO sector; and

(e) proactively conduct special theme-based review exercises targeting high-risk areas.

5.5 INSURANCE

5.5.1 The insurance market continues to play an instrumental role in the financial system of Hong Kong. In 2020, Hong Kong ranked first in the world by insurance penetration and second by insurance density.

5.5.2 Long-term business makes up around 90% of the market, with in-force premiums of HK$540.8 billion in 2021 (a decrease of 1.3%). Individual life and annuity business accounted for 90.8% (HK$491.2 billion) of long-term in-force business in 2021, with new individual life and annuity business premiums reaching HK$166.4 billion, of which HK$135.6 billion was non-linked long-term business, and HK$30.8 billion was linked long-term business.

5.5.3 By the end of 2021, there were 73 insurers authorised to carry on long-term insurance business in Hong Kong. The market, however, is relatively concentrated, with the top five long-term insurers making up 66% of the market and the top ten accounting for 87% in 2021. The distribution of long-term insurance products is predominately through licensed insurance intermediaries. By 2021, there were 733 licensed insurance broker companies, 380 licensed insurance agencies, and 116 237 licensed individual insurance agents carrying on regulated activities in long-term business. As licensed insurance agencies, banks accounted for 50% of the distribution of non-linked long-term business in 2021. Non-bank licensed insurance agents, predominantly serving as tied agents of long-term insurers, distributed 92% of the new business for linked long-term business products in 2021, with licensed insurance broker companies accounting for the remaining portion. In recent years, under the Fast Track authorisation route, two new virtual insurers have been authorised to underwrite long-term business and conduct business through non-traditional channels with the aim of introducing increased diversity to the distribution of long-term products and encouraging the development of digital distribution.

Box 5.13 - About the IA

The IA is a statutory body established under the IO to regulate and supervise the insurance industry for the promotion of the general stability of the insurance industry and the protection of existing and potential policyholders. The IA took over the statutory functions of the Office of the Commissioner of Insurance ("OCI") to supervise authorised insurers with effect from 26 June 2017. The IA then became responsible for regulating and supervising the entire insurance market by directly regulating insurance intermediaries on 23 September 2019 (putting an end to the previous self-regulatory regime). The IA also serves as the group supervisor of the insurance holding companies of certain global insurance groups headquartered in Hong Kong.

Since its establishment, the IA has introduced new rules, codes of conduct and guidelines establishing requirements for authorised insurers and licensed insurance intermediaries on the conduct of business, enterprise risk management, cybersecurity, continuing professional development and fit and proper requirements for intermediaries and key persons in control functions of insurers.

The IA is also empowered by the AMLO to supervise compliance by authorised insurers

carrying on long-term business, and licensed insurance intermediaries carrying on regulated activities in respect of long-term business (hereinafter referred to as "insurance institutions" ("IIs")), with all relevant requirements under the AMLO and related guidelines. The IA adopts a RBA to its AML/CFT supervisory work that considers each II's risk exposure.

The RBA framework combines on-site examinations, off-site measures, and other outreach activities. The IA also investigates suspected breaches of AML/CFT requirements and is empowered to impose disciplinary sanctions where appropriate.

To enhance cross-border and cross-sectoral supervisory cooperation, the IA/OCI has signed separate MoU or other formal arrangements with different overseas and local financial services regulators. The IA also actively participates in supervisory colleges to exchange supervisory information, including AML/CFT matters, with other insurance supervisors.

ML Threats in the Insurance Sector

5.5.4 Whilst the insurance sector bears an inherent ML threat, particularly on long-term insurance products linked to investments or with cash value build-up features, inherent ML risk is considered low by comparison to other sectors. Amongst the realisable assets from detected ML cases in Hong Kong between 2016 and 2020, only 0.1% of the restrained assets and 0.9% of the confiscated assets were in form of insurance products. There was also no complicit involvement of the staff in the insurance sector in the laundering of proceeds.

5.5.5 Given the global nature of the insurance market in Hong Kong, however, the sector is exposed to transnational ML threats. There have been isolated cases indicating that the insurance sector is susceptible to the injection of crime proceeds from foreign jurisdictions, which usually enter Hong Kong initially via the banking sector. The sector's exposure to foreign ML threat cannot, therefore, be discounted.

5.5.6 In view of the above, the ML threat level of the insurance sector is assessed as medium-low.

ML Vulnerabilities of the Insurance Sector

Payment controls implemented by insurance institutions

5.5.7 In general, IIs have demonstrated a good understanding of their AML/CFT obligations and ML/TF risks and put in place appropriate internal systems and controls to mitigate such risks, as evidenced by the increasing number of STRs filed.

5.5.8 Insurers have implemented controls on premium receipts and policy payouts to mitigate ML/TF risks. The vast majority of premium payments for long-term insurance policies are made by policyholders to insurers direct rather than routing them through licensed insurance intermediaries. Insurers have also set reasonable limits on the amount of premium payment they are willing to accept in cash.

5.5.9 Premium refunds due to policy cancellation during the cooling-off period has remained low. When they do occur, such refunds are generally made to policyholders through the same means by which the original payments were received. Policy payouts

from insurers are usually in the form of cheques, bank transfers or remittances to policyholders or named beneficiaries, but not to third parties. The proportion of lapse/surrender benefits paid within 25 months after policy issuance has not been significant. The proportion of incoming and outgoing international remittances has also remained low.

5.5.10 The proportion of premiums paid by policyholders who are PEPs or from high-risk jurisdictions has been low. These policyholders are subject to EDD requirements stipulated in the Guideline and the IIs' internal policies.

Universal life insurance products and Investment-linked assurance scheme ("ILAS") products

5.5.11 Universal life insurance products are a type of life insurance with a savings element that provides cash value buildup. The relatively high premium payments for universal life insurance products, coupled with product features that include flexibility for premium payment (allowing further "dump-in" of extra premiums subject to a cap) and withdrawal, make these products more vulnerable to ML risk (as identified in the last risk assessment exercise). While banks (as licensed insurance agencies) and licensed insurance broker companies remain the major distribution channels for universal life products targeting mainly high net-worth private-banking clients, an increasing number of insurers have started to offer these products via internet platforms to the retail market. Despite this nascent trend, however, the percentage of universal life business distributed through non-face-to-face channels remains negligible compared with the more traditional banking and broker channels.

5.5.12 Indemnity commission, or any form of excessive upfront commission, coupled with a short clawback period, may create a misaligned incentive for insurance intermediaries not only to mis-sell policies, but also to engage in ML or fraudulent acts. Such risks have been addressed through a ban on indemnity commission and requirements for authorised insurers to have in place appropriate remuneration structures for insurance intermediaries and suitable clawback mechanisms, imposed by the IA's Guideline on Underwriting Long Term Insurance Business (Other than Class C Business) which was issued in April 2016. Meanwhile, the AML/CFT controls on universal life business distributed through non-face-to-face channels will continue to be monitored through onsite inspections and reviews of Insurtech Sandbox applications submission (see para. 5.5.18 below).

5.5.13 Linked long term business, more commonly known as ILAS products, also entail increased inherent ML risk as identified in the last risk assessment exercise. ILAS policies are long term contracts of insurance that provide both life insurance protection and investment options, with the policy value determined by the performance of the underlying or reference funds. To address the risk of misaligned incentives for insurance intermediaries driving mis-selling or engagement in ML or fraudulent acts, indemnity commission on linked long term business has also been banned. There are requirements for insurers to have in place appropriate remuneration structures for insurance intermediaries and suitable clawback mechanisms pursuant to the IA's Guideline on Underwriting Class C Business which came into operation on 1 January 2015. From 2016 to 2021, new business premiums for ILAS products were a minor portion of total Individual Life and Annuity new business, making up less than 20% of this segment in 2021.

Mainland visitors

5.5.14 New individual long-term business premiums from the Mainland Chinese visitors ("MCVs") have gradually declined since the last risk assessment exercise, amounting to HK$43.4 billion in 2019, or 25.2% of total new individual long-term business premiums. From 2020 to 2021, there was a further sharp fall in new individual long-term business premiums from MCVs to HK$0.7 billion, which made up only 0.4% of total new individual long-term business premiums. This resulted from the imposition of cross-boundary passenger traffic restrictions to contain the COVID-19 pandemic.

5.5.15 Given that MCVs make up a large portion of all offshore policyholders, the drop in business from MCVs has also contributed to a significant decrease in new individual long-term business premiums for offshore business, which amounted to HK$62.2 billion in 2019, sharply reducing to HK$18.1 billion in 2020 and HK$ 9.4 billion in 2021, and only respectively accounting for 13.6% and 5.6% of total new individual long-term business premiums (onshore and offshore) in 2020 and 2021.

5.5.16 Additional controls relating to ML risk associated with long term insurance business products being sold to MCVs remain in place. These include the requirement for MCVs to sign the Important Facts Statement to acknowledge that insurers have the responsibility to ascertain the source of funds of applicants and the obligation to transfer relevant information to LEAs without the policy holder's prior consent in suspicious cases or upon requirement by LEAs in Hong Kong. These controls are in addition to the EDD and ongoing monitoring requirements, which are required for MCVs who are assessed as higher risk.

Virtual insurers and virtual on-boarding

5.5.17 To encourage and assist the insurance industry in embracing technology and attracting new digital insurers to Hong Kong, the IA launched its Insurtech Sandbox and its Fast Track for authorization in September 2017. The Fast Track provides a dedicated queue to expedite applications for new authorization submitted by new insurers using solely digital distribution channels. Before authorization is granted to a virtual insurer under the Fast Track, the applicant is required to furnish AML/CFT policies, procedures and controls for scrutiny by a specialized AML supervision team in the IA. The team will focus on the adequacy of the controls in place to mitigate, in particular, impersonation risks posed by non-face-to-face customers, which is an inherent part of a virtual insurer's distribution model.

5.5.18 Other than the emergence of virtual insurers, there has also been a surge in the adoption of virtual on-boarding processes by traditional insurers, as identified through applications made to the IA's Insurtech Sandbox. This trend has accelerated due to the disruption caused by the COVID-19 pandemic. These Sandbox applications usually involve approval for the distribution of long-term insurance policies via video conferencing. Insurers are required to submit details of the AML/CFT controls as part of the application, including ML/TF risk assessments and the corresponding additional measures relating to non-face-to-face customers, amongst other matters, for the IA's review.

5.5.19 To share best practices adopted by insurers in respect of AML/CFT controls for virtual customer onboarding (reviewed as part of the Sandbox applications received), the IA hosted an online sharing session for all long-term insurers in late 2020. Apart from

sharing best practices and suggested improvements as observed through various Sandbox applications reviewed, the IA also took the opportunity to promote the iAM Smart Pilot Sandbox Programme initiated by Cyberport in collaboration with the Government by highlighting its benefits in mitigating ML/TF risks posed by non-face-to-face customers.

AML/CFT Supervision of the Insurance Sector

Risk-based supervision

5.5.20 The commencement of the IA's functions coincided with the introduction of strengthened regulatory powers and the enhancement of corporate governance requirements for authorised insurers and licensed insurance intermediaries. In addition to certain controllers of authorised insurers having to obtain prior approval from the IA for their appointment, in July 2017, the appointment of key persons in control functions (such as compliance, risk, finance and internal audit) became subject to prior approval by the IA. In September 2019, the prior approval requirement was then extended to key persons in control function for intermediary management with strengthened corporate governance principles being promulgated for licensed insurance broker companies and licensed insurance agencies.

5.5.21 The AML/CFT Guideline issued by the IA for the insurance sector was amended in November 2018 to align its requirements with the latest international standards and better facilitate the implementation of the RBA by enhancing relevant guidance on risk assessments and the application of simplified and EDD.

5.5.22 As an integral part of the RBA, ML/TF risk profiling is conducted on all IIs. To further strengthen the IA's risk-based supervision on licensed insurance intermediaries, the risk-profiling model for insurance intermediaries was enhanced in 2020, with additional risk factors included to better reflect their risk exposure. The intensity and frequency of various on-site and off-site measures depend on the risk ratings that the IA assigns to IIs through its risk profiling exercise.

5.5.23 For deficiencies identified during on-site inspections and off-site reviews, the IA takes appropriate regulatory actions. In particular, the IA issues management letters requiring IIs to propose concrete remedial action plans with specific timelines for remediation being imposed. Remediation is then closely monitored until completion. In January 2022, the IA took its first AML disciplinary action against two authorised insurers for deficiencies in their AML/CFT controls and procedures which resulted in a public reprimand and fine of HK$7 million being imposed against them. The IA will continue to apply proportionate supervisory and enforcement measures to ensure IIs comply with the AMLO so as to prevent them from being used as a conduit for money laundering activities.

5.5.24 To ensure the IA's resources are adequate to carry out its requisite supervisory work, the AML supervision team has been progressively bolstered in terms of headcount and expertise. The team now includes staff with law enforcement background and financial crime compliance experience.

Capacity building and outreach

5.5.25 The IA has issued several circulars to inform the insurance industry on findings identified throughout its inspections and to promote understanding by IIs of the standards which the IA expects them to maintain. In April 2018, the IA issued a circular to all

authorised insurance brokers regarding its onsite inspection findings which included AML/CFT related matters. An additional circular summarizing key AML/CFT onsite observations was issued to all authorised long-term insurers in May 2018, after the IA had held a briefing session for around 100 compliance officers and ML reporting officers of insurers informing them of the findings.

5.5.26 The IA has also stepped up its outreach and capacity building work to promote awareness and understanding of ML/TF risks and AML/CFT obligations among small and medium-sized IIs. For example, the IA gave presentations to over 600 insurance practitioners in August 2018 and March 2019 in seminars organised by an industry body for its members on ML/TF threats and vulnerabilities associated with the insurance sector. This training covered, among other matters, the key risks identified in the last risk assessment report published by the Government in April 2018 and technical know-how in conducting a periodic assessment of ML/TF risks at an institutional level. The IA will continue these outreach activities and further expand the topics to cover other areas, including statutory obligations on TF and PF and suspicious transaction monitoring and reporting.

ML Risks

5.5.27 As indicated by the low amount of realisable assets for restraint and confiscation, which were in the form of insurance policies during the period 2016 to 2020, the risks associated with the insurance sector being used for ML are low when compared with other sectors. However, the ML threats brought about by the global nature of the insurance industry cannot be discounted, particularly in light of the size of the industry's offshore customer base (including MCVs). Whilst such risk is currently reduced due to the border controls imposed to combat the spread of COVID-19, the IA will remain vigilant in monitoring the trend and threats posed by non-resident policyholders in the post-pandemic period. ML/TF risks emerging from the growing use of virtual onboarding have been and will continue to be addressed through an early review of the proposals and risk assessments submitted by insurers through the IA's Insurtech Sandbox and the authorisation process for virtual insurers through the Fast Track.

5.5.28 Taking into account the ML threats and vulnerabilities above, the overall ML risk level of the insurance sector is assessed to remain at medium low.

Next Steps

5.5.29 To facilitate ongoing monitoring of the ML/TF trends and the effectiveness of risk mitigation measures, the IA has enhanced the granularity of the data it collects from the industry, which is collated and published as the long-term business statistics[157]. The IA will continue to consider, from time to time, appropriate refinements to the collection of such data, so it remains relevant and of practical use in the control and mitigation of ML and TF risks.

5.5.30 To continually enhance understanding of ML/TF risks and AML/CFT obligations across the insurance industry, the IA will continue its outreach and capacity-building

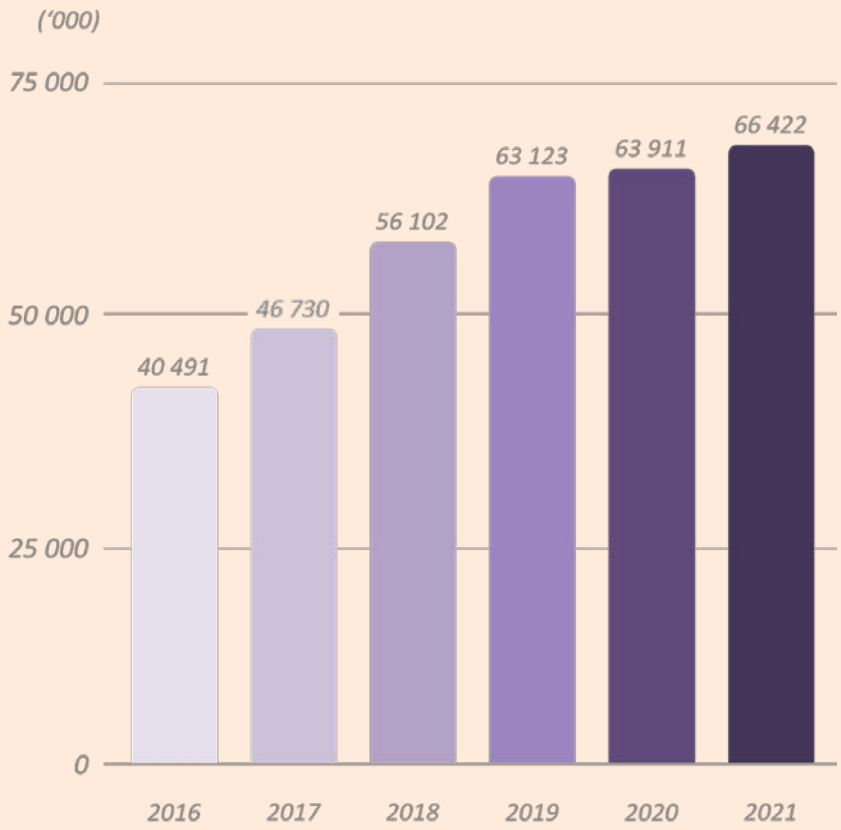
[157] The Form HKLQ6-1 of the Hong Kong Long Term Business Quarterly Returns was revised in 2017 with additional breakdown in product types for Class A business with a view to collecting more granular statistics on insurance policies issued to MCVs.

activities. The IA will also continue to monitor any emerging ML/TF risks, including those arising from the COVID-19 pandemic and will take a proactive approach to control and mitigate such risks in the post-pandemic period when an upswing in offshore business is expected.

5.6 STORED VALUE FACILITIES

5.6.1 SVFs are retail payment products whose target market is predominantly, though not exclusively, small-value payments or transfers. The sector has experienced notable growth, and increasing market penetration since the SVF regime under the PSSVFO was introduced in 2016. As at end 2021, 15 SVF licensees[158] were in operation, with approximately 66 million accounts (Figure 5.6), mainly focusing on the Hong Kong market. There were also notable increases in the total value of different types of SVF transactions (Figure 5.7), which reached HK$328 billion in 2021[159]. In particular, the total value of purchase of goods and services surged by 40% to HK$182 billion, mainly owing to the Government's Consumption Voucher Scheme. Typical products and services include stored value payment cards, e-wallets and internet payment services.

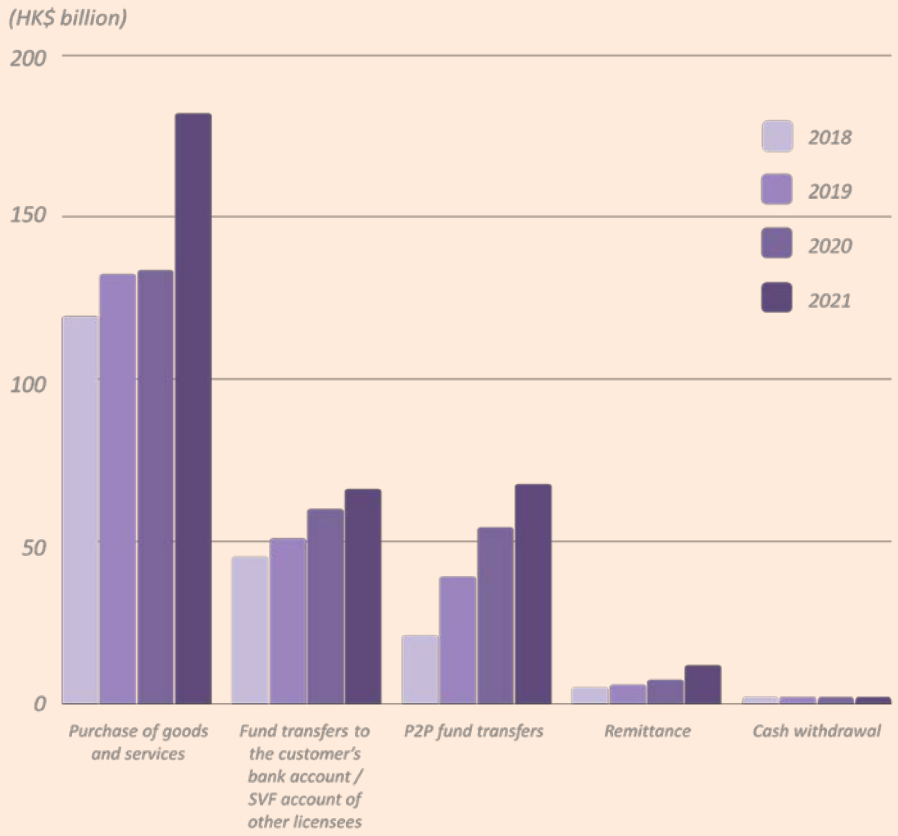
Figure 5.6: Total number of SVF accounts



[158] Twelve of these were granted licences under the PSSVFO and the remaining three are licensed banks.

[159] The total value of SVF transactions referred here include purchase of goods and services, P2P fund transfers, fund transfers to bank accounts, remittance and cash withdrawal, etc..

Figure 5.7: Total value of SVF transactions with breakdown by usage types



5.6.2 Given the rapid growth of the SVF sector, the preliminary ML/TF risk assessment included in the 1st HRA was updated in 2019[160]. The updated assessment broadly confirmed the findings of the 1st HRA that the majority of the SVF sector, featuring small stored values, limited functionality and predominant use for transport and low-value retail transactions domestically, is subject to lower ML/TF risks. Pockets of higher ML/TF risks exist in certain products particularly network-based SVFs such as e-wallets and prepaid cards, where risks continue to emerge in functions such as overseas cash withdrawal, cross-border remittance and P2P fund transfers, which introduce higher vulnerabilities for abuse. To address the emerging ML/TF risks identified as the sector develops and understanding of risks becomes more mature, the regulatory regime was enhanced in September 2020.

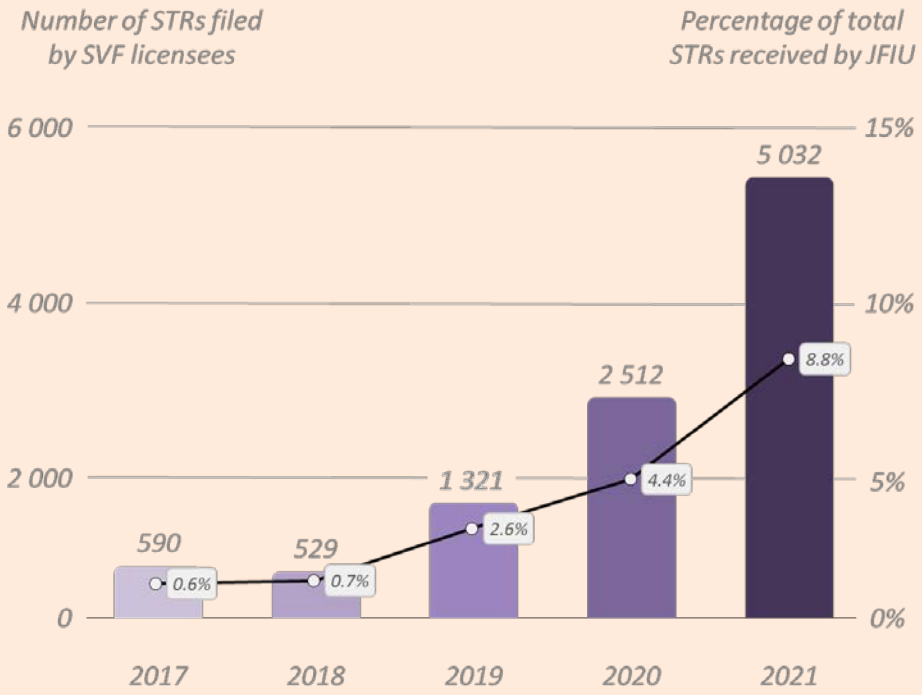
ML Threats in the SVF Sector

5.6.3 Consistent with business growth, there has been a corresponding increase in the number of STRs filed to the JFIU by SVF licensees, indicating increasing risk awareness of the sector. In 2021, SVF licensees filed around 5 000 STRs, representing 8.8% of total STRs received by the JFIU (Figure 5.8). Relevant typologies and alerts issued by the FMLIT and the JFIU have been shared with SVF licensees from time to time, enhancing

[160] Risk assessment of the SVF sector can be found in the "Stored Value Facility Sector: Money Laundering and Terrorist Financing Risk Assessment Report" published by the HKMA in July 2019. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190719e1.pdf

SVF licensees' awareness of the risk indicators and typologies of emerging ML threats and contributing to the increase of the number of STRs filed by SVF licensees over the past four years.

Figure 5.8: Total number of STRs filed by SVF licensees



5.6.4 JFIU analysis of observed criminal activities and STRs in the sector highlighted various key typologies, including network-based SVFs being exploited for fraud-related activities (e.g. e-shopping and social media deception), P2P fund transfer functionality being abused for illegal bookmaking and gambling activities, and use of SVFs to purchase illicit goods online.

Fraud

5.6.5 Fraud is by far the most prevalent predicate offence for ML in the SVF sector with SVF accounts being exploited as conduits to receive online fraud-related funds siphoned from victims' bank accounts and credit cards.

5.6.6 The global trend of criminals taking advantage of COVID-19 to perpetrate fraud and exploitation scams has also impacted Hong Kong and the SVF sector (case study on "personal protective equipment fraud using bank account" in Box 5.1 refers). Case-based intelligence and an alert to all banks and SVF licensees on face mask scams, outlined in greater detail in section 5.2.6, were disseminated to raise industry awareness.

Illegal bookmaking

5.6.7 There has been an increase in STRs relating to online gambling and illegal bookmaking, reflecting a well-known typology by which illegal bookmaking syndicates used P2P fund transfers between e-wallets to collect bets.

Box 5.14 - Case Example - Illegal bookmaking

An SVF licensee detected a number of accounts with frequent incoming P2P fund transfers in relatively small amounts followed by subsequent transfers to other unrelated individuals or back to the originators. As the account activities were inconsistent with the customers' normal transaction profile, the SVF licensee looked into the originators' text messages and discovered terms associated with illegal online gambling services, subsequently making an STR. Subsequent law enforcement investigation confirmed that a syndicate used the accounts to collect and consolidate gambling bets and later transferred the funds to bank accounts held by the syndicate members or back to the originators, depending on the gambling outcomes.

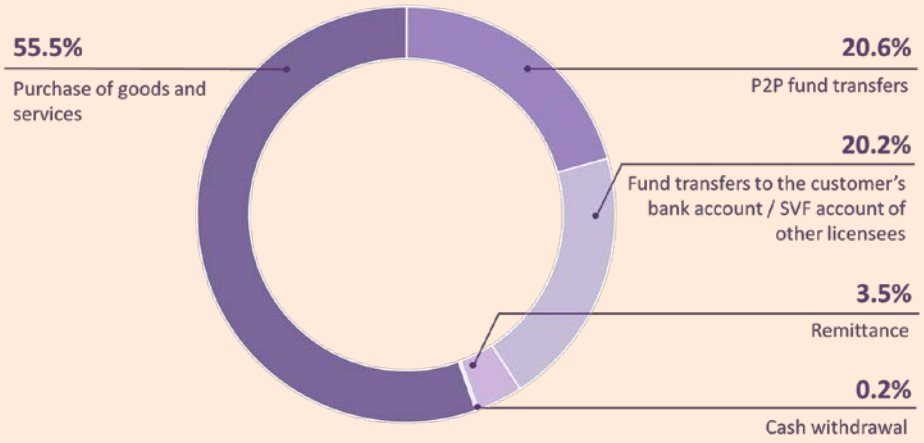
Other ML threats

5.6.8 As SVF products (e.g. prepaid cards) may facilitate online payments (e.g. to merchants under international card schemes such as Visa, MasterCard and UnionPay), typologies revealed that SVFs might have been abused to purchase illicit goods online. In view of the rapid development and innovation of the SVF sector, as well as its potential involvement and collaboration with NPMs[161], emerging ML risks continue to be closely monitored.

ML Vulnerabilities of the SVF Sector

5.6.9 The SVF market is generally characterised by lower-risk transactions, with purchases of goods and services accounting for about 55% of the total value of transactions in 2021 (see Figure 5.9). The great majority (about 96% by volume) of these were transactions of less than HK$100, with an average amount of HK$30. Such low-value retail transactions generally present low ML risks. Around a further 20% of the total value of transactions were fund transfers to customers' accounts with banks or other SVF licensees, which generally carry lower ML risks.

Figure 5.9: Total value of transactions by customer activities (2021)



[161] See paragraphs 5.2.22 and 5.2.23 on ML risks posed by NPMs and the measures taken by the HKMA.

P2P fund transfer

5.6.10 P2P fund transfer is a function provided by most e-wallets, and both the number and value of transactions have multiplied in the last few years. P2P fund transfer services were initially limited to transfers within the same SVF licensee. With the launch of the FPS[162] in September 2018, the function was extended to transfers between customers of different banks and SVF licensees. Hong Kong residents commonly use this function for conducting small-value fund transfers among peers, such as splitting the bill for meals. While the total value of P2P fund transfers (21% of the total value of all transactions in 2021) increased by 24% from 2020 to 2021, about 92% of these transactions by volume were below HK$1,000 with an average transaction value of HK$361. Though much of this volume represents lower-risk transactions, there are risks, particularly those arising from illegal gambling (see Box 5.14). To help mitigate these risks, SVF licensees are required to comply with relevant requirements for wire transfers in relation to cross-institutional fund transfers, while the customers are also subject to appropriate CDD measures.

Cross-border remittance

5.6.11 There is strong demand for remittance services provided by SVF licensees, particularly from FDHs. Currently, three SVF licensees offer remittance services in Hong Kong and processed remittance transactions of about HK$11.6 billion (3.5% of the total value of SVF transactions) in 2021, an increase of 59% from 2020. While remittance generally carries higher risks, most of the remittances processed by SVF licensees were initiated by FDHs and sent to their country of origin, generally the Philippines and Indonesia. Mainland China is also one of the most common destinations of remittance by virtue of close social and economic ties with Hong Kong. In 2021, around 89% of the transaction volume comprised transfers of less than HK$3,000 and the average amount per transaction was low at HK$1,196. Nevertheless, to mitigate the higher risks arising from this type of business, SVF licensees must conduct CDD on remittance customers and comply with relevant remittance requirements. In addition, SVF licensees have adopted appropriate transaction limits for remittance transfers.

Cash withdrawal

5.6.12 Customers, subject to relevant CDD measures, may withdraw cash from their e-wallets at SVF licensees' dedicated service points (e.g. convenience stores) or use prepaid cards via ATMs in Hong Kong and other jurisdictions. Although cash withdrawal only accounted for 0.2% of the total value of transactions in 2021, cash withdrawal through ATM networks presents higher ML risks as it allows funding in Hong Kong and withdrawal overseas, including in higher-risk jurisdictions. This risk is mitigated by measures including appropriate cash withdrawal limits and monitoring of customer transactions via management information system reports or automated systems.

Remote customer on-boarding

5.6.13 While SVF licensees adopt various business models with services offered through different channels, impersonation risk may be considered an area of vulnerability for remote customer onboarding if appropriate technology solutions were not adopted to

[162] The FPS, which is a system introduced by the HKMA in September 2018, operates round-the-clock and connects banks and SVF operators on the same platform. It enables the public to transfer funds across different banks or SVFs with funds available almost immediately. In addition to the Hong Kong Dollar, the FPS also supports RMB payments.

mitigate such risks. Factors that may aggravate the risks include the ability to make multiple fictitious account-opening applications and the possibility of identity fraud, which the SVF licensee may find more challenging to detect when onboarding is done, or service is offered remotely.

5.6.14 Given the expanding scope of SVF services and significant growth of the sector, the HKMA provided guidance to SVF licensees in September 2020 to facilitate the adoption of technology solutions for CDD in remote customer onboarding, which articulated the principles of identity authentication and identity matching. Many SVF licensees have recently introduced remote customer onboarding using appropriate technology to mitigate the risks, particularly impersonation risks when identifying and verifying the identity of their customers. The introduction of iAM Smart, which may be used to facilitate remote onboarding of customers, will further leverage on technology to strengthen CDD processes in remote onboarding.

New payment method

5.6.15 As discussed in 5.2.22, NPM provides convenience and efficiency to customers, especially for small and medium-sized enterprises, through the support of innovation and technology. Some SVF licensees, as for their peers in other jurisdictions, are increasingly having interface with NPM providers when facilitating their merchant customers' payment chains, and become more aware of the importance of understanding and managing the potential ML risks. Meanwhile, donation-based or crowdfunding platforms, often operating in conjunction with NPM providers, are another global development that may present risks, including for TF and other illegal activities. In this connection, the Government has conducted a preliminary study on legislation related to crowdfunding, and is planning to conduct a public consultation in 2022.

AML/CFT Supervision of SVF Sector

Legal and regulatory framework

5.6.16 A regulatory regime[163] for SVFs overseen by the HKMA was introduced in November 2015 under the PSSVFO. The implementation of the regime has been effective and smooth since its inception.

Risk-based supervision

5.6.17 Given market developments and the emerging ML/TF risks as identified, in September 2020, the HKMA enhanced its RBA to supervision and revised the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For SVF Licensees)[164], particularly about key areas including the introduction of a tiered CDD approach and provision of guidance to facilitate the adoption of technology solutions for remote customer on-boarding. The tiered CDD approach permits specific due diligence measures to be

[163] It is a licensing requirement for an SVF licensee to put in place adequate and appropriate AML/CFT systems and to comply with the provisions of the AMLO that are applicable to the SVF licensee; and the measures promulgated by the HKMA, whether in the form of rules, regulations, guidelines or otherwise, to prevent, combat or detect ML/TF.

[164] Details can be found in the HKMA circular "Amendments to Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Stored Value Facility Licensees)" dated 18 September 2020.https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2020/20200918e1.pdf

based on the assessed risk or not performed under specific low-risk scenarios. Consistent with the RBA, products with minimal functionality, such as exclusive use for domestic payments for goods or services, and subject to proportionate account limits to mitigate risk, may be provided to unverified customers (i.e. those for whom no CDD is required).

5.6.18 Similar to its supervision of banks, the HKMA continuously updates its understanding of the ML/TF risks of the SVF sector based on data collected on SVF licensees' operations and risk assessment and observations during the on-site visits. The HKMA now collects more frequent and up-to-date information in relation to customer portfolio, transactions and financial crime risks which are analysed and used for periodic risk profiling on all SVF licensees to determine supervisory measures, allowing the HKMA to focus its efforts on higher-risk areas. For example, as a follow-up to the ML/TF risk assessment of the SVF sector published in July 2019, the HKMA conducted thematic reviews[165] of SVF licensees' AML/CFT controls over prepaid card business, focusing on areas of higher ML/TF risk such as cash withdrawal activities and the effectiveness of AML/CFT systems in mitigating those risks. Where control deficiencies were identified, the SVF licensees concerned were required to undertake remedial actions to contain further impacts.

AML/CFT controls of SVF licensees

5.6.19 Based on the HKMA's supervisory engagement, SVF licensees have generally implemented AML/CFT systems to meet legal and regulatory requirements. The application of measures and controls is commensurate with the ML/TF risks of SVF products, with the effectiveness of implementation improving, despite variations being noted. For example, an increase in the number of STRs filed to the JFIU was observed (see Figure 5.8), which suggests an improving understanding of risk in the sector and AML/CFT systems to identify suspicious transactions arising from those risks. The HKMA also shares vital issues and good practices with the industry through ongoing supervisory communications including on-site examinations, visitations and thematic reviews and various forums to facilitate SVF licensees' understanding of risks and help strengthen their AML/CFT systems.

Supervisory and enforcement measures

5.6.20 The HKMA applies a range of supervisory and enforcement measures, progressive in severity, requiring SVF licensees to remedy control deficiencies and breaches of legal and regulatory requirements on AML/CFT. These include limiting or imposing conditions on businesses or activities, requiring commissioning of reports by external auditors on AML/CFT controls, remediation orders, pecuniary penalties and public reprimands under the PSSVFO. In determining which measures to impose, the HKMA will consider several factors, including the nature and seriousness of deficiencies, overall internal controls, the competence of the SVF licensee's senior management, etc.[166]. In

[165] Feedback from Thematic Review of Stored Value Facility Licensees' Application of AML/CFT Controls in Prepaid Card Business issued by the HKMA to SVF licensees on 24 September 2021. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210924e1.pdf

[166] Reference should be made to the relevant guidance issued by the HKMA, including:

- Policy and Supervisory Approach on Anti-Money Laundering and Counter-Financing of Terrorism/ https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2018/20181019e4.pdf;
- Guideline on Exercising Power to Impose Pecuniary Penalty. https://www.hkma.gov.hk/media/eng/doc/key-functions/Guideline_on_Exercising_Power_to_Order_a_Pecuniary_Penalty_PSSVFO_ENG.pdf; and
- Guidance Note on Cooperation with the HKMA in Investigations and Enforcement Proceedings.

addition, the HKMA also took disciplinary actions in December 2021 and January 2022 under the PSSVFO, including pecuniary penalties totalled HK$1.875 million and reprimands against two SVF licensees which failed to implement adequate and appropriate AML/CFT control systems relating to transaction monitoring, name screening and EDD in high risk situations. The SVF licensees were required to engage external auditors to validate the completeness and effectiveness of the remedial measures and enhancement.

ML Risks

5.6.21 Based on analysis of the nature and extent of observed criminal activity, the criminal threat to the SVF sector is assessed to be medium and primarily concentrated in network-based SVFs, where exploitation for fraud and illegal bookmaking related activities has been observed. In view of the growth and development of the sector, an enhanced regulatory framework for SVFs has been introduced to manage the overall risks of the sector, particularly those associated with overseas cash withdrawal, cross-border remittance, P2P fund transfer and remote customer onboarding. Taking into account these developments, ML vulnerabilities of the SVF sector are assessed as medium. Overall, the analysis confirms that the SVF sector continues to have a medium level of ML risk, which is in line with the risks presented by SVF sector internationally.

Next Steps

5.6.22 Given the assessment of ML risks in the SVF sector, the HKMA will continue to work closely with SVF licensees and other competent authorities to mitigate the ML risks in the SVF sector and has identified a number of areas for action:

(a) **Understanding of risk**: Continuing to strengthen the understanding of ML/TF risks, including new and emerging risks to enable proactive responses;

(b) **Supervision**: Staying vigilant to changing threats and vulnerabilities faced in the age of digital innovation and making more efficient use of HKMA resources, with wider adoption of Suptech tools and a more data-driven approach, to enhance our ability to take supervisory actions quickly and effectively;

(c) **Innovation**: Continuing to support innovation and the use of Regtech by SVF licensees to deliver improved outcomes in AML/CFT work and further reduce regulatory compliance burden;

(d) **Collaboration**: Scaling-up and enhancing public-private information sharing through the FMLIT and other initiatives, particularly for mitigating threats such as fraud and mule account networks; and

(e) **Sustainability**: Building sector-wide resilience through more timely and responsive education, outreach and awareness programmes that support a more holistic and sustainable response to ML/TF and other financial crime.

https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/g17_3.pdf

5.7 VIRTUAL ASSETS

5.7.1 In recent years, trading in cryptocurrencies and other asset classes in the virtual world has significantly blossomed, and it is widely recognised that these VAs, for all their potentials, pose significant ML/TF risks to the international financial system. VAs are vulnerable to ML/TF risks because they allow greater anonymity and decentralisation than traditional transfer, safekeeping, or custodian means, and such features can be easily abused to facilitate layering or conversion of crime proceeds into fiat money interfaces with the financial system. VAs also pose considerable challenges for investor protection due to their highly speculative nature, their frequent association with fraud, security breaches, and market manipulation.

5.7.2 To address the ML/TF risks of VA activities, the FATF revised its Standards, under Recommendation 15, in February 2019 to require member jurisdictions to regulate VASPs for AML/CFT purposes and supervise their compliance. In essence, the FATF requires member jurisdictions to impose on VASPs the full range of AML/CFT obligations that are currently applicable to FIs and DNFBPs. Prohibition is a permissible option, or VASPs can be licensed or registered and subject to the same AML/CFT requirements as FIs and DNFBPs.

5.7.3 Although VAs are not legal tender and not generally accepted as a means of payment in Hong Kong, we have noticed some VA trading activities operating locally. While there are no universally accepted rankings for VA activities, Hong Kong has been described as a place with significant VA activities[167]. There are different channels to conduct VA transactions in Hong Kong. In addition to online VA exchanges which provide transaction services of VA/VA-related products, it is also observed that there is an increasing number of physical VA exchange outlets providing direct VA exchange services (i.e. buy or sell VA with fiat currency). Besides, there are around 120 crypto-ATMs of limited scale in the territory. OTC trade exists but it is difficult to pinpoint the volume given the ambiguity in the transaction location that is often the case for VA trading activities. VA payment systems or VA custodian services operating as a stand-alone business in Hong Kong are still limited. Initial coin offering ("ICO") activities have reduced following repeated warnings by the SFC in the past few years.

ML Threats in the VA Sector

5.7.4 Echoing the increasing scale and popularity of VA activities in Hong Kong, VA-related crime has also been on an upward trend these days, though a notable proportion of cases were related to VA, only in name and may not have involved actual VA activities as can be seen in the paragraphs below. The number of VA-related crimes has increased from 324 in 2018 to 494 in 2020, so did the scale of losses. In the first eight months of 2021, around 739 VA-related cases have been registered (representing 155% increase compared

[167] In a 2021 ranking of VA exchanges, Hong Kong was listed as the fifth-largest with 34 exchanges, after the United Kingdom (with 70 exchanges), Singapore (with 47 exchanges), the United States (with 40 exchanges) and Seychelles (with 35 exchanges) [refers to Geography of Bitcoin Transaction Dynamics, 2014-H12021, Crystal Blockchain Analytics]. Hong Kong also ranked second globally for monthly VA trading by volume with US$32.5 billion worth of VA traded in December 2019 [refers to Crypto trading by location, CRYPTOCOMPARE].
https://www.marketwatch.com/story/this-country-leads-the-world-in-crypto-trading-and-it-isnt-the-one-you-think-2019-01-17

to the same period last year), while the losses amounted to HK$324 million – almost fifth-fold of the total (472%) compared to the same period last year. Fraud and theft constitute the major ML threats in the VA sector so far.

Fraud

5.7.5 Majority of deception and investment fraud cases involving VA involve victims who met fraudsters via different social media platforms, and were lured to invest into non-existing lucrative crypto investment plan. Victims were asked to open accounts in genuine VA exchange platforms and transfer the VA purchased to wallets provided by the fraudsters, usually through OTC or direct P2P methods. Very often, bogus websites or applications were set up for victims to create accounts in an effort to strengthen the "genuineness" of the scam. After the VA was transferred to the fraudsters, the fraudsters would alter the value of the victims' "investment portfolio" as shown on the dummy applications/websites controlled by them. Alternatively, victims were simply asked to transfer money to stooge bank accounts controlled by the fraudsters, and no VA transaction would take place at all.

Theft

5.7.6 Given the anonymity-enhanced nature of VAs and the lack of secure trading platforms, some VA owners tend to buy or sell VA in person to ensure that the VA transaction can be completed. However, there are reported cases in which people were robbed or conned out of millions of Hong Kong dollars in face-to-face VA transactions.

ML Vulnerabilities of the VA Sector

5.7.7 For this assessment, we have assessed the vulnerabilities of the VA products. VA trading platform is assessed 'Medium' vulnerability whereas other five products, including Crypto-ATM, OTC, P2P trading platforms, ICO and VA custodian wallets are assessed as 'Medium-Low' to 'Low'. Major risk components include its relatively large volume in the VA trading platform sector, resulting in a higher inherent vulnerability.

VA trading platform

5.7.8 VA exchanges, usually operate through web-based platform and mobile applications, are attractive to local and overseas money launderers, owing to their ease of accessibility, anonymity-enhanced feature and global reach without audit trail as a gateway to converting or layering crime proceeds into VAs or vice versa. Money launderers can also make use of third parties as a mule investor to conduct VA transaction. Owing to the anonymous nature of VAs, it is also easy for criminals to obfuscate the source of funds by utilising different wallets to transact on VA trading platform. This conceals their origin and ownership, further complicating the trail for law enforcement to detect and mitigate illicit activity.

5.7.9 As revealed by a major operation[168] carried out by the C&ED in July 2021, criminals attempted to open local bank accounts with shell companies and make transactions through a virtual currency exchange trading platform to turn laundered VAs into cash.

5.7.10 An online exchange where cash may be transferred to the exchange through a

[168] Involving a suspected ML syndicate involving $1.2 billion.

bank or other payment system, the relevant ML/TF risks are mitigated through its interface with local FIs who are subject to AML/CFT obligations under the AMLO.

Crypto-ATM

5.7.11 Cypto-ATMs are potentially vulnerable to abuse as they offer criminals the ability to convert the physical cash proceeds of crime directly. However, there is limited existence of Cypto-ATMs in Hong Kong. The physical cash capacity limits of Cypto-ATMs also limit the scale of funds laundered, thereby lowering the risk of abuse.

OTC

5.7.12 Given the potential challenges lie in crypto OTC activities (such as fraud, settlement risks), it is observed that the crypto OTC activities are not significant in Hong Kong, be it OTC dealers, brokers or exchange OTC desks.

5.7.13 Under the VA Trading platforms regulatory framework (see paragraph 5.3.20), the SFC regulates off-platform trading activities (i.e. OTC trading activities) which are carried out by a licensed VA trading platform. Upon commencement of the statutory licensing regime for VASPs under the AMLO (see paragraph 5.7.22), the SFC's regulatory remit will be extended to all VA trading platforms, which include their OTC trading activities, in Hong Kong. Besides, the SFC and the HKMA also published a joint circular on the guidelines for intermediaries to provide VA dealing services to clients (see paragraph 5.3.20). The SFC's regulation on crypto OTC activities conducted by licensed VA trading platforms and VA dealing services conducted by intermediaries should therefore have covered a substantial part of the VA universe that poses the highest risks to ML/TF and investor protection.

VA custodian wallets

5.7.14 Although custodian wallet providers are vulnerable to ML/TF abuse because criminals may use them to store and transfer illicit VAs, wider adoption for ML/TF abuse is limited by their relative lack of security and reliability, which stems from the fact that their operators can freeze accounts and impose censorship on their users' transactions. For dedicated custodians who offer their services to institutional investors, they tend to have higher financial barriers to entry, thus potentially decreasing their ML/TF vulnerability.

P2P trading platforms

5.7.15 P2P trading platforms only provide a forum where buyers and sellers of VAs can post their bids and offers, with or without automatic matching mechanisms, for the parties themselves to trade at an outside venue. In other words, P2P trading platforms can put users in direct contact over the internet or physical contact with one another, providing the opportunity to transfer ownership of VAs. P2P trading platforms can be abused by criminals to launder illicit proceeds directly by trading VAs for money without disclosing the source of fund or beneficial ownership.

5.7.16 According to a further analysis of VA-related reported cases, it is worthwhile to note that a substantial percentage (about 37%) of the cases did not involve actual transactions of VA (or the existence of VA transactions could not be confirmed). In more than half of the cases with actual VA transactions, criminals utilitised direct P2P transaction either as a means of receiving VA from victims or in subsequent layering processes.

5.7.17 While the FATF Guidance Note on VA and VASPs states that peer-to-peer trading platforms may not constitute a VASP as defined under the FATF Standards, we will remain vigilant given that the ML risk involved in P2P trading platforms could be on the rise.

ICOs

5.7.18 ICOs typically involve the issuance of digital tokens, created and disseminated using distributed ledger or blockchain technology. ICO scheme operators may promise buyers of digital tokens that the proceeds of an ICO will be used to fund development of a digital platform or related software which the token holders can subsequently access. Some token holders expect to make a return on their investment by reselling on the cryptocurrency exchanges. Investigations into ICOs predominantly revolve around fraud.

5.7.19 In September 2017, the SFC issued its first statement clarifying that depending on the facts and circumstances of an ICO, digital tokens that are offered or sold may be "securities" as defined in the SFO. In such cases, activities related to those tokens may constitute a regulated activity and may require a licence from the SFC. In particular, where the offer of a VA involves an offer to the HKSAR public to acquire securities or participate in a collective investment scheme ("CIS"), registration or authorization requirements under the law are applicable unless an exemption applies (e.g. offer to professional investors only). The SFC, further to its initial statement, reached out to a number of ICO issuers, warning them about the need to comply with the SFC's regulatory regime should they offer VAs that qualify as securities. Most of them confirmed compliance with the SFC's regime or ceased to offer tokens to Hong Kong investors. In March 2018, it also halted one ICO to the Hong Kong public, having considered the digital tokens might constitute a CIS under the SFO. ICO activity has significantly reduced since its peak in 2018 and while the SFC continues to monitor potential offers of VAs, it currently does not consider it a significant source of risk to investors.

AML/CFT Supervision of the VA Sector

Regulatory framework

5.7.20 Regulators including the SFC and the HKMA have been making full use of the existing regulatory tools to tackle risks associated with VAs. Under the prevailing regulatory framework, if the structure, facts and circumstances of individual VAs fall under the definition of "securities" or "futures contracts" in the SFO, they are already subject to the regulation of Hong Kong securities law and will fall under the legal remit of the SFC. To address the specific risks posed by VAs, the SFC has, since 2017, published multiple statements and circulars to clarify how the existing legal framework applies to different kinds of VA activities, ranging from warnings to investors on ICOs to regulatory initiatives on the relevant aspects of VA activities that relate to securities and futures markets.

5.7.21 In view of the development of VA, the SFC introduced a regime under the ambit of the SFO in November 2019 for the licensing of VA trading platforms. Under the regime, licensed VA trading platforms will be subject to regulatory standards comparable to those applicable to licensed securities brokers and automated trading venues, including requirements on safe custody of assets, know-your-client, AML/CFT, prevention of market manipulative and abusive activities, cybersecurity and risk management.

5.7.22 To strengthen the regulatory framework of VASPs, the Government has proposed to amend the AMLO to introduce a licensing regime for VASPs and subject them to a fit-and-proper test similar to that of other financial sectors. Licensed VASPs will be required to observe the AML/CFT requirements under Schedule 2 to the AMLO, as well as other regulatory requirements designed to ensure the protection of market integrity and investor interest. An applicant has to satisfy a fit-and-proper test, similar to other FIs regulated under the AMLO as set out in specific legislation of their sectors, to be considered for the granting of a VASP licence. The fit-and-proper test will cover all responsible officers and ultimate owners of the applicant, and any change in this regard would require prior approval by the SFC. To ensure the proper management of a licensed VASP, for accountability consideration an applicant will have to appoint at least two responsible officers to assume the general responsibility of ensuring compliance with AML/CFT requirements and other regulatory requirements, and be held personally accountable in case of contravention or non-compliance of the requirements. Similar to the requirement under the SFO for LCs, all executive directors of a licensed VASP must be made responsible officers upon approval by the SFC.

5.7.23 The HKMA has issued a number of circulars since 2014 on how banks should manage the ML/TF risks associated with VAs and VASPs, for example when providing banking services to VASPs (see paragraph 5.2.22). Given the HKMA's role in maintaining monetary and financial stability, and with a view to aligning with international standards and ensuring proper user protection, it is considering regulating different kinds of activities relating to payment-related stablecoins which are, or have the potential for becoming, a widely accepted means of payments. In January 2022, the HKMA issued a discussion paper on crypto-assets and stablecoins to set out the thinking on the regulatory approach for crypto-assets, particularly payment-related stablecoins, and invite views from the industry and public. The HKMA is now considering the feedback received.

Supervision

5.7.24 Under the SFC's voluntary regime for VA trading platforms introduced in November 2019, the applicant will go through an intensive licensing process. In the assessment process, the SFC places emphasis on whether the applicant is able to comply with its expected standards on key risk areas such as custody of client assets, know-your-client, AML/CFT, market surveillance, cybersecurity and risk management.

5.7.25 Upon becoming licensed, the VA trading platform operator will be placed in the SFC Regulatory Sandbox and be subject to frequent reporting, monitoring and reviews.

5.7.26 A licensed VA trading platform operator is subject to licensing conditions imposed by the SFC, which set out the regulatory standards that apply to all VA trading activities and any activities incidental to the provision of these trading services, irrespective of whether the VAs involved amount to "securities" or "futures contracts" as defined under the SFO. Under the licensing conditions, the licensed VA trading platform operator is required to comply with the AML/CFT requirements as well as other regulatory requirements that are comparable to those which apply to licensed securities brokers and automated trading systems, but also incorporate additional requirements to address specific risks associated with VAs.

5.7.27 A licensed VA trading platform operator is also required under the licensing conditions to engage an independent professional firm acceptable to the SFC to conduct an annual review of its activities and operations and prepare a report confirming that it has complied with the licensing conditions and all relevant legal and regulatory requirements. Such independent review is expected to cover the licensed firm's compliance with AML/CFT requirements in the licensing conditions and in the SFC's AML/CFT Guideline.

5.7.28 Currently there is one VA trading platform licensed, and the licence was granted by the SFC in December 2020.

5.7.29 The SFC has been keeping a close watch on the latest development of VA activities in Hong Kong. It will continue to monitor the VA sector through various channels including engagement with industry, public information, complaints received and desktop monitoring, and maintain ongoing dialogues with international bodies to ensure the SFC stays abreast of the latest market developments and evolving risks and opportunities of VAs. Where appropriate, the SFC may consider issuing further guidance.

Investigation and enforcement

5.7.30 The HKPF is committed to combating the uprising VA-related crime. A taskforce has been formed up to study and monitor the latest industry development and crime trend. Local and overseas training are provided to officers to enhance their professional investigation capabilities. Proactive engagement is also carried out with stakeholders including but not limited to policy bureaux, regulatory authorities, LEAs and business entities to continually enhance intelligence and experience sharing. Promotion and public education has also been provided though channels such as the ADCC to strengthen public awareness of the latest VA-related crime.

ML Risks

5.7.31 In light of the heightened ML threat and vulnerabilities of the sector, the ML risk of the VASP sector is re-assessed to medium compared to medium-low in the 1st HRA.

Next Steps

5.7.32 Looking ahead, the Government has introduced an amendment bill into the LegCo in July 2022 with a view to introducing a statutory licensing regime for VASPs through amendments to the AMLO.

5.7.33 As the VA market and regulatory landscape is evolving, the Government also sees a need of stepping up coordination and strengthening communication among our financial regulators on various technical and implementation matters. A formal regulatory dialogue among the three financial regulators, with the FSTB as necessary, will be established to develop forward-looking and consistent responses on VA-related regulatory issues (including issues on prudential supervision, AML/CFT supervision and investor/customer protection).

5.7.34 In light of the increasing trend of VA-related crime, our LEAs have stepped up efforts in combating fraud and ML cases involving the use of VAs. The LEAs will keep in view the trend of VA-related crime and the FSTB will review the need of extending the

regulatory regime to other VA activities e.g. VA exchange outlets, crypto ATM, etc. to mitigate their risk of criminal exploitation. The HKPF has also closely cooperated with the SFC in organising promotional campaigns to alert the public about possible fake websites/applications purported to be providing VA investment services as well as possible VA investment scams.

5.8 MONEY LENDERS

5.8.1 Money lenders in Hong Kong are regulated by the MLO[169]. The MLO stipulates that any person carrying on business as a money lender must obtain a money lenders licence. A person who carries on business as a money lender without a licence commits an offence and is liable on conviction to a fine of HK$100,000 and imprisonment for two years. As at 31 December 2021, there were 2 490 licensed money lenders. The business of the money lender sector occupies a very small share in the financing service market and the role of the sector in the financial market is very small. As at end-2021, total customer loan size of money lenders amounted to $218.3 billion, while those comparable loans made by the banking sector was $7 235.7 billion. The total customer loan size of money lenders is only 3% of that of the banking sector.

ML Threats in the Money Lender Sector

5.8.2 Since the 1st HRA, loan sharking and fraud with the use of false documents to prove regular salary income for applying loans and settling the loans in a short period of time remain as the major ML threats in the money lender sector. As shown in the convicted cases, illegal money lending businesses (loansharks) acquired control of the bank accounts of the borrowers who could not repay their debt for collecting payments from loansharking activities or other organised crimes.

5.8.3 Between 2016 and 2020, the number of STRs filed by the sector ranged from 0.03% to 0.07% of the total annual STRs filed. Out of the 9 197 reported ML investigation cases, only 19 cases involved money lenders. Besides, out of the 323 convicted ML cases, only eight cases involved money lenders. Among the total crime proceeds involved in all the convicted ML cases, only 1.49% were laundered via money lenders. The persistently small proportion of STRs filed by the sector to some extent reflects the relatively less active ML activities in the sector. The ML threat level of the money lender sector is considered medium-low.

ML Vulnerabilities of the Money Lender Sector

5.8.4 Unlike banks, money lenders do not take deposits from customers. They have very limited exposure to non-resident customers as most of their loans are made to the local population. While the sector is required to keep identity and transaction (loan payment and repayment) records, which is subject to regulation of the MLO, there is also the genuine need in the sector to conduct thorough identification checks on prospective borrowers and keep relevant identification and transaction records as this practice helps secure recovery of loans and interests. It is a usual practice for the sector to release loans and receive loan repayment through the borrowers' bank accounts, which, if suspected to be related to ML/TF activities, will provide an audit trail of the transactions. Although online or telephone applications have become increasingly popular, it is a usual practice for money lenders to conduct face-to-face interviews with their prospective clients before release of loans to ensure that information provided is in order.

[169] Chapter 163 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap163

AML/CFT Supervision of the Money Lender Sector

Supervision and enforcement

5.8.5 Under the MLO, an applicant for the grant or renewal of a money lenders licence[170] is required to submit an application to the Registrar of Money Lenders ("RML") and a copy of the application to the HKPF. Subject to any objection that may be raised by the RML or the HKPF, the Licensing Court, presided over by a magistrate, shall hear and determine the application. A licence shall be subject to such conditions as the Licensing Court may impose. The Licensing Court shall not grant a licence unless it is satisfied, among other things, that the applicant is fit and proper to carry on business as a money lender. Besides, any non-compliance with the Guideline on Compliance of Anti-Money Laundering and Counter-Terrorist Financing Requirements for Licensed Money Lenders ("the AML/CFT Guideline")[171] may cast doubt on whether the money lender and its related persons are fit and proper persons to carry on or be associated with the money lending business. The RML may base on this ground raise objection to the grant or renewal of the licence by the Licensing Court. In addition, on the application of the RML or the HKPF, the Licensing Court may revoke or suspend the licence if it is of the opinion that the money lender has ceased to be fit and proper to carry on business as a money lender or has been in serious breach of any licensing conditions.

5.8.6 Between 2016 and 2020, the HKPF objected to 47 applications, two of which were reaffirmed by the Licensing Court. Over the same period, the HKPF issued 22 warning letters to money lenders for breach of licensing conditions[172]. The Licensing Court suspended one money lender licence on the application of the HKPF. In the same period (2016 to 2020), the RML objected to 15 applications. Following the objection by the RML, four applicants withdrew their applications and ten applicants rectified the relevant non-compliance upon which the RML withdrew the objections. The RML issued a total of 238 rectification orders and three warning letters to the money lenders in relation to non-compliance with the licensing condition which require the money lenders to comply with the AML/CFT Guideline and 652 rectification orders and 56 warning letters to the money lenders for non-compliance with other licensing conditions.

Risk-based supervision

5.8.7 The RML adopts a risk-based supervision for money lenders. Supervisory attention and resources of the RML are focused on money lenders that are subject to higher ML/TF risks, while maintaining adequate and appropriate levels of engagement with money lenders that present lower ML/TF risks. All money lenders are subject to onsite inspections by the RML where AML/ CFT compliance and practices is a review area of every routine inspection. Money lenders are also subject to offsite monitoring. They are required to complete Supplementary Information Sheets to provide the relevant information to the RML for monitoring their compliance with the AML/ CFT requirements and to assess the ML/TF risks presented by the sector and by the individual money lenders. The RML will issue rectification order to the money lenders who are in breach of the AML/ CFT requirements as found during onsite inspection or offsite monitoring. The RML would conduct follow-up

[170] Licences are subject to renewal every 12 months.

[171] The AML/CFT Guideline is available at the website of the CR. https://www.cr.gov.hk/en/ publications/docs/AntiMoneyGuide_e.pdf

[172] The conditions are related to collection of debt, protection of personal data, handling of complaints in respect of loan activities and record-keeping.

inspections to ensure the irregularities are rectified, and issue warning letters to money lenders who remain non-compliant. Further inspections would be conducted on such cases, and depending on severity of the non-compliance, the RML would consider raising objection to the Licensing Court in respect of the application for licence renewal made by the money lender concerned.

5.8.8 With effect from October 2018, an additional licensing condition has been imposed on money lenders licences which require money lenders to comply with the AML/CFT Guideline as and when the licences are granted or renewed. In addition, with effect from March 2021, a new licensing condition has been imposed that licensed money lenders shall conduct assessment on the repayment ability of the borrower before entering into a loan agreement for an unsecured personal loan, and keep written or video or audio records showing such requirement has been complied with. It helps promote responsible lending by money lenders, making loan transactions even less possible for ML/TF purposes. Breach of a licensing condition is an offence under the MLO[173] and would render the money lender concerned and its officers liable to prosecution.

5.8.9 To strengthen the regulation of money lenders, the RML revised the AML/ CFT Guideline in October 2020 with an aim to addressing the deficiencies as identified by the FATF ME. Furthermore, the RML has published two sets of guidelines, namely, the Guideline on Fit and Proper Criteria for Licensing of Money Lenders and the Guideline on Submission of Business Plan by Applicant of a Money Lenders Licence. Both sets of guidelines took effect from 1 April 2021. The Fit and Proper Guideline outlines the criteria and matters that the RML will normally consider in determining the fitness and properness of applicants for money lenders licences, money lenders, and their related persons. These criteria include whether the money lender has established effective AML/ CFT system to ensure compliance with all applicable AML/ CFT requirements for money lenders.

5.8.10 With effect from 1 April 2021, applicants for a new money lenders licence are required to submit a business plan for their money lending business together with their application to show that they have a comprehensive understanding of the money lending business and are ready to carry on the business. The Business Plan Guideline sets out the key items of information that should be included in the business plan. The applicant is required to confirm in the business plan that the applicant is fully aware of and will comply with the provisions of the MLO, the licensing conditions and the AML/ CFT requirements for money lenders.

Education and outreach

5.8.11 To promote the awareness of money lenders on the AML/ CFT requirements, the RML issues circular through emails to remind money lenders of their obligations to comply with the statutory requirements on financial sanction, TF and PF. They are also informed of the publication of statement and relevant guidance issued by the FATF. The RML will also communicate with the associations of money lenders for dissemination of information to their members. Also, the RML conducts annual AML/CFT seminars for money lenders to promote the sector's understanding and identification of ML/TF risks, particularly in respect of TFS obligations and the reporting of suspicious transactions.

[173] Section 29(1)(c) of the Money Lenders Ordinance.

5.8.12 In view of the above, the ML vulnerability of the sector is assessed as medium-low.

ML Risks

5.8.13 Taking into account the threat and vulnerability assessments, the overall ML risk for the sector is considered to be medium-low.

Next Steps

5.8.14 With a view to adopting a more robust and comprehensive risk-based supervision of money lenders, the RML has been developing a supervisory plan which includes the risk profiling of individual money lenders based on a range of risk assessment criteria. The RML will work closely with the HKPF to keep abreast of AML/ CFT trends relating to the sector and review the supervisory plan from time to time as necessary. The RML will continue to conduct capacity building programmes for the sector to raise its awareness of ML/TF risks and AML/CFT obligations.

5.9 NON-BANK CREDIT CARD

5.9.1 There is only one non-bank credit card company operating in Hong Kong. It is also a regulated entity in its home jurisdiction and applies AML/CFT controls globally as part of the group requirements.

ML Threats and Vulnerabilities of the Non-bank Credit Card Sector

5.9.2 Before the invention of "Chip Card Security" (i.e. the tradition magnetic-stripe cards), criminals were able to produce bogus credit cards and to make various purchase and cash withdrawals. Chip card security is the latest standard in credit card security, which includes a small microchip in the credit card that protects buyers against fraudulent transactions. The security function of a chip card is designed to prevent fraudulent transactions that take place when someone physically swipes a counterfeit card at a payment terminal and they are very difficult to clone. There were cases in which criminals had uttered various forged supporting documents for credit card applications and passed the CDD test. However, these cases are very limited in Hong Kong.

5.9.3 Overall speaking, the sectoral ML risk remains at Low.

Next Steps

5.9.4 There will be continuous monitoring and review on the vulnerability of this sector to assess if any further actions such as additional mitigating measures or regulations will be needed.

5.10 FINANCIAL LEASING

5.10.1 In Hong Kong, the size of the financial leasing businesses is relatively small with limited scale of activities. Majority of the businesses engaged in the financial leasing are FIs and money lenders, which are already subject to AML/CFT obligations under the AMLO and the MLO. It is confirmed that there is no LC and authorised insurer engaging in financial leasing activities.

5.10.2 To understand the landscape of the sector and its awareness and implementation of relevant AML/CFT preventive measures, a survey was conducted on the financial leasing companies in Hong Kong in July 2021. From survey results, an example of principal business by non-FI/money lender financial leasing company (so called "standalone financial leasing company") include financial lease arrangement related to shipping.

ML Threats and Vulnerabilities of the Financial Leasing Sector

5.10.3 Financial leasing businesses pose a low ML threat as compared with other financial products and services, as the businesses are generally premised upon long-term relationships between the lessors and lessees, and financial leasing agreements do not result in the lessee receiving funds, but rather the usage of an asset, e.g. an aircraft or a ship in which the legal and beneficial title of the underlying asset remains with the leasing businesses. As revealed in the survey, the financial leasing business is not cash-intensive by nature and such lease arrangement is usually conducted through the banking system. Thus, financial leasing transactions are unlikely to be used for ML.

5.10.4 There is no case involved the use of financial leasing business in Hong Kong to commit ML and/or associated predicate offence. In terms of assets restrained/confiscated for ML and/or associated predicate offence(s), none of which involved financial leasing business in Hong Kong. Finally, there is no known financial intelligence or international request for assistance concerning misuse of financial leasing business in Hong Kong for ML purpose. These quantitative data suggest that financial leasing business is not a common conduit for ML in Hong Kong.

5.10.5 Amongst the APG Typologies Reports published between 2016 and 2020, none of the member jurisdictions have noted the use of financial leasing business for laundering of crime proceeds. The situation in Hong Kong, whereby financial leasing business is not a common tool used for ML purpose, is therefore consistent with the overall trend in the Asia –Pacific region.

5.10.6 Standalone financial leasing companies have also put in place scores of preventive measures, including conducting CDD; exercising ongoing monitoring; making suspicious transactions reports to the authorities; keeping records; organizing training for staff; conducting risk assessment systems prior to the launch or use of new products; carrying out independent review of internal AML/CFT systems, etc.

5.10.7 Considering the absence of quantitative or qualitative data indicating misuse of financial leasing business for ML in Hong Kong, the overall ML risk of the sector is considered to be low, based on the low level of ML threat and vulnerability of the financial

leasing sector.

Next Steps

5.10.8 Although the inherent nature of leasing arrangement poses strong obstacles for it to be abused for ML, the Government will continue to monitor and review the ML threat and vulnerability of the sector, to consider if additional mitigating measures will be needed.

CHAPTER 6

SECTORAL RISK ASSESSMENT – DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

6.1 OVERVIEW

6.1.1 This Chapter sets out the ML risk assessment of DNFBPs in Hong Kong, including legal professionals, accounting professionals, TCSPs, estate agents, and DPMS.

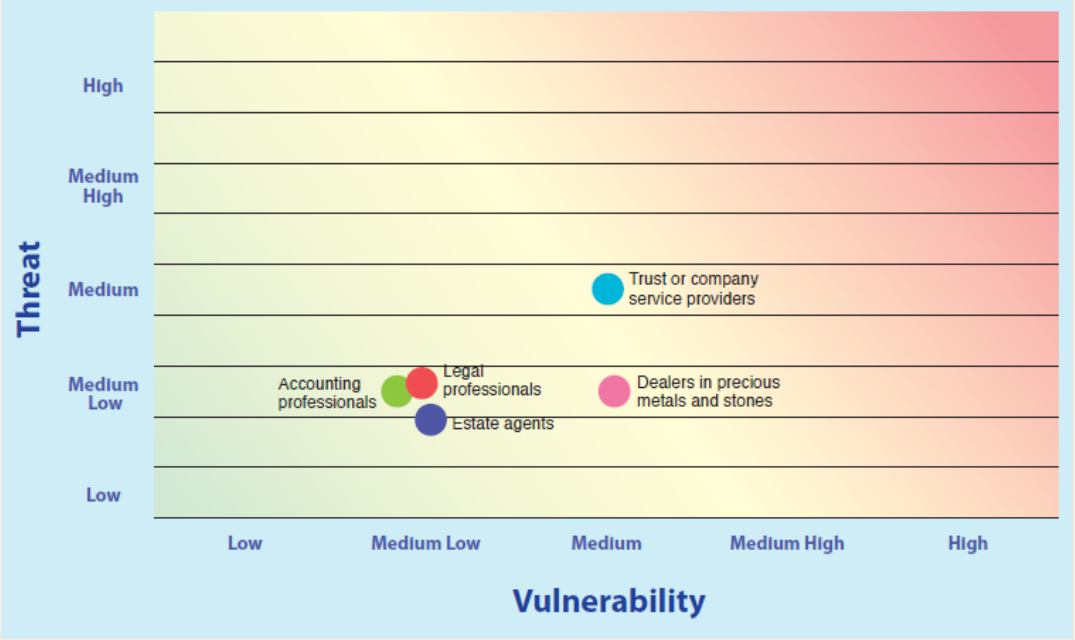
6.1.2 Since 1 March 2018, legal professionals, accounting professionals, TCSPs and estate agents are subject to the statutory AML/CFT obligations under the AMLO. The LSHK, the HKICPA, the CR and the EAA are the designated relevant authority or regulatory bodies in supervising the AML/CFT compliance of these sectors respectively.

6.1.3 To fulfil Hong Kong's international obligations under the FATF and to safeguard the integrity of our financial systems, the Government has proposed to cover the DPMS sector under the AML/CFT regulatory framework of the AMLO, with the relevant amendment bill being introduced into the LegCo in July 2022.

Table 6.1: Size – Designated non-financial business and professions

Legal professionals	Solicitors: 12 677 Registered foreign lawyers: 1 463 Hong Kong law firms: 941 Registered foreign law firms: 82
Accounting professionals	Certified public accountants (CPA) with practising certificates: 5 195 CPA firms: 1 268 Corporate practices: 668
Trust or company service providers	TCSP licensees: 6 711
Estate agents	Estate Agent's Licence (company): 3 938 Estate Agent's Licence (individual)/Salesperson's Licence: 42 062
Dealers in precious metals and stones	Retail (establishments): 1 960 Import (establishments)/Export (establishments): 1 010/2220 Manufacture (establishments)/Wholesale: 510/200

Figure 6.2: Overview of risk levels of designated non-financial business and professions



6.2 LEGAL PROFESSIONALS

6.2.1 Legal professionals in Hong Kong are broadly divided into solicitors and barristers. Of the two, legal services relating to activities identified by the FATF to be at risk for ML/TF are predominantly engaged by solicitors, for example conveyancing (real estate transactions), trustee services, services relating to the formation and administration of companies and entities, and the buying and selling of businesses. Practising barristers are prohibited under their Code of Conduct to accept any instructions to receive, disburse or otherwise handle clients' money, securities or other assets other than by receiving payment of their fees, and are hence not involved in activities covered by the FATF Recommendations.

6.2.2 The LSHK regulates Hong Kong law firms and foreign law firms registered with the LSHK. Solicitors and registered foreign lawyers are regulated under the Legal Practitioners Ordinance ("LPO") (Cap. 159)[174], under which the LSHK is the statutory regulatory body. A practicing solicitor must be a member of the LSHK and hold a practising certificate. The LSHK is empowered by LPO to investigate breaches of and take disciplinary action against professional misconduct. As at the end of 2021, the LSHK had 12 677 members, of which 10 965 held a current practising certificate, and 72% of members with a current practising certificate were in private practice. There were 941 Hong Kong law firms, of which 47% were sole proprietorships and 41% were firms with two to five partners, and the remaining were firms with more than five partners or were limited liability partnerships formed pursuant to the LPO. In addition, there were 1 463 registered foreign lawyers and 82 registered foreign law firms registered with LSHK.

ML Threats in Legal Professionals Sector

6.2.3 Solicitors often provide trust or company services and are thus subject to the threat associated with TCSPs (see section 6.4). They also play a key role in processing real estate transactions, including stakeholding of deposits and purchaser's monies for their clients. As crime proceeds may be converted into different types of assets, including real estates, presenting a potential threat that solicitors involved in real estate transactions might be wittingly or unwittingly involved in ML. However, only limited threat has actually been detected in respect of legal professionals involved in ML. From 2016 to 2020, only in two ML convicted cases were lawyers found to be unwittingly involved in real estate transactions, in which the properties were obtained fraudulently by the offenders.

6.2.4 The legal sector filed an average of around 710 STRs annually from 2016 to 2020. In 2020, the sector filed 807 STRs, of which 58 were classified as high risk by the JFIU. Nature of the high-risk STRs varied from case to case, with no particular trend observed. Meanwhile, a large proportion of STRs were found to be related to real estate transactions without any mortgage or financial assistance. The STRs involved natural persons or companies from different jurisdictions, reflecting that the legal sector in general has a diverse clientele and is subject to a cross-boundary ML threat.

6.2.5 Legal professionals are exposed to potential ML activities mainly through estate transactions and trust or company services, though the actual threat of using legal professionals as conduit for ML, particularly through witting involvement, detected is only

[174] Chapter 159 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap159

limited as revealed in the enforcement experience and statistics. The ML threat level of the sector is assessed to be medium-low.

ML Vulnerabilities in Legal Professionals Sector

Entry controls and integrity

6.2.6 Stringent and effective entry controls have been established by the LSHK pursuant to the LPO, which sets out the statutory requirements for the admission of solicitors practising in Hong Kong. Admission as a solicitor is subject to stringent examination, qualification and practice requirements. Legal professionals must also obtain a certificate from the LSHK and renew it annually to practise as a solicitor. The LSHK assesses the fitness and propriety of applicants, including through a declaration of conviction record by applicants. The DoJ conducts the fit-and-proper check, which covers the past conviction record of every applicant for admission as a legal professional.

6.2.7 The LSHK also closely monitors staff who are employed by solicitors' firms. Law firms are required to notify the LSHK of any new staff within 14 days and to report any association with other firms or use of service companies. Annual returns of staff and their salaries are also required to be filed to the LSHK. A list of employees who cannot be employed by law firms is published by the LSHK. To maintain the professional integrity of solicitors, law firms are prohibited from employing solicitors or foreign registered lawyers subject to disciplinary actions by the Solicitors Disciplinary Tribunal suspended from practice; declared bankrupt; or convicted of a criminal offence involving dishonesty without the LSHK's prior written consent.

6.2.8 Solicitors in Hong Kong are generally known to have strong ethics, integrity and a culture of compliance with professional rules and standards. Solicitors have to comply with the Hong Kong Solicitors' Guide to Professional Conduct stipulated by the LSHK, which sets out ethical standards and obligations that are higher than the requirements of the law in upholding their integrity and responsibilities.

Guidance and AML/CFT knowledge of professionals

6.2.9 Recognising the ML/TF risk in the sector, the LSHK introduced the Practice Direction P back in 2008 which makes application of essential AML/CFT preventive measures mandatory for all law firms and solicitors. The Practice Direction P provides a framework of AML/CFT compliance, including CDD, record-keeping, staff awareness and training measures, and further guidelines on how firms should apply a RBA, and recognition and reporting of suspicious transactions. With the commencement of the amended AMLO on 1 March 2018, the LSHK conveyed to legal professionals on the operation of the AMLO and statutory requirements as stipulated in its Practice Direction P.

6.2.10 The LSHK has also been working with the Government to raise the AML/CFT awareness of solicitors and enhance solicitors' understanding of their duties and responsibilities by conducting regular AML/CFT seminars From 2016 to 2021, about 3 500 members attended 13 AML/CFT seminars organised/co-organised by the LSHK with the Government.

6.2.11 Overall, solicitors in Hong Kong are generally well aware of the importance of AML/CFT and the CDD and record keeping requirements of the Practice Direction P. Law

firms in general have implemented programmes against ML, including internal policies and ongoing employee training programmes. The filing of STRs by solicitors has been the highest among DNFBPs, which reflects that the AML/CFT awareness of solicitors is high and an effective system in monitoring and reporting suspicious activity has been established.

Supervision

6.2.12 Currently, the LSHK acts upon information obtained in the course of carrying out their regulatory functions. It will also conduct investigation and inspection as appropriate.

Sanctions

6.2.13 The LSHK is empowered under LPO to investigate breaches of and take disciplinary action against professional misconduct. A breach of Practice Direction P including non-compliance with AMLO amounts to a breach of the code of conduct and this can result in disciplinary proceedings. A wide range of effective, proportionate and dissuasive administrative sanctions are applicable including warnings and, in more serious cases, disqualification as a solicitor. The LSHK can make referrals as appropriate to the Solicitors Disciplinary Tribunal which has the power to impose penalties. In 2020, Investigation Committees of the Standing Committee on Compliance considered 316 complaints, of which 0.88% related to property fraud. 16 visits to 13 law firms were conducted by the Investigation Counsel of the LSHK. A total of five cases were referred to the Tribunal Convenor, of which three were determined by the Solicitors Disciplinary Tribunal. One case resulted in disqualification as a solicitor, none of the cases related to ML or TF.

6.2.14 The AMLO provides a comprehensive statutory framework in requiring legal professionals to carry out AML/CFT preventive measures; there are also stringent and effective entry controls for the sector, rules governing accepting monies from clients and the sector members generally have high integrity and solid AML knowledge. The continuous enhancements of the LSHK supervisory role are being pursued to further reduce exposure of the legal profession to ML/TF. All in all, the ML vulnerability level of the legal professionals sector is assessed to be medium-low.

ML Risks

6.2.15 Taking into account the level of ML threat and ML vulnerability of the legal professionals sector discussed above, which are both assessed to be medium-low, the ML risk level for the sector is assessed to be medium-low.

6.3 ACCOUNTING PROFESSIONALS

6.3.1 Hong Kong has a well-developed accounting professionals sector. Accounting professionals, in addition to providing statutory auditing work, also render other services, including assurance, tax compliance and advisory, business advisory and consulting, corporate finance, restructuring and insolvency, trust and company services and forensic accounting.

6.3.2 HKICPA, incorporated under the Professional Accountants Ordinance ("PAO") (Cap.50)[175], is the statutory regulatory body of accountants in Hong Kong. The HKICPA is currently responsible for regulating entry to the profession, registering certified public accountants ("CPAs") and issuing practising certificates, regulating the professional conduct and standards of its members (currently including conducting practice reviews, taking disciplinary actions and imposing sanctions), setting codes of ethics and standards of accounting and auditing, providing continuing education and other services to members, and promoting the accountancy profession in Hong Kong and overseas.

6.3.3 As at the end of 2021, membership of the HKICPA stood at 47 059, including 6 024 fellow members. There were 5 195 members holding practising certificates, 1 268 firms and 668 corporate practices.

ML Threats in Accounting Professionals Sector

6.3.4 Accounting professionals engaging in the trust and company services business will generally operate through separate legal entities because of the need to maintain independence from their auditing duties. Therefore, they are also subject to the ML threat associated with TCSPs (see section 6.4). From 2016 to 2020, there was one convicted ML case involving accounting professionals, in which an accounting firm was an unwitting facilitator of the formation of corporate vehicle that was misused to receive crime proceeds generated from fraud.

6.3.5 Accounting professionals filed around 16 STRs annually from 2016 to 2020 on average. In 2020, the accounting professionals sector filed 16 STRs, of which two were classified as high risk by the JFIU. STRs were mainly triggered by adverse information from other sources including open search, detection of abnormal transactions or suspected crime involvement. In some cases, auditors were unable to obtain sufficient and appropriate audit evidence for the recognition of sales which were settled in cash.

6.3.6 Accounting professionals are exposed to potential ML activities mainly through trust or company services, though the actual threat detected is only limited. The ML threat level of the sector is assessed to be medium-low.

ML Vulnerabilities in Accounting Professionals Sector

Entry controls and integrity

6.3.7 There are stringent entry control procedures prescribed under the PAO, in which individuals have to apply for registration as a CPA with the HKICPA. The HKICPA will assess the fitness and properness of applicants. The procedures for entry to the

[175] Chapter 50 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap50

profession have recently been strengthened and, in particular, with the assistance of the HKPF, the HKICPA will verify whether new applicants for membership have any criminal record. The HKICPA has been provided with the appropriate powers and has sufficient staff and resources to carry out the registration duties.

6.3.8 Accounting professionals generally have high standards of professionalism and integrity. Members of the HKICPA have to comply with the Code of Ethics for Professional Accountants (the "Code") issued by the HKICPA, including, the five fundamental principles of the Code, namely, integrity, objectivity, professional competence and due care, confidentiality and professional behaviour. Overall, accounting is a well-regulated profession in Hong Kong and CPAs are generally known to place considerable emphasis on ethics and integrity, with a culture that is risk-averse and compliance orientated.

Guidance and AML/CFT knowledge of professionals

6.3.9 The HKICPA promulgated the AML/CFT Guidelines and published an AML Procedures Manual for accountants, as well as posting FAQs on the HKICPA website, to facilitate compliance with the statutory requirements. These materials, which also include a separate set of questions and answers on STR available on the website, are regularly brought to the attention of members. The HKICPA also addresses members' technical enquiries on AML/CFT issues, providing quick responses and directing members to the relevant sources of AML/CFT information. It also provided members with timely notices of relevant FATF announcements and updates.

6.3.10 Face-to-face or virtual workshops and seminars on AML/CFT compliance have been organized on a regular basis. From 2016 to 2021, the HKICPA organised around 70 AML/CFT workshops and seminars, including some co-organised with the Government, to keep the accounting sector up-to-date with developments in the STR regime and to increase awareness of the sector's role in combating ML/TF and other illicit activities. About 13 800 accounting professionals attended these events.

6.3.11 Most of the large practice units have well-established, stringent and comprehensive AML/CFT measures in place to address the requirements of relevant laws and regulations and the AML/CFT Guidelines. While the level of AML/CFT controls among smaller practice units varies, members working in practice units are in general aware of AML/CFT compliance and reporting procedures and obligations.

Supervision

6.3.12 The HKICPA also makes ongoing and consistent efforts to oversee the professional conduct of its members and practice units and their compliance with its rules and regulations, and to promote good practices, including conducting outreach activities to promote awareness of AML/CFT. Since October 2018, the HKICPA has been carrying out supervision of AML/CFT compliance by practice units[176], through a new AML/CFT Compliance Monitoring Review Programme within its statutory practice review regime, and over 800 practice units have been reviewed. The supervisory policies and procedures are clear, involving a mix of on-site inspections and desktop reviews.

[176] Under the PAO, a practice unit means a CPA (practicing), a corporate practice or a firm of CPAs (practising).

Sanctions

6.3.13 The HKICPA is empowered by law to investigate breaches of professional standards and to take disciplinary actions against professional misconduct. A wide range of effective, proportionate and dissuasive administrative sanctions are applicable, including financial penalties and, in more serious cases, removal from registration as an accounting professional. From 2016 to 2020, the HKICPA handled one disciplinary case involving a CPA convicted of ML. The CPA was ordered to be removed from the register of CPAs for 10 years. Meanwhile, HKICPA's AML/CFT Compliance Monitoring Review Programme, with extensive inspection and review, has revealed no non-compliance case up to 2020.

6.3.14 The AMLO provides a comprehensive statutory framework requiring accounting professionals to carry out AML/CFT preventive measures; there are also stringent and effective entry controls for the sector, and sector members generally have a high degree of integrity and sound AML/CFT knowledge. The vulnerability of the sector has been reduced by the introduction of risk-based supervision of practice units, and the monitoring programme to check practice units' compliance with AMLO. The ML vulnerability level of the accounting professionals sector is assessed to be medium-low.

ML Risks

6.3.15 Taking into account that the level of ML threat and ML vulnerability of the accounting professionals are both assessed to be medium-low, the ML risk level for the sector is assessed to be medium-low.

6.4 TRUST OR COMPANY SERVICE PROVIDERS

6.4.1 TCSPs include all those persons and entities that, on a professional basis, participate in the creation, administration and management of trusts and corporate vehicles. They engage in the business of company formation, acting as nominee shareholders and directors, providing registered office and business addresses, ongoing corporate administration and secretarial work, trust services, etc.

6.4.2 With effect from March 2018, any person who wishes to carry on a trust or company service[177] business in Hong Kong is required to obtain a licence from the Registrar of Companies and is regulated by the AMLO[178]. A person who carried on a trust or company service business without a licence commits an offence and is liable on conviction to a fine of HK$100,000 and imprisonment for six months. As at 31 December 2021, there were 6 711 licensees on the Register of TCSP Licensees kept by the Registrar.

ML Threats in TCSP Sector

6.4.3 As mentioned in Chapter 4, the engagement of shell or front companies with complex and layering structures was prone to be used in the facilitation of ML activities. Services provided by TCSPs, such as the selling of shelf companies and the setting up of front companies with the opening of bank accounts may be misused for ML purposes such as handling crime proceeds being transferred within, into or away from Hong Kong. Between 2016 and 2020, an average of 67 STRs were filed by the TCSP sector to the JFIU annually. Out of 8 843 reported ML investigation cases, only 71 cases involved TCSPs with transactions amounted to HK$ 201 million which represents about 0.2% of the total proceeds. During the period, 55 out of the total 323 ML conviction cases involved TCSPs. Among the HK$ 11.17 billion crime proceeds involved in all convicted cases, the laundering of about HK$6.99 billion involved TCSPs. Although TCSPs were found to be involved in these convicted ML cases, those were cases in which the material time of the crimes were before the commencement of the TCSP licensing regime. Cases after investigation revealed that the clients of the TCSPs might be involved in ML cases but no evidence showed that TCSPs were consciously assisting the criminals.

ML Vulnerabilities in TCSP Sector

6.4.4 The TCSP sector can be divided into two segments, company service providers and trust service providers. For trust service providers, their clients may include high net-worth individuals, while company service providers may also have clients from high risk jurisdictions who are PEPs. However, for higher risk customers, they are now either subject to the statutory mandatory EDD measures or EDD on RBA. Notwithstanding the inherent risks associated with the wide client base profile of TCSP licensees, the compliance with the relevant CDD and risk assessment requirements has, to a large extent, mitigated the risks and reduced the vulnerability of the TCSP sector.

6.4.5 Moreover, many key officers or staff of TCSP licensees are members of professional bodies, such as the Hong Kong Chartered Governance Institute (formerly known as the Hong Kong Institute of Chartered Secretaries), Hong Kong Trustees'

[177] Trust or company service means the provision, by way of business, the services defined in section 1 of Part 1 of Schedule 1 to the AMLO.

[178] Chapter 615 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap615

Association, the LSHK and the HKICPA. These bodies supervise the conduct of their members and/or provide training and guidance to members on corporate governance and AML/CFT preventive measures. This further mitigates the ML vulnerability of the sector.

Legal and regulatory framework

6.4.6 With the commencement of the amended AMLO on 1 March 2018, which extended the statutory CDD and record-keeping requirements to the DNFBPs, including TCSPs, the implementation of the AML/CFT regime for the TCSP profession has been effective and smooth. The CR, the regulator of the TCSP profession, has continued to step up efforts in enforcing the AML/CFT compliance of the sector.

6.4.7 Under the TCSP licensing regime, the Registrar of Companies is empowered to refuse an application for the grant or renewal of a licence[179] if the relevant person(s) of the applicant/licensee cannot pass the fit-and-proper test. The Registrar of Companies may also revoke or suspend a licence if the relevant person(s) of the licensee are no longer fit and proper to carry on or be associated with the trust or company service business. The AMLO also provides for a range of proportionate and dissuasive sanctions to address non-compliance.

6.4.8 To promulgate the licensing regime for TCSPs and to enhance the understanding of and compliance with the AML/CFT requirements by the TCSP sector, the Registrar of Companies has issued three guidelines, namely Guideline on Licensing of Trust or Company Service Providers, Guideline on Compliance of Anti-Money Laundering and Counter-Terrorist Financing Requirements for Trust or Company Service Providers, and Guideline on Imposition of Pecuniary Penalty. These guidelines are available on the CR's dedicated website for TCSPs[180].

Supervision and enforcement

6.4.9 The CR applies strict entry control to the TCSP sector and has been taking prosecution against persons carrying on a trust or company service business without a licence under the AMLO. By adopting an RBA in the supervision of TCSPs, the CR conducts onsite inspections, interviews and offsite monitoring to ensure the applicants and licensees are in compliance with the requirements under the AMLO, the licensing conditions imposed by the Registrar of Companies and the relevant guidelines issued by the Registrar of Companies.

6.4.10 If any non-compliance with the requirements under the AMLO or AML/CFT Guideline on TCSPs is identified by the CR, follow-up actions will be taken as appropriate such as issuing advisory/warning letters, taking prosecution or disciplinary actions (including public reprimands, pecuniary penalties and remedial orders), making further onsite inspections to ensure that the TCSP licensees have addressed the specific areas that need further improvement.

[179] Licences are normally valid for three years.
[180] https://www.tcsp.cr.gov.hk

Education and outreach

6.4.11 The CR has also organised or participated in over 50 seminars since 2017 to promote the licensing regime and AML/CFT requirements for TCSPs. The JFIU was invited to join in some seminars to highlight the trends and typologies of ML as well as the reporting of suspicious transactions. This helps enhance the understanding of the TCSPs of the ML/TF risks and the measures to mitigate the risks in the sector.

6.4.12 A dedicated website for TCSPs has been set up by the CR to provide detailed information including guidelines, forms, external circulars, information pamphlets, FAQs, other publicity materials on the licensing regime for TCSPs. There is a thematic section on AML/CFT at the website which provides comprehensive information on Hong Kong's AML/CFT regime.

6.4.13 The CR issues circular emails to remind TCSP licensees of their obligations to comply with the statutory requirements on financial sanction, TF and PF. They are also informed of the publication of statement / relevant guidance issued by the FATF. Similar emails are also sent to the associations of TCSPs for dissemination to their members.

6.4.14 Attributed to the TCSP licensing regime, which has been in operation for more than three years since March 2018, the sectoral vulnerability of the TCSP sector has been improving. Unscrupulous practitioners were barred from entering the sector while the compliance with the AML/CFT requirements by TCSP licensees is monitored by the CR. The sector's awareness of ML/TF risks is also improving as evidenced by, e.g. the increase in the number of STRs filed by TCSPs from around 30 in 2017 to over 100 in 2020.

ML Risks

6.4.15 Taking into account the ML threat and vulnerability levels of the TCSP sector discussed above, which are both assessed to be medium, the ML risk level of the sector is assessed to be medium.

6.5 ESTATE AGENTS

6.5.1 In Hong Kong, the real estate brokerage and agency industry includes companies engaged in estate agency work that involved the sale and purchase of actual or prospective properties or the leasing of premises for a client. Together with the real estate development and leasing industry, and the real estate maintenance management industry, they form the three major components of the real estate sector in Hong Kong.

6.5.2 As at 31 December 2021, there were 42 062 individual estate agent or salesperson licences and 3 938 company licences.

6.5.3 The EAA is an independent, self-financing statutory body established in November 1997 under the Estate Agents Ordinance ("EAO") (Cap.511) [181] to regulate and control the practices of the Hong Kong estate agency trade, to promote the integrity and competence of estate agents, and enhance the status of the trade.

6.5.4 In Hong Kong, the main role of estate agents in property transactions is acting as a middleman between potential purchasers and sellers, arranging property viewings and the signing of provisional agreements for sale and purchase. Estate agents commonly have face-to-face contact with purchasers and sellers, allowing them to acquire knowledge of the background of their clients.

6.5.5 While estate agents play an important role in property transactions, they are inherently less vulnerable than other facilitators such as conveyancing solicitors and banks, as they are generally not involved in the fund-flow chain. Where estate agents do handle funds, the amount only commonly constitutes the initial deposit of around 3% to 5% of the transaction value, and even such value is seldom settled in cash. In most, if not all, cases, the estate agents' role in handling clients' money is confined to passing the purchaser's personal cheque for the initial deposit to the seller or the seller's solicitors upon signing of the provisional agreement for sale and purchase. After the provisional agreement for sale and purchase is signed, payment of the further deposit and balance of the purchase price invariably involves conveyancing solicitors and banks.

6.5.6 In the first-hand sale of residential properties, prospective purchasers usually submit a registration of intent together with a payment (usually by way of a cashier order) to the seller (the property developer) to express their intent to purchase when the sale commences. It is common for estate agents to assist prospective purchasers to participate in the lot drawing for purchasing these properties. In doing so, they may, on receipt of the same amount of money from a prospective purchaser (usually paid by credit card or cheque), arrange issuance of a cashier order by a bank for submission to the seller. Dealing with cash is rare in such circumstances.

ML Threats in Real Estate Sector

6.5.7 It is not uncommon for crime proceeds to be converted into different types of assets including real estate. Based on Confiscation Orders granted between 2016 and 2020, around 15% (around HK$216 million) of crime proceeds confiscated were real estate property. From 2016 to 2020, there were four convicted ML cases which estate agents

[181] Chapter 511 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap511

involved either directly in the predicate and ML offences or as unwitting agents. From 2016 to 2020, STRs filed by estate agents only took up a small proportion of total STRs submitted, with around 69 STRs on average annually. In 2020, the sector filed 93 STRs and none of these were classified as high risk. A large proportion of STRs were also found related to real estate transactions without any mortgage or financial assistance. Estate agents play an important role in the transactions as they are responsible, at an early stage of the transaction, for conducting CDD of the buyers and sometimes recommending different financial and legal service to the buyers. Although estate agents are generally not part of the fund-flow chain, ML threat is presented to them where they facilitate the transaction.

6.5.8 Estate agents are exposed to potential ML activities mainly through real estate transactions, and property as an asset class which attract buyers of high net-worth individuals. With the limited role of estate agents and limited actual threat of using estate agents as conduit for ML, particularly through witting involvement, the ML threat level of the sector is assessed to be medium-low.

ML Vulnerabilities in Real Estate Sector

Entry controls and integrity

6.5.9 Unless otherwise exempted, all individuals and companies carrying on estate agency work must hold a licence issued by the EAA under the EAO. It is an offence to practice estate agency work without a valid licence. The EAO provides that an individual shall not be eligible to be granted an estate agent or salesperson's licence unless he satisfies the prescribed requirements and the EAA otherwise considers him/her a fit and proper person to hold a licence. In practice, the EAA assesses the fitness and properness of applicants having regard to a number of factors including their criminal records from the Police. The EAA has been provided with appropriate powers to carry out the licensing duties.

Guidance and AML/CFT knowledge of professionals

6.5.10 The EAA has promulgated guidelines in its Practice Circular[182] to facilitate compliance with the statutory AML/CFT requirements, which require licensees to implement CDD and record-keeping measures and establish internal procedures against ML/TF.

6.5.11 The Government has been working with the EAA to raise the awareness of the sector through outreach programmes such as seminars promoting the FATF's international standards. Moreover, to strengthen licensees' understanding of their AML/CFT obligations, the EAA has also taken extensive awareness building and outreaching measures since the AMLO took effect, such as created a designated AML Corner in the EAA's website, an AML/CFT outreach educational programme to estate agency operators, and courses on AML/CFT for frontline licensees and senior management of estate agency firms; as well as encouraged estate agency firms to provide AML/CFT internal training to their employees. From 2018 to 2021, an average of about 60 continuing professional development activities on AML/CFT were held annually and the number of enrolments of continuing professional development activities on AML/CFT averaged at about 5 100 enrolments every year.

[182] Practice Circular No. 18-01.

Supervision

6.5.12 The EAA conducted an intensive study in 2019/20 on the estate agency operators' threat and vulnerability to ML and TF risks at institutional level. Through this study, the EAA updated its risk profiling and classification of individual estate agency operators into different risk categories. Based on the findings derived from the study, the EAA has been adopting a RBA in its supervision of the estate agency trade practitioners' compliance with AML/CFT requirements. From April to December 2020, the EAA conducted around 1 000 compliance inspections for AML/CFT requirements.

Sanctions

6.5.13 The EAA is empowered by law to investigate breaches of and take disciplinary action against professional misconduct. A wide range of effective, proportionate and dissuasive administrative sanctions are applicable including monetary penalty and, in more serious cases, revocation of licence. During the period from 1 March 2018 to 31 December 2020, one licensed estate agent was disciplined for breach of AML related requirements and the sanctions imposed on her were reprimand and attachment of a condition to the licence which required her to attend additional continuing professional development trainings. For a number of cases investigated in 2020, applicable sanctions were applied subsequently in 2021, including reprimand, fine and attendance of additional continuing professional development trainings.

6.5.14 The AMLO provides a comprehensive statutory framework in requiring estate agents to carry out AML/CFT preventive measures; there are also effective entry controls for the sector through fit-and-proper tests. The robust risk-based supervision regime implemented by the EAA has further reduced the sector's vulnerability and facilitated the EAA to acquire good understanding of the risks of licensees and devise supervision plans. The ML vulnerability level of the sector is assessed to be medium-low.

ML Risks

6.5.15 Taking into account the ML threat and vulnerability of the estate agents sector discussed above, which are both assessed to be medium-low, the ML risk level for the sector is assessed to be medium-low.

6.6 DEALERS IN PRECIOUS METALS AND STONES

6.6.1 DPMS in Hong Kong can be roughly divided into three categories: retail, wholesale and metal exchange, selling products of diverse value. In 2021, retail sales of jewellery, watches and precious metals accounted for about 11% of total retail sales by value, at HK$39 billion[183]. The retail business is supported by both local and non-local clientele.

6.6.2 The jewellery industry is largely export-oriented. Hong Kong manufactures and exports jewellery, with jewellery and precious metals accounting for around 9% of the total exports in 2021, at HK$473 billion[184]. Hong Kong also organises annual jewellery trade fairs for local and overseas buyers.

6.6.3 Hong Kong operates a precious metal exchange market, with paper or physical precious metals available as investment products. Besides FIs, the Chinese Gold and Silver Exchange Society ("CGSE") is a major exchange of precious metals. In December 2021, the CGSE had 170 corporate members which provide precious metal trading services for individual or corporate clients.

6.6.4 The import and export of gold, other precious metals and precious stones are governed by the IEO and associated regulations. Controls are in place with respect to (i) declaration and manifestation for imports and exports; (ii) registration and certification of the rough diamond traders; (iii) regulation of the standard of fineness of precious metals (i.e. gold, gold alloy, and platinum); and (iv) protection of intellectual property rights. The regulatory regime helps reduce the risk of misuse of the sector for ML/TF purposes as, for instance, an audit trail of the precious metals and stones can be established as and when necessary.

6.6.5 The larger establishments have commonly taken steps against ML/TF activities, such as identifying risky transactions and verifying customers' identity, especially for transactions that involve large amounts of cash. Dealers tend to trade with reputable and reliable business partners with whom they have established long-term relationships. On the precious metal exchange, settlements are generally not cash-based.

6.6.6 To provide a comprehensive legal framework and regulatory regime for the DPMS sector under AMLO, the Government launched a consultation exercise from November 2020 to January 2021 to gauge public views on legislative proposals to enhance AML/CFT regulation through the introduction of a registration regime for DPMS under the AMLO.

6.6.7 Under the new registration regime, any person seeking to conduct the regulated business of dealing in precious metals, precious stones, precious products, or precious-asset-based instruments in Hong Kong will be required to register with the CCE. Persons who do not seek to engage in cash transactions at or above HK$120,000 during their course of business will be registered as Category A registrants while those who do so, upon

[183] Census and Statistics Department – retail sales by type of retail outlet. The figure drops when compared with last report in 2017 of HK$75 billion due to impact by the pandemic.

[184] Census and Statistics Department – generated from Interactive Data Dissemination Service for Trade Statistics.

passing a fit and proper test, are to be registered as Category B registrants who will be subject to the full range of AML/CFT requirements under Schedule 2 to the AMLO. The CCE will be empowered to supervise the DPMS in accordance with the AMLO requirements, and various sanctions against breach of requirements are provided under the proposed regulatory regime, including administrative sanctions, fine and imprisonment.

ML Threats in DPMS Sector

6.6.8 While crime proceeds can be converted into precious metals and stones, a review on the Confiscation Orders granted between 2016 and 2020 shows that only about HK$ 3.26 million of assets out of around HK$ 1.43 billion confiscated were related to precious metals and stones, jewellery and watches. From 2016 to 2020, there were three convicted ML cases related to DPMS, in which DPMS were involved either directly in the predicate or ML offences or as an unwitting agent. From 2016 to 2020, STRs filed by DPMS only took up a small proportion of total STR submitted, with around 47 STRs on average annually. In 2020, the sector filed 25 STRs, of which eight were classified as high risk. Reasons of filing STR varied, which included the purchase of large amount of gold or other precious metals using cash, making it difficult to ascertain the source of fund.

6.6.9 DPMS are exposed to potential ML activities mainly through the buying and selling of precious metals and stones. Although some products are of very high value, the level of cash transaction is relatively low. The ML threat level for the sector is assessed to be medium-low.

ML Vulnerabilities in DPMS Sector

6.6.10 DPMS are encouraged to adopt the AML/CFT measures under the AMLO. The CGSE has been promoting good practices among corporate members and their staff. Since 2010, CGSE has implemented a registration system requiring responsible persons and traders among corporate members to be fit-and-proper persons. All responsible persons and traders are also required to undergo continuing professional development programmes, in which AML/CFT is a key topic..

6.6.11 The Government has continued its efforts to raise the AML/CFT awareness of the DPMS sector and enhance their understanding of ML/TF risks. An updated AML/CFT Guideline for the DPMS sector was issued in 2018 to assist its development of best practices and procedures to guard against potential abuse for ML/TF. From 2016 to 2021, regular capacity-building seminars were held.

6.6.12 Currently, statutory AML/CFT preventive measures are not yet imposed specifically on the sector. The ML vulnerability level of the sector is assessed to be medium. Vulnerability of the sector would be further addressed by the introduction of a registration regime for DPMS under the AMLO.

ML Risks

6.6.13 Pending the introduction of a regulatory framework, the ML threat and ML vulnerability of the sector are assessed to be medium-low and medium respectively. Combining the two, the ML risk level is assessed to be medium.

6.7 NEXT STEPS

6.7.1 The implementation of the statutory AML/CFT regime under AMLO for DNFBP sectors has been generally smooth. Regulators of DNFBPs have gained more experience in RBA, and have been stepping up efforts to enhance RBA, including the implementation of on-site and off-site inspection, capacity building initiatives and outreaching programmes to the sectors. Looking ahead, the Government and the sectors concerned will continue to work together to enhance the relevant AML/CFT regimes, among others, including the following measures –

(a) for the legal professionals sector, the LSHK is developing a more robust risk-based supervision regime, such as conducting a survey of law firms' risk profiles, as well as enhancing supervision of law firms on AML/CFT practices. The LSHK has appointed an AML Executive and the adequacy of compliance with the AML/CFT requirements is being constantly reviewed and monitored by the AML Committee of LSHK.

(b) for the accounting professionals sector, with the passage of the Financial Reporting Council (Amendment) Bill 2021 in October 2021, the Financial Reporting Council (to be renamed as Accounting and Financial Reporting Council ("AFRC")) will take up the regulatory functions from the HKICPA in respect of accounting professionals in Hong Kong, including issuance of practising certificates to CPAs; registration and inspection of practice units; investigation and discipline of all CPAs, CPAs (practicing) and practice units; and overseeing the remaining statutory functions of the HKICPA in respect of setting of requirements for and provision of continuing professional development, setting of standards of professional ethics, and setting of accounting and auditing standards, as well as registration of CPAs including conducting qualifying examinations for CPAs and mutual and reciprocal recognition of accountants with overseas accountancy bodies. The AFRC will become the regulatory body of accounting professionals from October 2022.

(c) for the TCSP sector, the CR will remain vigilant in identifying emerging ML risks and continue to take a proactive approach to mitigate such risks in the sector. CR will also revise the AML/CFT Guideline, adopt a more robust supervision of the TCSP sector by developing a supervisory plan for TCSPs which includes the risk profiling of individual TCSP licensees according to risk assessment criteria and enhance the sector's understanding of AML/CFT requirements through outreach programmes;

(d) for the estate agents sector, the EAA will continue its efforts in implementing its risk-based supervision programme, and other capacity building efforts; and

(e) for the DPMS sector, the Government will introduce a registration regime for the DPMS sector under the AMLO. The Government has introduced the amendment bill into the LegCo in July 2022. The registration regime for DPMS is expected to come into full operation in 2023.

CHAPTER 7

LEGAL PERSONS AND ARRANGEMENTS

7.1 Corporate vehicles can be misused for illicit purposes. As discussed in Chapter 4, typologies continue to suggest shell companies remain as a common conduit for ML. It is common that criminals will recruit stooges to conceal their ownership of the shell companies so that they can process illicit funds without physical presence. On the other hand, the use of offshore companies to facilitate ML activities has become less popular because reporting entities have enhanced their CDD requirements to identify beneficial owners of all types of companies. Misuse of corporate bank accounts continues to feature in cases of predicate offences such as online fraud, email/telephone scams and investment fraud. Offshore companies as well as corporate vehicles, trusts, and nonprofit entities are used to hide proceeds of corruption. Complex corporate structures and trusts are used to conceal ownership and control of proceeds of foreign tax evasion. A good number of the ML cases prosecuted in Hong Kong involve corporate accounts of legitimate businesses which have been exploited, or set up by shell companies to hide beneficial ownership.

7.2 There remains little evidence that Hong Kong trusts are being abused for misuse for ML/TF purposes. Our law enforcement authorities continue to keep a close eye on the risk of abuse of foreign trusts through linked complex structures. In addition, revelations from the Pandora Papers have highlighted the abuse of corporate structures and legal arrangements at the international level.

7.3 This Chapter therefore examines the position of companies and other entities and trusts in Hong Kong and their transparency in the context of ML. Since the 1st HRA, there are several major policy changes which boosted the effectiveness of Hong Kong's legal persons and legal arrangements regime, including the commencement of a statutory licensing regime for TCSPs and mandatory requirements on the keeping of SCR by companies since March 2018.

Legal Persons and Other Entities

7.4 From 2017 to 2021, an average of around 129 400 companies have been newly incorporated each year[185]. By end 2017, around 1.38 million live companies were on the Companies Register, with around 10 400 registered non-Hong Kong companies. By end 2021, the number of live companies on the Companies Register remained at around 1.38 million[186], while the number of registered non-Hong Kong companies increased to around 14 350.

[185] The numbers of new companies incorporated in 2020 and 2021 were 99 405 and 110 840 respectively. These figures reflected the dampening economic condition as a result of the COVID-19 pandemic.

[186] Out of 14 350 registered non-Hong Kong companies, around 2 350 are listed companies which are subject to the more stringent disclosure requirements under the SFO.

Table 7.1: Number of companies incorporated from 2017-2021

	Year				
	2017	**2018**	**2019**	**2020**	**2021**
Public companies	40	38	54	78	61
Private companies	159 239	150 738	123 700	98 368	109 745
Companies limited by guarantee	950	963	987	959	1 034
Total	160 229	151 739	124 741	99 405	110 840

Table 7.2: Number of non-Hong Kong companies registered from 2017-2021

Year	**2017**	**2018**	**2019**	**2020**	**2021**
Total	1 028	1 193	2 000	1 757	1 316

Business registration

7.5 Unless exempted under the Business Registration Ordinance ("BRO") (Cap. 310)[187], every person carrying on business[188] in Hong Kong must apply for business registration within one month of commencement of business. Under the one-stop company and business registration service, a person who submits an incorporation form of a local company or an application form for registration of a non-Hong Kong company at the CR is deemed to have simultaneously applied for business registration. Other types of businesses, including sole proprietorships, partnerships and unincorporated bodies of persons, and branch businesses are required to submit their business registration applications to the Business Registration Office under the IRD direct.

[187] Chapter 310 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap310

[188] Business includes any form of trade, commerce, craftsmanship, profession, calling or other activity carried on for the purpose of gain; any club which provides facilities, services and exclusive club premises to its members for social intercourse or recreation; and every non-Hong Kong company that has a representative or liaison office in Hong Kong, or has let out its property situated in Hong Kong, regardless of whether it has established a place of business in Hong Kong.

7.6 By end 2021, there were 1.55 million business registrations. Companies continue to account for the largest population of business entities in Hong Kong. Around 80% of the newly incorporated companies were one-member companies. The rest of the business registration is mainly attributable to sole proprietorships and partnerships[189]. Persons carrying on business in these forms, such as law and accounting firms[190] may have registered under the BRO without registering as a company under the CO.

Table 7.3: Number of business registration during 2017-2021

	Number of business registration as at 31 December				
	2017	**2018**	**2019**	**2020**	**2021**
Corporations	1 264 675	1 271 846	1 266 676	1 276 427	1 258 776
Sole proprietorships	234 119	231 110	236 535	250 360	258 932
Partnerships	27 736	26 471	26 006	26 452	26 479
Other bodies unincorporated (e.g. club, joint venture)	755	790	831	1 059	1 100
Total	1 527 285	1 530 217	1 530 048	1 554 298	1 545 287

OFC and LPF

7.7 A new OFC structure was introduced in July 2018 to enhance the market infrastructure for investment funds (see section 5.3.23). For the OFC regime, the SFC is the primary regulator responsible for the registration and regulation of OFCs under the SFO. The CR oversees the incorporation and statutory corporate filings of OFCs and maintains an OFC Register for public inspection of the name index of OFCs and digitised images of the registered documents in relation to OFCs. The CR also administers a new limited partnership fund ("LPF") regime with effect from 31 August 2020 for private investment funds to set up and register in the form of a limited partnership in Hong Kong. An LPF does not have a legal personality. Since the introduction of the two new regimes in 2018 and 2020, 48 OFCs were incorporated and 410 LPFs were registered as at end 2021.

[189] Sole proprietorships and partnerships are not separate legal persons from proprietors or partners. For a sole proprietorship, the business is owned and operated by a person who is entitled to all the profits but also solely and personally responsible for all liabilities. Partnerships are businesses established and co-owned by two or more persons (who may be individuals or corporations). General partnerships make every partner personally liable for the debts and liabilities of the business, as well as the actions of another partner conducted in the course of the partnership business. LPs constitute both general and limited partners. A general partner has unlimited liability for the firm's debts and is responsible for day-to-day running of the business, while limited partners' liability is limited to the amount of their contribution. Limited partners cannot participate in the management of the partnership.

[190] Law firms and accounting firms may be required to first obtain the relevant professional practicing certificates before commencement of business.

Credit unions

7.8 For credit unions, the ML vulnerability level of the credit union sector remains at low. Credit unions in Hong Kong are regulated under the Credit Unions Ordinance (Cap. 119)[191]. By nature and constitution credit unions are not meant to operate as a business. Credit unions in Hong Kong provide only basic services of savings by share subscription and lending to their members. Membership of the credit unions is usually restricted to members of specific employment or trades as prescribed in their respective by-laws. While individual members maintain separate accounts in a credit union, saving and lending activities are essentially conducted through bank accounts designated by members. Credit unions generally do not handle cash transactions. By end 2021, there were 44 registered credit unions in Hong Kong, with a total membership of around 95 600 and total capital of about HK$22 billion. Over 99% of assets of credit unions belong to those formed by employees of government departments and large public and private institutions.

Limited partnerships ("LPs")

7.9 The CR is responsible for registering LPs. There are 227 LPs on the register of LPs as at end December 2021 and they mainly engaged in different kinds of professional/consultancy services and investment businesses. Majority of the LPs receive contribution from limited partners in the amount of less than HK$100,000. No cases of LPs involved in ML/TF activities was found. This indicates that the LP sector is low in ML/TF risks.

7.10 Other legal persons, such as co-operatives, trade unions, and owners corporations do exist in Hong Kong, but their use and membership is highly restrictive, so they have no material ML/TF risk at all. Partnerships, including limited liability partnerships, are not companies under Hong Kong law and have no separate legal personality from the individuals forming the partnership. Nevertheless, law enforcement authorities continue to keep a close eye on STRs and typologies involving these types of legal persons.

7.11 Hong Kong is known for efficient company-formation procedures and some Hong Kong companies were incorporated to hold properties or club memberships. Corporations are used in ML cases in Hong Kong in the layering process to increase the difficulty and time taken to trace proceeds of crime. In cases involving the use of more advanced ML techniques, front companies are established to transfer crime proceeds from one jurisdiction to another under the disguise of payments resulting from legitimate business activities, such as imports and exports.

7.12 To hide the true beneficial ownership, criminals may set up shell companies and launder money through corporate bank accounts. Case examples indicate that these shell companies usually have similar risk profiles such as (i) single shareholder or director; (ii) no nexus to Hong Kong; and (iii) with a vague business nature. They often make use of newly established corporate accounts to process large and frequent transactions while maintaining low account balances.

[191] Chapter 119 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap119

Box 7.1 - Case study

In October 2014, the former President of a publicly listed company in Hong Kong (the defendant) was convicted after trial at the Court of First Instance on charges of bribery and fraud. Upon conviction, an application for a confiscation order was made against the defendant. During the confiscation proceedings, it was discovered that the defendant is the sole director of a shell company, BVI company A which maintains a bank account in Hong Kong having a credit balance of about HK$29.5 million. Investigation revealed that the defendant had effective control of the bank account held in the name of the BVI company A and that another BVI company (BVI company B) is the sole shareholder of the BVI company A. Investigation further revealed that an offshore person is the registered shareholder of BVI company B, hence the ultimate owner of BVI company A. When interviewed, the offshore person confirmed that he had no beneficial interest in both BVI companies or in the assets held by BVI company A and that he signed documents upon the request of the defendant's ex-wife.

The bank account held in the name of BVI company A was restrained in April 2016. In February 2018, a confiscation order in the sum of HK$8 million was made against the defendant, which was settled by BVI company A.

Legal Arrangements

7.13 The law of trusts in Hong Kong is based on and derived from the English law of trusts[192]. The common law concept of trust is in use in Hong Kong. A trust may be defined as "the relationship which arises whenever a person (called the trustee) is compelled in equity to hold property, whether real or personal, and whether by legal or equitable title, for the benefit of some persons (of whom he may be one and who are termed beneficiaries) or for some object permitted by law, in such a way that the real benefit of the property accrues, not to the trustees, but to the beneficiaries or other objects of the trust"[193]. The common law rule is that a trustee must execute the trust with reasonable diligence, and conduct its affairs in the same manner as an ordinary prudent man of business would conduct his own affairs. A higher standard of care applies to a trust corporation or similar body which carries on a specialised business of trust management[194].

7.14 The principal legislation relating to trusts in Hong Kong is the Trustee Ordinance ("TO") (Cap. 29)[195]. It governs, *inter alia*, the powers and duties of trustees. The TO has been amended with effect from 1 December 2013 to introduce a statutory duty in relation to certain functions a trustee carries out, including investment, delegation, appointing nominees and custodians, taking out insurance and powers in relation to accepting property, valuations and audit[196]. Where the statutory duty applies, the trustee must exercise the care and skill that is reasonable in the circumstances, having regard to (a) any special knowledge or experience that the trustee has or holds out as having; and (b) if the trustee is acting in that capacity in the course of a business or profession, any

[192] Halsbury's Laws of Hong Kong, [400.001].
[193] Law of Trusts (12th edn), p3; quoted in Lewin on Trusts (19th edn), 1-003. 201 Halsbury's Laws of Hong Kong, [400.332].
[194] Halsbury's Laws of Hong Kong, [400.332].
[195] Chapter 29 of the Laws of Hong Kong. https://www.elegislation.gov.hk/hk/cap29
[196] Schedule 3 to the TO.

special knowledge or experience that is reasonably expected of a person acting in the course of that kind of business or profession[197]. The duty of care imposed on trustees under the general law continues to govern the administration of trusts where the statutory duty of care does not apply.

7.15 Trusts can be used for both private (e.g. personal inheritance) and commercial purposes (e.g. fund management). Any company incorporated in Hong Kong (which is not a private company) may apply to the Registrar of Companies to be registered as a trust company under the TO, subject to certain requirements (including restrictions on the company's objects and its issued share capital being not less than HK$3 million). Registration as a trust company under the TO is voluntary. Although there is no registration requirement for express trusts[198], the common law principle requires trustees of any express trust to discharge a number of duties in the administration of the trust. Such duties include acquaintance with the terms of the trust and its affairs, conforming to and carrying out the terms of the trust, taking possession and preserving trust property, keeping an accurate account of the trust property and rendering the account when required[199].

7.16 There is little in the way of typologies or data to suggest domestic trusts are being abused for ML/TF purposes in Hong Kong. There is no confirmed ML case involving the use of a Hong Kong trust. Our LEAs rarely encounter abuse of Hong Kong trusts in high-end ML investigations. Private trusts may also be administered by legal professionals, accounting professionals, or TCSPs, for obvious reason of ensuring legal protection especially when assets are involved, which are all regulated under the AMLO. As for charitable trusts, they would qualify as such for tax exemption under section 88 of the IRO only if they are subject to the jurisdiction of the courts in Hong Kong and established for charitable purposes and for public benefit, which means that they must not be established for the benefit of specific individuals. Trust companies incorporated under the CO are required to maintain beneficial ownership information by way of keeping SCRs for inspection by LEAs.

7.17 Under the IRO, reporting FIs are required to report certain financial account information to the IRD for exchanging with other jurisdictions with which Hong Kong has an arrangement for AEOI. The legal obligation applies to any trust which has any beneficial owner being a tax resident of a reportable jurisdiction if either of the following applies (a) the trust is a reporting FI, or (b) the trust is a non-financial entity that maintains a financial account with a reporting FI. In essence this captures most trusts with financial assets in Hong Kong which have a beneficial owner being a tax resident of a reportable jurisdiction. Hong Kong also has an extensive network of bilateral / multilateral tax arrangements with other jurisdictions to enable the EOI (i.e. through comprehensive avoidance of double taxation agreements/arrangements, tax information exchange agreements and the Convention), in addition to the Foreign Account Tax Compliance Act Intergovernmental Agreement with the United States which requires reporting Hong Kong FIs to report to the United States the financial information in respect of their United States clients.

---

[197] Section 3A of the TO.

[198] An express trust is usually formalised by an agreement or deed.

[199] Halsbury's Laws of Hong Kong [400.326] to [400.328] and [400.340] to [400.432] and Equity and Trust Law in Hong Kong, Lawrence Yan-Kwok Ma, LexisNexis, 2006, [19-30] to [19-56], in particular, [19-35] and [19-50].

7.18 The risks posed by foreign trusts are, however, more significant particularly when they form part of complex multi-jurisdictional structures with links to or through Hong Kong. International typologies continue to suggest that trusts can be abused to form part of a complex structure for evading tax or laundering illicit funds. Complex corporate and trust-related structures are frequently used to evade tax, but they can also be used to launder illicit funds. Such foreign trust structures thus pose medium to medium-high ML risks to the financial sector and DNFBPs in Hong Kong. The risk of trusts being misused for TF purposes is assessed as low.

Company Formation and Legal Requirements

Company formation

7.19 The CR is primarily responsible for the administration of the CO. The major roles of the CR include incorporating and registering new companies, registering documents filed by companies, providing public search services, and enforcing the CO. An application for company incorporation will only be approved if all the statutory requirements under the CO are complied with. The CR may reject an application for incorporation if, for example, the proposed company is not formed for a lawful purpose. The incorporation form contains a statement of compliance and the founder member who signs the form is accountable for the accuracy of the information reported therein.

7.20 All companies are required by the CO to keep registers of directors, members and company secretaries, and, since 1 March 2018, their SCRs. Basic ownership information of companies can be accessed by any person through the CR's electronic search services. Such records can be readily accessed by FIs and DNFBPs performing CDD, making legal persons sufficiently transparent.

Bearer shares and corporate directors

7.21 Bearer shares are unregistered shares wholly owned by whoever holds the physical stock certificate. The issuing company neither registers the owner nor tracks transfers of ownership. The company pays dividends when a physical share warrant is presented. Transferring ownership involves only delivering the physical document. Such shares are anonymous and easily transferrable which presents a threat of misuse for ML and TF.

7.22 Since March 2014, companies are prohibited to issue share warrants to bearer. All bearers' names were required to be entered in the register of members of the company [200].

7.23 To enhance transparency and accountability, it has also been a requirement since 2014 for private companies to have at least one director who is a natural person. Companies which failed to comply with such requirements (which might include shell companies) had been struck off or had resorted to deregistration. This had a significant impact on companies formerly established with corporate directors, with 111 000 applications for deregistration of solvent inactive companies received between October 2014 and December 2016. It had become more popular for solvent inactive companies to resort to deregistration with a total of around 323 800 applications for deregistration received from 2017 to 2021.

[200] Section 139 of the CO.

Major updates on transparency and beneficial ownership information

7.24 Under the Companies (Amendment) Ordinance 2018, which commenced operation on 1 March 2018, companies incorporated in Hong Kong[201] are required to maintain beneficial ownership information by way of keeping an SCR. Significant controllers include registrable persons and registrable legal entities exercising significant control over the company. A registrable person is a natural person or specified entity that ultimately has significant control over the company and a registrable legal entity is a legal entity (whether or not incorporated in Hong Kong) which has significant control over the company and is a member of the company. Specified condition to determine significant control over the company comprise any of the following: (i) directly or indirectly holding more than 25% of the issued shares of the company; (ii) directly or indirectly holding more than 25% of the voting rights of the company; (iii) directly or indirectly holding the right to appoint or remove a majority of the board of directors of the company; (iv) having the right to exercise or actually exercising significant influence or control over the company; (v) having the right to exercise or actually exercising significant influence or control over the activities of trust or a firm that is not a legal person, but whose trustees or members meet any of the foregoing conditions in relation to the company. A company must maintain the SCR at the company's registered office or a prescribed place in Hong Kong, keep the information up-to-date and make it available to a law enforcement officer for inspection and copying.

7.25 Companies are required to identify, verify and record personal particulars of the natural persons who exercise ultimate control of the companies as well as the particulars of the legal entities through which the beneficial owners exercise control. Accuracy of SCRs is ensured by requiring companies to serve notices on beneficial owners or related parties, confirm in writing personal particulars of beneficial owners and report changes within prescribed timeframe, and by inspections conducted by the CR for ensuring compliance with the statutory requirements. SCRs must be made available for inspection on demand by LEAs (without the need to obtain court orders) for the performance of their functions under the law of Hong Kong including ML/TF prevention, detection and investigation purposes. It is a criminal offence not to keep an accurate and up-to-date SCR or to refuse inspection by LEAs. Through the inspection of SCR, beneficial ownership information of companies is accessible by law enforcement officers.

7.26 The SCR must also contain the name and contact details of a person designated by the company as its representative to provide assistance to the law enforcement officers. The designated person must be a member, director or an employee of the company who is a natural person resident in Hong Kong; an accounting professional; a legal professional; or a licensed TCSP. Law enforcement officers also have powers under relevant Ordinances to obtain beneficial ownership information from FIs, which are required to keep such information under the AMLO.

7.27 The implementation of SCR regime enhances LEAs' ability to obtain beneficial ownership information, and LEAs will make use of the SCR to cross-check information obtained from banks. SCR is a useful investigative tool as it provides detailed personal particulars of the controllers (usually shareholders), identifies the ultimate beneficial owner(s) of the company, and provides information of the person that instructed the

[201] Listed companies are exempted and remain subject to the more stringent disclosure requirements under the SFO.

secretarial firm to establish the company. Companies can no longer claim ignorance of beneficial owners given the legal requirements for them to take proactive steps to identify and verify such and to designate a representative for rendering assistance to LEAs. It also helps with the case where a company does not have bank accounts in Hong Kong.

Information verification and enforcement

7.28 Sometimes, the subjects of ML investigation have been found to be shell companies with no actual business in Hong Kong. Although the director or shareholder who controls a shell company is normally a non-resident, the OSCO and the DTROP empower LEAs to seek restraint and confiscation of the proceeds of the shell company in Hong Kong pursuant to absconder proceedings.

7.29 Although the CR is not required to verify the contents of documents under the CO, the CR adopts an RBA in conducting checks of applications for incorporation of local companies / registration of non-Hong Kong companies to ensure that accurate information on identities of individuals is provided. In these cases, certificates of incorporation/registration will only be issued after the identity documents and any other documentary evidence are checked.

7.30 The CR conducts regular on-site inspections at registered offices of local companies (including company service providers) and at principal places of business of registered non-Hong Kong companies to check the correct location of companies and the existence of relevant companies, ensure compliance with the requirements for publication of company names and, for local companies, the keeping of proper registers. Since the implementation of the SCR regime in March 2018, onsite inspections of companies for compliance of the requirements for keeping SCR had been conducted. During the site inspections, CR officers will check the accuracy of the information in the SCR. If discrepancies are noted during the site inspections, follow-up actions, including prosecutions, will be taken. The CR also instituted prosecutions against companies for failing to keep SCR which were identified by other LEAs during their investigations and reported to the CR. The compliance rate has been improving over the years with an average of over 95% as revealed from the CR's site inspections conducted in 2020 and 2021.

7.31 To ensure that information in the Companies Register is accurate and up-to-date, the CR has a well-established mechanism to strike defunct companies off the Register. The HKPF will provide the information on local companies that are opened without any business operation for the CR to take appropriate action. From 2017 to 2021, about 296 900 companies were struck off the Register.

7.32 To ensure availability and transparency of information, the CR has identified cases of non-compliance with filing obligations, such as annual returns, for enforcement action. There is a system programme for issuing compliance notices to companies for delivery of annual returns. Companies that do not comply are liable to prosecution and/or being struck off.

7.33 To facilitate public scrutiny of information on the Companies Register, an e-Monitor Service was introduced in December 2011. Subscribers receive instant electronic notification when a document is registered in the public records of a specified company. As

at 31 December 2021, there were 175 116 subscribers.

7.34 As an international financial centre with efficient company formation and banking sectors, Hong Kong remains an attractive location for local and foreign criminal elements to abuse corporate entities in order to disguise the flow of illicit proceeds and beneficial ownership and control. Typologies and data confirm that the risk of companies being abused for ML purposes in Hong Kong is high. The effective implementation of the SCR regime and the licensing regime for TCSPs (discussed in paragraphs 7.35 to 7.42 below and in Chapter 6), combined with enhanced law enforcement powers and efforts has helped mitigating the risk. At the same time, FIs and DNFBPs (including TCSPs) providing services to registered non-Hong Kong companies are subject to CDD and record-keeping requirements of the AMLO. Due to the lack of evidence of exploitation of companies for TF purposes, the risk of companies being abused for TF is assessed as low.

Implementation of the TCSP licensing regime

7.35 Criminals may use the services of TCSPs in the exploitation of legal entities and arrangements, for example by creating the complex structures which impede investigations or obscure beneficial ownership. Since the 1st HRA, TCSPs are required to be licensed and must satisfy the fit and proper test before a licence can be granted. They are required to comply with the AML/CFT requirements of the AMLO as enforced by the CR and the guidelines issued by the Registrar of Companies.

7.36 By end 2021, there was 6 711 licensed TCSPs. The majority of the TCSP licensees are established as companies (around 97%) with a very low percentage of licensees operates in the form of sole proprietor and partnership. There are a number of TCSPs established by FIs, accountancy or legal firms to compliment the suite of financial, accountancy or legal services they offered to clients.

7.37 The CR applies stringent controls in the licensing process. These controls resulted in applications being rejected or withdrawn. The applications were rejected mainly because the applicants failed to meet the fit-and-proper test.

7.38 Since the commencement of the licensing regime for TCSPs, there is an upward trend of STRs submitted by TCSPs. The number of STRs filed by TCSPs from 2018 to 2020 was significantly higher than those years before the commencement of the licensing regime and the 1st HRA. This can be attributable to the increasing awareness of TCSPs about their obligations of submitting STR and the CR's efforts in putting forward educational campaign and training.

Table 7.4: Number of STRs submitted by TCSPs

Year	2016	2017	2018	2019	2020
No. of STRs	27	31	81	91	104

7.39 The CR has been developing a more robust risk-based supervisory approach with a supervisory plan including on-site inspections and off-site monitoring for monitoring TCSP licensees' ongoing AML/CFT compliance. The CR continues to identify those TCSPs of higher risk to Hong Kong. For higher risk cases, on-site inspections are conducted on a priority basis and the TCSP licensees are subject to more frequent compliance inspections to ensure their continuous compliance with the statutory CDD and record-keeping requirements.

7.40 By end 2020, major findings of the inspection on TCSP licensees are as follows:

- A vast majority of licensees have put in place adequate and proper AML/CFT policies, procedures and control in respect of filing and record-keeping of STRs.
- Most licensees maintain their records of customers and transactions in digital format (in-house IT system or cloud technology) and are able to provide those records readily for inspection by CR staff.
- A majority of licensees have subscribed to use commercially available database services for customer screening and monitoring (including the screening of PEP). Some very small licensees rely on open-source information and information available at government websites.
- Some large licensees maintain very sophisticated IT system to assist them to identify suspicious transactions.

7.41 The law enforcement authorities also collaborate with the CR in the referral of cases where the clients of TCSPs are/may be involved in ML/TF activities for CR's investigation. The JFIU also identified typologies involving the engagement of the TCSP sector. For instance, JFIU observed majority of the TCSP reported STR were relating to adverse news both locally or overseas and majority of the subjects were non-residents with a company incorporated in Hong Kong or maintained with bank accounts in Hong Kong.

7.42 In addition, the AMLO provides that the accounting professional or legal professional who prepares for or carries out for a client a transaction with respect to trust or company service is required to comply with the statutory CDD and record-keeping requirements.

Next Steps

7.43 Hong Kong has strived to improve the transparency of beneficial ownership of Hong Kong companies in line with the FATF standards in the past few years. The implementation of SCR, accompanied with the verification and inspection mechanism by the CR, as well as the implementation of the TCSP licensing regime have further strengthened the defence of our company regime.

7.44 The CR will continue its efforts to ensure the integrity of the Companies Register through vigorous checks, on-site inspections, and enforcement including prosecution and striking off where appropriate. To ensure the integrity of the SCR, the CR will conduct inspection of companies and also take appropriate enforcement actions. For the alleged cases of DPRK using front companies based in Hong Kong to evade sanctions imposed by the UNSC, the CR has been keeping a close watch and has conducted thematic

inspection of companies and connecting parties including TCSPs that are at higher risks of being abused for involvement in prohibited activities. The CR will continue the outreach to TCSPs with a view to enhancing their AML/CFT capacities, including ML/TF risk understanding, CDD, TF/PF TFS sanction screening, etc.

7.45 We believe that the effective implementation of the SCR regime and the TCSP licensing regime, coupled with the statutory AML/CFT requirements for accounting professionals and legal professionals with respect to trust or company service, will continue to mitigate the risk of companies or trusts being abused for ML/TF purposes. Looking ahead, the Government will keep a close watch on the operation of the two regimes and review the framework from time to time.

CHAPTER 8

TERRORIST FINANCING

8.1 The overall TF risk in Hong Kong is discussed in this Chapter. Similar to the 1st HRA, the assessment has taken into account all relevant considerations, including the extent of terrorism threat posed to Hong Kong, TF threat and TF vulnerability in Hong Kong as well as the updates since last HRA. Upon assessment, Hong Kong continued to maintain a medium-low TF risk.

Terrorism Threats

8.2 As at mid-year 2021, Hong Kong had a population of about 7.4 million[202], with over 90% of its population were ethnic Chinese[203]. The ethnic minority population stood at about 653 000, consisting of about 390 000 FDHs[204] and about 14 000 non-refoulement claimants remaining in Hong Kong, with some of them coming from terrorism-afflicted jurisdictions[205]. Being a cultural pot, the world's major religions are all practised in Hong Kong, without any religion dominating[206].

8.3 Hong Kong is an international city with visa-free entry for over 160 countries, over 300 million passengers passing through Hong Kong and over 56 million visitors recorded per year from 2016 to 2019[207&208], before the COVID-19 pandemic.

8.4 External sources terrorist acts continue to pose terrorism threat to Hong Kong. Internally, while the social unrest[209] beginning in 2019 has led to disturbances, the unrest has subsided and law and order have been restored. In particular, the National Security Law enacted on 30 June 2020 has established and improved the legal system and enforcement mechanisms to safeguard national security in Hong Kong. The implementation of the National Security Law has put an end to chaos and effectively restored order in society.

Terrorism threat level

8.5 Hong Kong has an established mechanism to continually monitor the local terrorism threat. Under this mechanism, the threat of a terrorist attack is categorised into three levels, namely "high", "moderate" and "low", taking into account a wide range of factors, including international, regional and local situations, ideologies and motives of international

---

[202] Census and Statistics Department. (2021). *Population*. https://www.censtatd.gov.hk/en/scode150.html

[203] Race Relations Unit, Home Affairs Department. (2018). *The Demographics: Ethnic Groups*. https://www.had.gov.hk/rru/english/info/info_dem.html

[204] The Chief Secretary for Administration's Office. (2019). *Comprehensive support for ethnic minorities*. https://www.news.gov.hk/eng/2019/10/20191027/20191027_093632_116.html

[205] These countries were amongst the top 20 in the Global Terrorism Index 2020. Institute for Economics & Peace. (2021). *Global Terrorism Index 2020*. https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-2.pdf

[206] HKSAR Government. (2018). *Hong Kong Fact Sheets*. https://www.gov.hk/en/about/abouthk/factsheets/docs/religion.pdf

[207] IMMD. (2021). *Annual Reports 2016 to 2019*. https://www.immd.gov.hk/eng/press/press-publications.html

[208] Hong Kong Tourism Board. (2021). *Monthly Report – Visitor Arrival Statistics: Dec 2020*. Retrieved from https://partnernet.hktb.com/filemanager/intranet/pm/VisitorArrivalStatistics/ViS_Stat_E/VisE_2020/Tourism%20Statistics%2012%202020.pdf

[209] Arising from opposition to the proposed legislative amendments to the FOO in 2019.

terrorism, the trend of terrorist activities, the source of the threat, as well as the intention and capability of terrorists. At present, the terrorism threat level of Hong Kong is assessed to be "moderate", meaning there is a possibility of an attack, but there is no specific intelligence suggesting that Hong Kong is likely to be a target. This is commensurate with the overall assessment of "Medium" of terrorism threat using the World Bank Tool.

8.6 The Government is fully committed to combating terrorism through adopting a counter-terrorism policy that focuses on prevention and maintaining comprehensive contingency plans for response to terrorist incidents. Counter-terrorism is also an operational priority of the HKPF, with a four-pronged strategy - prevention, preparedness, response and recovery, adopted. The following paragraphs sets out the major categories of terrorism threats that the LEAs have been monitoring and guarding against.

External terrorism threats

(a) Islamist Terrorism

8.7 There have not been signs of Islamic State of Iraq and the Levant ("ISIL") activity in Hong Kong, though we will remain vigilant and guard against the possibility that online propaganda of ISIL might affect our local residents. Moreover, given the turmoil in Afghanistan after the power transition in 2021, there could be a new wave of refugees in the region. As non-refoulement claimant with possible connections with terrorism might enter Hong Kong, the threat from Islamist terrorism, albeit small, may still post threat to the territory.

(b) Far-right Extremism

8.8 Apart from Islamist Terrorism, far-right extremism has caused rising concern globally with increased numbers of attacks in some developed economics. So far, there is no sign that transnational far-right groups have any presence or substantial influence in Hong Kong. That said, considering the extremism reach that far-right ideologies may have in the cyberspace, the threat from far-right extremism is one of the categories that are closely monitored by LEAs.

Internal terrorism threats

8.9 The social unrest and related violence in 2019 have the potential to induce radical activities locally, and thereby pose threat to Hong Kong. However, with the implementation of the National Security Law, it is observed that such violent activities have largely diminished, and the threats arising from such activities have correspondingly been reduced. That being said, our LEAs will remain vigilant and keep a close watch over any intelligence or trendon possible terrorism threats.

TF Threats

8.10 Hong Kong is an international financial centre with an open and advanced financial system. The threat of financing terrorism abroad (including for foreign terrorist fighters) remains given our cultural and economic connectedness between certain segments of the community and regions affected by terrorism.

8.11 In assessing the TF threats faced by Hong Kong, reference has been made to the studies and reports published by the FATF, in particular on the modus operandi of

terrorists (e.g. for raising funds, Islamist terrorist groups), which often includes sophisticated and systematic ways such as extortion, oil selling, imposing tax and illicit trade in areas controlled by the groups; contribution from non-profit organisations ("NPOs"); donation from individual supporters and even investment in legal banking systems. Funds are moved through cash couriers, hawala, money or value transfer services, bank transfers and even VAs. For far-right extremist groups, they encompass a wide range of actors with scales and levels varied, from individuals to small organizations and sometimes transnational movements. Sources of funding of these groups ranged from non-illegitimate sources such as crowdfunding, donations, membership fees and commercial activities, to illegal sources such as commission of proceeds of crime. Internationally, funds are also observed to be moved through cash, money or value transfer services, VA and the use of professional financial management services. Checking the channels of illicit funding identified by the FATF, it is noted that the actual TF risks faced by Hong Kong and in relation to external threats are limited. This is corroborated by the limited number of reporting received and the detailed analysis has in the past utilised on the intelligence gathered (see paragraphs 8.13-8.14 below).

8.12 As regards the use of technology for TF purposes, there was indication that local radicals use social media platforms, VAs or crowdfunding to raise funds. However, with the repeated warnings issued by the LEAs, the relevant fund-raising activities have largely disappeared from the local scene. For other emerging technology such as online payment systems, prepaid cards and other electronic payment methods, there are no signs indicating their involvement in suspected TF cases. Having said that, LEAs will remain vigilant in monitoring the situation.

TF-related STRs, investigations and MLA requests

8.13 STR is a very important source of information and intelligence for CFT and one of the indicators in assessment TF threat. TF-related STRs received were mainly concerned with the suspicious movement of funds in bank accounts. Among the 106 TF-related STRs received between 2016 and 2020, around one-third are false-positive cases involving (i) false-positive name or alias hits of known terrorists or terrorist associates on terrorist lists which, upon investigation were found to be a false alarm, or (ii) financial transactions related to entities in high-risk jurisdictions which were found to have insufficient evidence to substantiate the TF linkage. For the remaining two-third of TF-related STRs, subsequent investigation failed to substantiate the funds have any linkage with any terrorists or terrorist acts, or with any terrorist groups, except for a limited number of STRs which might have been related to illegal activities of local radicals. In addition, there is no TF case that requires the invoking of freezing power, and no cases being warranting prosecution with TF offences so far.

8.14 Between 2016 and 2020, one MLA request relating to TF was received. Apart from MLA, the number of other intelligence exchanges and information requests, including via the platform of Egmont Group, remained at a low level, and were mainly related to factual information exchange and requests.

Overall TF threat level

8.15 At the time of the preparation of this report, there is no confirmed TF prosecution or conviction case in Hong Kong. Investigations and intelligence suggested that there is no substantial evidence of international TF activities in Hong Kong. As Hong Kong is an

international financial, trade and transportation hub, it is inevitable that Hong Kong will continue face exposure to external TF threat. On the other hand, it is observed that there was possible threat, though limited, posed by local radicals and indication of associated financing activities. With the continued implementation of the National Security Law, the threat should further diminish. The TF threat is therefore assessed as medium low in the 2nd HRA.

TF Vulnerabilities

8.16 Hong Kong has adopted a solid defense mechanism, with strong strength of controls to detect and counter TF in different aspects including legislation, intelligence, resources, cooperation, commitment and awareness. Several major updates are described below.

Legislation

(a) UNATMO and UNSO

8.17 Hong Kong has a sound legal framework which effectively criminalises TF through the UNATMO and the UNSO. Under the law, both natural persons and legal entities can be prosecuted. In addition, the UNATMO provides for the freezing of terrorist property and prohibits persons and entities within Hong Kong, and all Hong Kong permanent residents and legal entities incorporated under the law of Hong Kong from making available property or financial services to, or for the benefit of, terrorists or terrorist associates. The amendment of UNATMO in 2018 further enhances the prohibition on dealing with terrorist property and criminalises the financing of travel of foreign fighters.

(b) AMLO, CO and R32 Ordinance

8.18 AMLO came into effect in March 2018 to extend the statutory CDD and record-keeping requirements to legal professionals, accounting professionals, TCSPs and estate agents. Meanwhile, the amended CO and the new R32 Ordinance introduced in 2018 have further safeguarded against TF by requiring companies to keep record of beneficial ownership and enhancing the declaration and disclosure regime for the cross-boundary movement of physical CBNIs.

(c) The National Security Law

8.19 The National Security Law was promulgated for implementation on 30 June 2020 to, inter alia, prevent, suppress and impose punishment for the offence of organisation and perpetration of terrorist activities. Moreover, Schedule 3 to the Implementation Rules for Article 43 of the National Security Law provides that if the Secretary for Security has reasonable grounds to suspect that any property is property related to an offence endangering national security (including that concerning terrorist activities), he may direct that a person must not deal with the property, thereby freezing such property.

Dual alert system

8.20 To facilitate the implementation of UNSC sanctions, the most updated list of Persons and Entities subject to TFS under the UNAMTO and UNSO are published by Gazette notice and/or on the website of CEDB. Moreover, since May 2018, SB has introduced an alert dual track mechanism which runs parallel to the existing use of Gazette

Extraordinary, for the monitoring of TFS related to the 1267/1989/2253[210] and 1988[211] list at the start of every working day. Reporting entities are notified through the SB, the FSTB and the relevant supervisors within one working day via their relevant regulatory authority. Such notification triggers an obligation to stop making available any property of any person or entity known or suspected to be on the updated list or deal with property of specified terrorists or terrorist associates, and to file an STR to the JFIU. Regulatory authorities are required to freeze property at the earlier of the two events: (i) publishing of the designation in Gazette or (ii) a person becomes aware he is dealing with property relating to a UNSC-designated person or entity, including but not limited to through the alert mechanism.

8.21 Since the introduction of the dual track system, 39 alerts have been issued according to the 39 UNSC designations, and all were published within one working day.

Collaboration

8.22 Combating ML/TF is a common goal for all LEAs. Our LEAs have maintained close collaboration with each other in investigation, intelligence exchange and analysis. Priority is given to all TF-related STRs and other TF-related information received, with all of them disseminated to the designated units for immediate investigation. Every investigation, whether the allegation is substantiated or otherwise, has been properly recorded in the HKPF database according to the protocol and the intelligence learning has been fed back into the relevant units.

8.23 In order to enhance the collaboration between LEAs, the Inter-departmental Counter-terrorism Unit ("ICTU"), a cross-departmental platform was set up by the SB in April 2018 to facilitate co-operation and co-ordination on counter-terrorism. It is aimed to promote intelligence sharing and focuses investigative efforts on important cases requiring joint efforts of local LEAs. All relevant law enforcement and intelligence agencies, namely the HKPF, IMMD, the C&ED, the Correctional Services Department, the Fire Services Department and the Government Flying Service, are included. The establishment of ICTU should have enhanced the counter-terrorism and CFT strategies, action plans, cross-departmental co-ordination, intelligence gathering, training and public education.

8.24 Collaboration with other jurisdictions are also important. From time to time, the HKPF and the DoJ maintain close liaison with counterparts in other jurisdictions and provide assistance in intelligence sharing, investigation and other legal matters. Proper mechanism for collaboration is in place. The HKPF has also intelligence exchange channels specifically designated for TF.

Capacity building

8.25 Our robust AML/CFT regime is also backed by operational excellence and effective executional arms. To enhance our capacities in combating ML/TF, a new strategic bureau, i.e. the FIIB has been established under the HKPF since June 2021, specialising in both financial investigation and intelligence gathering with additional resources. Also, the HKPF is developing a FDAP to harness the opportunities brought by advanced technologies, with a view to improving the efficiency and effectiveness in intelligence analysis and case investigation. (Details have been provided in Chapter 3.)

[210] https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list
[211] https://www.un.org/securitycouncil/sanctions/1988/materials

8.26 For private sector, regulatory authorities, self-regulatory bodies and professional groups have stepped up efforts in raising the awareness of reporting entities on TF risks and the obligation in relation to TFS. (Details have been provided in Chapter 5 and 6.)

Vulnerabilities associated with non-profit organisation

8.27 Self-funding from legitimate sources for financing terrorist activities is a growing issue for TF internationally. In Hong Kong, there could be concerns that banks, SVF licensees and MSOs are at risk, as foreign workers remit monies to their homelands. The financial regulators continue to monitor compliance by these sectors with the AML/CFT obligations, and to promote awareness of TF among FIs, which already use multiple sources such as terrorist lists issued by the United Nations, specific AML/CFT databases, open sources and transaction monitoring to identify suspicious transactions.

8.28 As recognised in the 4th round FATF ME, NPOs in Hong Kong may exist in various forms including organisations subvented by the Social Welfare Department, companies, trusts, charitable bodies with or without tax-exempt status, statutory bodies , societies registered under the Societies Ordinance , and educational institutes. NPOs are subject to the regulatory and governance requirements under various Ordinances depending on their activities, funding sources, legal structures etc. The regulatory regimes are not mutually exclusive. Where public funding is involved, there is stringent control (e.g. submission of regular reports or audited statements by NPOs to regulators) to ensure transparency and accountability. In relation to those charities whose tax exemption status are recognised, the IRD conducts periodic reviews to ascertain whether they continue to be eligible for tax exemption status under the IRO. The Government has published CFT-specific guidelines for charities and been drawing NPOs' attention to the designated names of terrorists or terrorist associates. LEAs have the powers to obtain information from Government departments concerned if necessary for counter-terrorism or CFT purposes.

8.29 There has been no report of NPOs or charities in Hong Kong being misused for TF purposes, or found to sympathise with or condone terrorism, or linked to known or suspected terrorist groups. There has been no intelligence or evidence from STRs, investigation suggesting that NPOs in Hong Kong are being exploited for raising or moving funds for TF. On this basis, there is no apparent TF threat identified for the NPO sector in Hong Kong.

8.30 The inherent TF vulnerability of NPOs in Hong Kong is low, having regard to the current regulatory regimes and governance, the landscape of terrorism and TF threats in Hong Kong as well as the inward focus of the majority of NPOs in Hong Kong. With reference to international TF typologies and the local context, organisations operating and raising funds in Hong Kong for the purpose of supporting humanitarian services in conflict zones could be susceptible to TF risk. Nevertheless, these NPOs are commonly part of the international charities network to which the funds raised are disbursed, and have to a large extent put in place internal due diligence controls on their own. Donations of these NPOs are mainly received through traceable means such as bank transfer, credit card payment and direct debit. These NPOs have internal guidelines in conducting risk assessment in respect of donations from anonymous donors. Banks are also aware of the potential TF risks associated with the NPO sector and monitor closely for funding or transactional

patterns which may give rise to higher risks and the need for enhanced monitoring.

8.31 SB regularly conducts assessment to review risks of NPOs in Hong Kong being misused for TF purpose. SB will continue to regularly assess the landscape of NPOs in Hong Kong, including whether there are any changes to the nature and number of higher-risk NPOs, as well as to pay close attention to whether there are effective controls and policies in place with NPOs to contain TF risks. SB will also keep in view whether there is a need to update the "Advisory Guideline on Preventing the Misuse of Charities for Terrorist Financing" in future. Furthermore, regular liaison with high-risk NPOs will be maintained by informing these NPOs of the latest updates of the United Nations Terrorist List and Sanction List.

8.32 Considering the above, vulnerability associated to NPOs is assessed to remain as low.

Overall TF vulnerabilities

8.33 The proper legislative and institutional framework to counter TF activities is in place and which is commensurate with the threat identified. Effort has been made to enhance the CFT framework and the city's capacity in combating TF. Hence, the overall TF vulnerability remained to be assessed as medium-low.

TF Risks

8.34 Hong Kong has a medium-low TF risk, with threat and vulnerability both rated as medium-low.

Next Steps

8.35 While Hong Kong faces a relatively low TF risk, the situation must be closely monitored, with current preventive measures kept under constant review. For operational and intelligence aspects, additional manpower resources have been allocated to enhance the capacities in combating TF and the effectiveness of the coordination among LEAs. Moreover, a new FDAP, supported by advanced technologies including machine learning and artificial intelligence, is being developed by HKPF with a view to improving the efficiency and effectiveness in ML/TF intelligence analysis and case investigation.

8.36 Under the influence of global and the local terrorism threat, the Government will continue to take five-pronged enhancement approaches to combat terrorism including investigation, intelligence and training, protection of critical infrastructures, law reform and public education and awareness. Continuous effort will be made to ensure the responsiveness and resilience of the CFT regime.

CHAPTER 9

PROLIFERATION FINANCING

9.1 This Chapter contains the first assessment of PF risks in Hong Kong. In October 2020, the FATF revised Recommendation 1 ("R.1") and its Interpretive Note to require countries and private sector entities to identify, assess, understand and mitigate their PF risks. In the context of R.1, PF risk refers strictly and only to the potential breach, non-implementation or evasion of the TFS obligations referred to in Recommendation 7.

9.2 This assessment has taken into account inter-agency inputs concerning the Government, regulators as well as the private sector. It sets out the key PF threats faced by Hong Kong today, as well as the specific vulnerabilities in relevant sectors of Hong Kong. This assessment does not only help the Government in formulating and enhancing its counter-proliferation strategy, but also informs the private sector of the overall PF risk of Hong Kong and facilitates their implementation of measures to mitigate risks posed by possible PF activities. The overall PF risk of Hong Kong is assessed to be medium-low, with PF threat and vulnerability level both assessed to be medium-low.

Hong Kong's Counter-Proliferation Regime

9.3 To safeguard Hong Kong from PF risks, we have put in place a robust counter-proliferation regime with core elements that include a comprehensive legal framework and strategic trade control system, effective coordination and cooperation among policy bureaux, departments, LEAs and regulators/supervisors, as well as a well-implemented defence system by the private sector.

Comprehensive legal framework

9.4 In Hong Kong, sanctions imposed by the UNSC including TFS against proliferation of WMD are primarily implemented by way of the DPRK Regulation and the Iran Regulation, complemented by the WMDO and the CWCO, and assisted by the strategic trade control regime under the IEO.

DPRK

9.5 To implement TFS against DPRK in Hong Kong, section 8 of the DPRK Regulation prohibits all natural persons within Hong Kong, all Hong Kong permanent residents acting outside Hong Kong and legal persons incorporated or constituted under the law of Hong Kong from making available funds or other financial assets or economic resources to, or for the benefit of, "relevant persons" or "relevant entities", or dealing with any funds, other financial assets or economic resources belonging to, or wholly or jointly owned or controlled by such persons or entities. "Relevant persons" and "relevant entities" under the DPRK Regulation include all individuals and entities on the sanctions lists maintained by the UNSC or its Committee established under Resolution 1718 ("the DPRK Committee"), as well as individuals and entities acting on behalf of, at the direction, and owned or controlled by UNSC-sanctioned individuals/entities. Whenever there are updates to the UNSC's sanctions lists, corresponding changes are made to the lists maintained by Hong Kong under the DPRK Regulation, and the updated lists are published as soon as possible within one working day. As at end 2021, TFS have been imposed under the DPRK

Regulation on all 80 individuals and 75 entities designated by the UNSC or the DPRK Committee.

9.6 In respect of imposing asset freeze on designated ships, section 10A(2D) of the DPRK Regulation prohibits any persons from dealing with "relevant ships", which include ships designated by the UNSC or the DPRK Committee for the purposes of paragraph 8(d) of UNSCR 1718, paragraph 12 of UNSCR 2270 and paragraph 12 of UNSCR 2321. The lists of "relevant ships" maintained by Hong Kong are updated and published, following the updates by the UNSC or the DPRK Committee, as soon as possible within one working day. As at end 2021, asset freeze has been imposed on all 37 ships designated by the UNSC or the DPRK Committee.

Iran

9.7 Similar to the regime against DPRK, section 9 of the Iran Regulation implements TFS in respect of Iran by prohibiting both natural and legal persons from making available funds or other financial assets or economic resources to, or for the benefit of "relevant persons" or "relevant entities", or dealing with any funds, other financial assets or economic resources belonging to, or wholly or jointly owned or controlled by such persons or entities. "Relevant persons" and "relevant entities" under the Iran Regulation include all individuals and entities on the sanctions lists maintained by the UNSC or its Committee established under Resolution 1737 ("the Iran Committee"), as well as individuals and entities acting on behalf of, at the direction of, and owned or controlled by UNSC-sanctioned individuals/entities. Whenever there are updates to the UNSC's sanctions lists, corresponding changes are made to the lists maintained by Hong Kong under the Iran Regulation, and the updated lists are published as soon as possible within one working day. As at end 2021, TFS have been imposed on all 23 individuals and 61 entities designed by the UNSC or the Iran Committee.

Alert mechanism

9.8 To complement the timely implementation of TFS, similar to TF-TFS, the Government has implemented an alert mechanism such that FI and DNFBPs are alerted by the regulators/supervisors of updates made by the CEDB to the sanctions lists (including listing or de-listing) as soon as possible within one working day. FIs and DNFBPs are well informed of the actions that should be taken regarding sanctions imposed by the UNSC (see paragraphs 9.12 to 9.14).

Strategic trade control system

9.9 Besides the UNSO as a dedicated piece of legislation implementing UNSC sanctions in Hong Kong, Hong Kong also implements a law-based and transparent strategic trade control system backed by stringent licensing controls by the TID, vigorous enforcement by the C&ED, and close international cooperation. Strategic commodities under the strategic trade control system, as stipulated under the IEO and its subsidiary legislations, include munitions items, chemical and biological weapons and their precursors, nuclear materials and equipment, and dual-use goods that are capable to be developed into WMD.

9.10 Under the strategic trade control system, import, export, and transhipment of strategic commodities are subject to licensing control. On top of that, transit of the "more

sensitive" items amongst the list of strategic commodities, such as arms and munitions, ground vehicles, chemical or toxic agents, etc., also requires import/export licences. The control system also imposes end-use control on products that can be used in connection with the development of WMD. Persons who import or export strategic commodities without licence commit an offence and are liable to imprisonment for seven years and a fine of unlimited amount. These stringent controls prevent Hong Kong from being used as a conduit for the proliferation of WMD.

Effective coordination and cooperation

9.11 The CEDB, as the leading policy bureau on implementation of UNSC sanctions including PF-TFS, convenes an inter-agency platform to share intelligence, discuss typologies, trends and cases, and coordinate government-wide actions and responses on proliferation. Inter-agency meetings are attended by the FSTB, the SB, the HKPF, the C&ED, the CR, the MD, the TID and the HKMA on a regular basis, and other co-opted members where needed. Follow-up actions, such as pursuing further investigation and enforcement, have been taken following the meetings, and alerts have been issued to the relevant trades to remind them of the need to comply with UNSC sanctions. All relevant parties maintain close liaison with one another for exchanging intelligence and other information for investigations and follow-up actions in relation to PF.

Investigation and supervision

9.12 All intelligence and reports on alleged/potential sanctions evasions, including STRs, are thoroughly examined by LEAs using a multi-disciplinary approach. On receipt of intelligence/reports, the HKPF coordinates and conducts comprehensive checks on the subjects from various information sources, with a view to probing into all relevant parties and entities exhaustively. In respect of information relating to bank accounts, the HKMA shares details provided by overseas authorities, LEAs or obtained from the media or other open sources of all alleged persons/entities with all AIs and require them to identify any business relationship maintained with those persons/entities, and to provide all necessary information in terms of bank accounts and transactions through filing of STRs to the JFIU. With close coordination among competent authorities, thorough investigations have been conducted into all suspected PF cases, with no funds, assets and economic resources associated with UNSC-designated persons or entities found in Hong Kong.

Box 9.1 - Case example

A vessel, registered in Jurisdiction X, was alleged to have been involved in DPRK-related activities prohibited by the UNSC (namely delivering coal from DPRK). It has been placed on Hong Kong's watchlist since 2017. In early 2018, the vessel sought to enter Hong Kong waters for cargo operation. The Hong Kong authorities immediately contacted the shipping agent and gathered that the vessel was carrying a kind of coal product, intended to be discharged to another vessel in Hong Kong. Although the documents submitted by the shipping agent indicated that the coal product on the vessel was produced in Jurisdiction Y and not DPRK, Hong Kong authorities considered the vessel highly suspicious. In accordance with UNSC Resolution 2270 which requires all Member States to prohibit the entry into their ports of any vessel if the Member State has information that provides reasonable grounds to believe the vessel contains cargo the supply, sale, transfer or export of which is prohibited, Hong Kong authorities denied entry of the vessel

into Hong Kong waters.

The case demonstrates that while potential sanctions evaders may seek to make use of Hong Kong, a busy port located not far from proliferation-sanctioned states (particularly DPRK), for cargo operations which might be related to UNSC-prohibited activities, Hong Kong stays highly vigilant against any potential evasion activities and takes prompt actions to deny the entry of suspicious vessels through effective coordination and cooperation amongst Hong Kong authorities.

Well-implemented defence system by the private sector

9.13 The Government recognises that a well informed and responsive private sector is essential in countering PF. FIs and DNFBPs are well aware of their obligations to implement TFS in respect of designated persons and entities, and have put in place a defence system to counter PF.

9.14 Under the alert mechanism, upon notification by regulators/supervisors of updates to the sanctions list, FIs and DNFBPs screen their client database for potential matches. They are obliged under the OSCO to file an STR if they know or suspect that a property is intended to be used in connection with the provision of services that will or may assist the development, production, acquisition or stockpiling of WMD.

9.15 In addition, in the process of conducting CDD as required under the AMLO, FIs and DNFBPs make reference to reliable sources, including the sanctions lists promulgated on the Gazette, the CEDB's website, and/or internal screening systems to screen for designated persons or entities. Where there is a potential match, FIs and DNFBPs will halt any business relationship and any transaction and file STRs, thereby preventing execution of proliferation-related operations or financial transactions. FIs and DNFBPs are well aware of their obligations to implement TFS in respect of designated persons and entities, and have put in place screening systems to this end. On-site inspections by regulators have confirmed a high level of compliance in this regard. So far, no potential match in respect of DPRK or Iran has been reported.

9.16 For capacity building, the Government organises AML seminars annually for individual sectors, covering the topic of PF among others. In addition, in view of the FATF's revisions of R.1 in October 2020 introducing a new requirement to conduct PF risk assessment, the CEDB promptly organised a webinar on PF Risk Assessment and Mitigation in August 2021 for the private sector to facilitate their understanding and compliance of the latest requirements following the adoption of the relevant Guidance by FATF in June 2021. The webinar was attended by practitioners from the banking, SVF, securities and futures and insurance sectors, as well as MSOs and licensed money lenders.

Proliferation Financing Threats

9.17 According to the FATF Guidance on PF Risk Assessment and Mitigation, PF threat refers to "designated persons and entities that have previously caused or with the potential to evade, breach or exploit a failure to implement PF-TFS", and "may also be caused by those persons or entities acting for or on behalf of designated persons or entities".

9.18 Hong Kong has been closely monitoring the lists of persons and entities designated by the UNSC or its relevant Committees. So far, no Hong Kong residents have been designated. Four companies formerly registered in Hong Kong are on the UNSC's sanctions list in respect of DPRK, but they have all been dissolved and struck off Hong Kong's Companies Register.

9.19 Noting that PF threats may be posed by not only designated persons/entities themselves, but also the international network they create to disguise their activities, Hong Kong has been keeping a close watch on reports published by the UNSC Panel of Experts, as well as other sources such as intelligence from other jurisdictions and media reports, to identify traits of possible involvement of Hong Kong residents or companies incorporated in Hong Kong in the circuitous financing routes relating to proliferation. Vigilant investigations by our LEAs, as discussed in paragraph 9.12 above, found no PF-related funds, assets and economic resources in Hong Kong.

9.20 Although there is an absence of substantiated PF cases in Hong Kong, this assessment looks into how designated persons and entities, or those acting on their behalf (collectively known as "proliferation actors"), might make use of diverse and constantly evolving methods to disguise their attempts to breach UNSC sanctions.

Procurement, export and transshipment/transit

9.21 As Hong Kong is not a major manufacturer, intermediary nor supplier of arms, nuclear or ballistic missile-related material, the threat of direct procurement of such items from Hong Kong is minimal. Nonetheless, given Hong Kong's geographical location and status as one of the most popular and busiest entrepots in the world, proliferation actors might find Hong Kong a convenient transshipment/transit point for the above prohibited items. To guard against such activities, Hong Kong has put in place a robust strategic trade control system covering import, export, transit and transhipment of strategic commodities (see paragraphs 9.9 and 9.10). On the whole, the threat posed by proliferation actors procuring, export or transshipping/transiting prohibited items through Hong Kong is medium-low.

Use of front or shell companies to hide PF activities

9.22 As analysed in Chapters 4 and 7, Hong Kong is known for its efficient company formation process. It is possible that front companies are established or used for PF purpose under the disguise of legitimate business activities, as part of a layering process to mask the proliferation actors. Also, corporate bank accounts may be set up, locally or off shore, in the name of the front companies to hide the identity of proliferation actors. The threat posed by the abuse of Hong Kong's company formation regime through the use of front companies is medium in Hong Kong.

Role of intermediaries

9.23 As pointed out in the FATF Guidance on PF, TCSPs and other professionals may be involved in creating corporate entities that proliferation actors use to obscure the links between a financial transaction and a designated person or entity. As discussed in Chapter 6, a new licensing regime for TCSPs has been implemented in Hong Kong since 2018 and is vigilantly enforced. Also, supervision and outreach to other professionals have been stepped up. In this regard, the threat posed by the use of TCSPs and other

professionals in Hong Kong in sanctions evasion is assessed to be medium-low.

Proliferation-related investigations

9.24 Between 2016 and 2020, an average of 53 proliferation-related STRs were received each year. Together with other intelligence and reports on alleged/potential sanctions evasions, a yearly average of around 90 investigations were conducted by LEAs. All cases have been vigilantly investigated, and none have been substantiated. In most cases, FIs reported to JFIU that a company might have businesses with Iran / DPRK based on adverse news or World check results, etc. However, LEAs' analysis into the transaction records did not reveal anything involving trading with DPRK/Iran or PF activities.

Overall PF threat level

9.25 Designations by the UNSC and its relevant Committees as at end-2021 do not include any Hong Kong residents or companies incorporated in Hong Kong still in operation. At the same time, robust investigations by LEAs have found no evidence of PF activities in Hong Kong. Nevertheless, as Hong Kong is an international financial, trade and transportation hub with geographical proximity to DPRK/Iran, Hong Kong may be exposed to external PF threat. On the whole, the PF threat level is assessed as medium-low.

PF Vulnerabilities

9.26 According to the FATF Guidance on PF Risk Assessment and Mitigation, PF vulnerability refers to "matters that can be exploited by the threat or that may support or facilitate the breach, non-implementation or evasion of PF-TFS". As one of the world's leading international financial centres, Hong Kong is a prime location for financial and other professional services and home to global FIs and businesses, which capitalise on the city's openness, extensive networks with the rest of the world, free flow of capital, ease of company formation, full range of financial products, and large pool of financial talents and professionals. Strategically located in the heart of Asia, Hong Kong is also a transportation hub with busy cargo activities. Hong Kong's business friendliness could also be a vulnerability if exploited by proliferation actors, as discussed below.

Financial sector

9.27 Being an important player in the global financial system, Hong Kong's banking and payment sectors may inadvertently facilitate proliferation actors' access to financial services if players in the sectors, such as banks, SVF licensees and MSOs, do not put in place sufficient compliance controls. Therefore, regulators in Hong Kong attach great importance to engaging with the relevant sectors to prevent any PF vulnerability from being exploited.

9.28 The HKMA continues to see evidence of a sound understanding amongst banks in Hong Kong of their TFS obligations against DPRK and Iran. Banks generally have robust CDD processes to obtain quality data on beneficial owners and connected parties, and effective systems for screening against relevant UNSC designations. Following the thematic examinations on banks' sanctions screening systems and publication of a circular on "Feedback from Recent Thematic Review of AIs' Sanctions Screening" in 2018, the HKMA collected information from all banks on their individual action plans through a questionnaire and based on the questionnaire results, further conducted examinations on some banks on their understanding of TF/PF risks and oversight over screening process in end 2018. The

HKMA used the analysis of such information to target further supervision, using an external Regtech firm to facilitate testing of AIs' sanctions screening systems in a number of examinations, work of which is still ongoing. Case studies of banks adopting Regtech to enhance efficiency of sanctions screening systems have been shared with the industry to enhance the collective ability of the banking sector to meet their TFS obligations related to proliferation.

9.29 As for SVF licensees, they are predominantly used for domestic payments for goods and services. Based on data obtained from SVF licensees, there exists no known indicator in relation to a customer or transaction that may suggest suspicion of PF. While the cross-border remittance function might be more vulnerable to PF, no remittance corridor with DPRK and Iran is available in the SVF sector so the risks of SVFs being misused for PF purposes are low. In addition, guidance and lessons learned from the banking sector has been shared with SVF licensees who generally have a good understanding of the legal obligations to ensure compliance with resolutions of the UNSC, and have imposed restrictions against DPRK and Iran. In particular, SVF licensees are required to conduct sanctions screening on both the customers (except for those using products with minimal stored value where CDD is not required) and remittance transactions.

9.30 The implementation of CPF control has greatly improved within the MSO sector in the past few years. With a robust licensing and supervisory regime overseen by the C&ED, MSOs are currently required to demonstrate their capabilities in PF screening and monitoring when they submit licence applications. To ensure compliance of relevant TFS obligations by MSOs, the C&ED has incorporated PF risk understanding and PF-TFS screening as one of the key elements for the department's on-site inspections of MSOs. Outreach activities on PF have particularly enhanced MSOs' awareness of their statutory obligations to file STRs and to freeze PF-related assets.

9.31 For the securities sector which is comparatively less exposed to PF, LCs generally have a good understanding of their obligations relating to PF, and apply appropriate preventive measures including PF-TFS screening controls. The SFC also updates LCs on the latest regulatory developments and risk issues. For instance, the SFC issued an advisory circular in July 2021 to inform LCs the FATF's adoption of a guidance on PF risk assessment and mitigation.

9.32 While the PF exposure of the money lender sector remains to be relatively low, money lenders are generally well aware of their obligations in relation to PF. The RML conducts regular AML/CFT seminars for money lenders to promote their understanding and awareness of PF-TFS obligations. The AML/CFT Guideline issued by the RML to money lenders provides guidance on the compliance with the requirements relating to financial sanctions and PF. Onsite inspections which cover the area of PF are conducted by the RML to ensure compliance of money lenders with relevant requirements.

9.33 For the insurance sector, the IA keeps the insurance industry abreast of the latest developments relating to PF by issuing circulars and promptly circulates the UNSC designations to the regulated entities for appropriate action. Based on the IA's onsite inspection observations, insurers in general are aware of the requirements in relation to PF-TFS, and have measures in place to ensure compliance. They screen customers and beneficial owners before the establishment of a business relationship, during the course of

the business relationship as well as at the time of payout. Beneficiaries are also screened at the time of filing death claims.

Maritime sector

9.34 Hong Kong is an international transportation hub with a busy port; suspicious ships involved in UNSC-prohibited activities might seek to pass through Hong Kong or carry out cargo operation in Hong Kong. We have therefore compiled a comprehensive watchlist covering not only ships designated by the UNSC or its relevant Committees, but also those alleged in intelligence or other reports to be involved in prohibited activities. The MD is highly alert to requests from ships on the watchlist which seek to enter Hong Kong waters, and works together with the CEDB and LEAs (particularly the C&ED) in handling such requests. As seen from the case example above, Hong Kong has denied entry of suspicious ships into Hong Kong waters. In addition, to heighten the shipping industry's awareness, the MD shares information with the industry (including ship owners and ship management companies) on UNSC sanctions as well as deceptive practices for ships to evade sanctions or disguise their identities.

TCSP sector

9.35 Proliferation actors seeking to obscure their identities by setting up front companies may be attracted by Hong Kong's efficient company formation, and TCSPs could be vulnerable to abuse during the process. To address this vulnerability, the CR will not grant or renew a TCSP licence if the relevant person(s) of the applicant / licensee are not fit and proper to carry on a trust or company service business (e.g. he or she is found to be associated with PF or sanctions evasion). To ensure compliance of TFS by TCSP licensees, the CR has taken precautionary measures to require applicants for TCSP licence to declare that they do not have any business relationship with any UNSC-designated person or entity which are subject to TFS. In the notification for grant of TCSP licence, TCSP licensees are again reminded, among other things, that they should not have any business relationship with the aforesaid persons or entities.

9.36 The AML/CFT Guideline issued by the Registrar of Companies for TCSPs provides guidance on the compliance with the requirements relating to TFS and PF. Onsite inspections which cover the CPF aspect are conducted to ensure compliance of relevant requirements by TCSPs, and appropriate enforcement action will be taken for non-compliance by the licensees. The CR has also issued circular emails to remind TCSP licensees of their obligations to comply with the statutory requirements on financial sanctions, including PF-TFS. The TCSP licensees and relevant associations are informed of the publication of statement / relevant guidance issued by the FATF. The CR will continue with its various measures to monitor compliance of TCSP licensees with the relevant regulations and legislation on PF.

9.37 The CR conducts regular on-site inspections to ensure that companies are not defunct and comply with the statutory requirements under the CO, including the keeping of registers. If companies are found not to be in operation or carrying on business, the CR will strike them off the Companies Register.

9.38 A new regime to disclose the beneficial ownership of companies has been introduced since March 2018. Companies are required to ascertain and maintain up-to-date beneficial ownership information by way of keeping a SCR. The SCR is open for inspection

by law enforcement officers on demand (Details are in Chapter 7).

Professional services sector

9.39 Various vulnerabilities may emerge from Hong Kong's role as an international financial centre, including through the provision of professional services in relation to potential efforts to evade UNSC sanctions. Intelligence and typology reports indicate that PF-related cases in many jurisdictions have very often involved the use of the front or shell companies, with complex corporate and ownership structures sharing similar characteristics. This may involve certain professional services, such as legal or accounting services. Meanwhile, the risk for sanctioned parties to access other DNFBPs (such as estate agents and DPMS) cannot be dismissed.

9.40 Despite these vulnerabilities, it is observed further to the 4th round of ME that there is an improved understanding of DNFBPs regarding their CPF obligations and implementation of CPF measures. Having recognised the sectoral threats and vulnerabilities (details have been provided in Chapter 6), the DNFBPs' supervisors have stepped up efforts in enhancing CPF awareness of respective sectors. With continued educational efforts, understanding among legal professionals, accounting professionals, estate agents and DPMS of the legal obligations to ensure compliance with the resolutions of the UNSC, as well as the legislation in Hong Kong combating PF, including the UNSO and the WMDO, etc., have been improving over time. Concrete efforts by various sectors are set out below –

(a) Legal sector: To enhance members' awareness of PF, the LSHK featured a dedicated section on PF at its website and highlighted the topic in its AML/CFT seminars for members. It is also a common practice for law firms to establish screening mechanism to screen their clients and any beneficial owners of their clients against the latest sanctions lists.

(b) Accounting sector: The HKICPA's website contains a designated page that provides the latest PF-related information, including timely updates of sanctions lists, as well as frequently-asked-questions on compliance, which provide practical guidance to members so as to enhance the awareness of members on PF. Meanwhile, accounting professionals must conduct adequate CDD and record keeping and, under the AML/CFT Guidelines, are expected to perform sanctions screening of clients before the establishment of a business relationship, regardless of the services they will be offering, and to perform ongoing screening regularly thereafter, to ensure that clients and/or their beneficial owners are not included in the UNSC's sanctions lists.

(c) Estate agent sector: To enhance licensees' awareness of PF, the EAA website promulgates the United Nations terrorists and sanctions lists, as well as FATF's public statements on high-risk jurisdictions, in a timely manner. Estate agents inherently handle limited funds, and in the course of complying with the mandatory CDD and record-keeping requirements, they would also be able to identify clients who are affiliated with sanctioned jurisdictions.

(d) DPMS sector: The Government provides timely updates to the trade associations on the UNSC's sanctions lists, as well as FATF's public statements on high-risk jurisdictions to enhance the awareness of PF of the DPMS sector. To draw the sector's

attention to the legal requirements under the relevant United Nations Sanction Regulations and enhance its awareness on PF, the Government issued "Supplement to the Anti-Money Laundering and Counter-Terrorist Financing Guideline for Dealers in Precious Metals and Stones" in 2020 to provide DPMS specific and targeted information in relation to PF. The PF topic was also highlighted in the AML/CFT seminars.

Use of VAs

9.41 There has been an increasing global trend in recent years of sanctions actors utilising VAs and other new technologies to evade international sanctions regimes given the anonymous nature of VAs. There is no audit trail for activities involving actors connected to DPRK and Iran. The use of VAs as both a tool for fund raising as well as fund movement may be vulnerable to proliferating actors seeking to evade the traditional financial system.

9.42 It is expected that with the implementation of the licensing regime for VASPs under the amended AMLO, the vulnerability of the use of VAs in facilitating PF activities can be addressed.

Overall PF vulnerability

9.43 Despite the factors contributing to Hong Kong's PF vulnerability as discussed above, Hong Kong has a robust counter-proliferation regime that includes comprehensive legislation and a proper institutional framework involving government agencies, regulators/supervisors and the private sector to counter PF activities. Hence, the overall PF vulnerability is assessed as medium-low.

PF Risks

9.44 Hong Kong has a medium-low PF risk, with threat and vulnerability both rated as medium-low.

Next Steps

9.45 To better focus the on-going CPF efforts of all parties concerned, the Government has drawn up the counter-proliferation strategy, with (a) Prevention; (b) Alert; (c) Coordination; and (d) Enforcement (i.e. "PACE") as the major elements –

(a) **Prevention:** Maintaining a robust legal regime to fully implement sanctions decided by the UNSC against DPRK and Iran to counter proliferation of WMD; and heightening the awareness, through training and outreach, of all relevant government bureaux/departments (including LEAs), regulators, DNFBP supervisors, as well as FIs and DNFBPs in respect of the UNSC sanctions in place (including TFS) and their obligations, with a view to preventing proliferation activities;

(b) **Alert:** Giving early alerts to FIs, DNFBPs and other relevant sectors on the latest updates to UNSC sanctions implemented in Hong Kong; and closely monitoring the lists of persons and entities designated by the UNSC for TFS and alerting FIs and DNFBPs of the updates without delay, so that they could conduct screening and report any suspected proliferation/PF-related activities to relevant authorities in a timely manner;

(c) **Coordination**: Maintaining effective coordination within the Government through the inter-agency platform coordinated by CEDB, which shares intelligence, discusses

typologies, trends and cases, and coordinates government-wide actions and responses; and keeping close communication with regulators and DNFBP supervisors to enhance the counter proliferation/PF efforts of FIs, DNFBPs and other relevant sectors; and

(d) **Enforcement**: Conducting vigilant investigations into suspected proliferation/PF cases, in accordance with the law through LEAs; and maintaining effective supervision and close monitoring by regulators and DNFBP supervisors of the compliance by FIs and DNFBPs with their TFS obligations.

9.46 Guided by the above strategy, government agencies, regulators/supervisors and the private sector will continue to work together and enhance their counter-proliferation efforts.

ANNEX A – LIST OF ABBREVIATIONS

ADCC	Anti-Deception Coordination Centre
AEOI	Automatic exchange of financial account information in tax matters
AFCD	Agriculture, Fisheries and Conservation Department
AFRC	Accounting and Financial Reporting Council
AIs	Authorised institutions
AML	Anti-money laundering
AMLO	Anti-Money Laundering and Counter-Terrorist Financing Ordinance
APG	Asia/Pacific Group on Money Laundering
ATM	Automatic teller machine
BDDS	Bank Document Digitisation System
BEPS	Base erosion and profit shifting
BO	Banking Ordinance
BRO	Business Registration Ordinance
CBNIs	Currency and bearer negotiable instruments
CCB	Commercial Crime Bureau
CCC	Central Coordinating Committee on AML/CFT
CCE	Commissioner of Customs and Excise
CDD	Customer due diligence
C&ED	Customs and Excise Department
CEDB	Commerce and Economic Development Bureau
CEO	Chief Executive Officer
CFT	Counter-financing of terrorism
CGSE	Chinese Gold and Silver Exchange Society
CIS	Collective Investment Scheme
CO	Companies Ordinance
CPAs	Certified public accountants
CPD	Corruption Prevention Department
CPF	Counter proliferation financing
CR	Companies Registry
CRD	Community Relations Department
CSTCB	Cyber Security and Technology Crime Bureau
DNFBPs	Designated non-financial businesses or professions
DPMS	Dealers in precious metals and stones
DPRK	Democratic People's Republic of Korea
DPRK Committee	Democratic People's Republic of Korea Committee established under Resolution 1718
DPRK Regulation	United Nations Sanctions (Democratic People's Republic of Korea) Regulation
DoJ	Department of Justice
DTROP	Drug Trafficking (Recovery of Proceeds) Ordinance
EAA	Estate Agents Authority
EAO	Estate Agents Ordinance
EDD	Enhanced customer due diligence
EOI	Exchange of information
FAQs	Frequently asked questions

FATF	Financial Action Task Force
FCU	Financial Crimes Unit
FDAP	Financial Data Analytic Platform
FDHs	Foreign domestic helpers
Fintech	Financial technology
FIs	Financial institutions
FID	Financial Investigation Division
FIG	Financial Investigation Group
FIIB	Financial Intelligence and Investigation Bureau
FIUs	Financial Intelligence Units
FMLIT	Fraud and Money Laundering Intelligence Taskforce
FOO	Fugitive Offenders Ordinance
FPS	Faster Payment System
FSTB	Financial Services and the Treasury Bureau
GDP	Gross domestic product
HKAB	Hong Kong Association of Banks
HKEX	Hong Kong Exchanges and Clearing Limited
HKICPA	Hong Kong Institute of Certified Public Accountants
HKMA	Hong Kong Monetary Authority
HKPF	Hong Kong Police Force
HKSAR	Hong Kong Special Administrative Region
HRA	Risk Assessment of Money Laundering and Terrorist Financing of Hong Kong
IA	Insurance Authority
IAACA	International Association of Anti-Corruption Authorities
ICAC	Independent Commission Against Corruption
ICO	Initial coin offering
ICTU	Inter-departmental Counter-terrorism Unit
IEO	Import and Export Ordinance
IIs	Insurance Institutions ("Authorised insurers carrying on long term business, and licensed insurance intermediaries carrying on regulated activities in respect of long-term business")
ILAS	Investment-linked Assurance Scheme
IMMD	Immigration Department
INTERPOL	International Criminal Police Organisation
IOSCO	International Organization of Securities Commissions
IO	Insurance Ordinance
IP	Internet protocol
Iran Regulation	United Nations Sanctions (Joint Comprehensive Plan of Action - Iran) Regulation
Iran Committee	Iran Committee established under Resolution 1737
IRD	Inland Revenue Department
IRO	Inland Revenue Ordinance
ISIL	Islamic State of Iraq and the Levant
JFIU	Joint Financial Intelligence Unit
LB	Liaison Bureau
LCs	Licensed corporations

LEAs	Law enforcement agencies
LegCo	Legislative Council
LPs	Limited partnerships
LPF	Limited partnership fund
LPO	Legal Practitioners Ordinance
LSHK	Law Society of Hong Kong
MCVs	Mainland Chinese visitors
MD	Marine Department
ME	Mutual evaluation
ML	Money laundering
MLA	Mutual legal assistance
MLAO	Mutual Legal Assistance in Criminal Matters Ordinance
MLO	Money Lenders Ordinance
MMOU	Multilateral Memorandum of Understanding
MOU	Memorandum of Understanding
MSOs	Money services operators
MSSB	Money Service Supervision Bureau
National Security Law	Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region
NB	Narcotics Bureau
NEC	Non-ethnic Chinese
NPMs	New payment methods
NPOs	Non-profit organisations
OCI	Office of the Commissioner of Insurance
OECD	Organisation for Economic Co-operation and Development
OFC	Open-ended fund company
OTC	Over-the-counter
OSCO	Organized and Serious Crimes Ordinance
P2P	Peer-to-peer transaction
PAO	Professional Accountants Ordinance
PBOC	People’s Bank of China
PEPs	Politically exposed persons
PF	Proliferation financing
POBO	Prevention of Bribery Ordinance
POS	Point-of-sale
PRC	People’s Republic of China
PSSVFO	Payment Systems and Stored Value Facilities Ordinance
R32 Ordinance	Cross-boundary Movement of Physical Currency and Bearer Negotiable Instruments Ordinance
RAU	Risk Assessment Unit
RBA	Risk-based approach
Registrar	Registrar of Companies
Regtech	Regulatory technology
RIs	Registered institutions
RMB	Renminbi
RML	Registrar of Money Lenders

SB	Security Bureau
SCR	Significant controllers registers
SFC	Securities and Futures Commission
SFO	Securities and Futures Ordinance
SMEs	Small-and-medium-sized enterprises
STR	Suspicious transaction reporting
Suptech	Supervisory technology
SVF	Stored value facility
Steering Committee	Steering Committee of the ML and TF Risk Assessment in Hong Kong
TBML	Trade-based money laundering
TCSPs	Trust or company service providers
TF	Terrorist financing
TFS	Targeted Financial Sanctions
TID	Trade and Industry Department
TO	Trustee Ordinance
UMSO	Unlicensed money service operation
UNATMO	The United Nations (Anti-Terrorism Measures) Ordinance
UNSC	United Nations Security Council
UNSCRs	United Nations Security Council Resolutions
UNSO	United Nations Sanctions Ordinance
World Bank Tool	World Bank National Risk Assessment Tool
WMD	Weapons of mass destruction
WMDO	Weapons of Mass Destruction (Control of Provision of Services) Ordinance
VAs	Virtual assets
VASP	Virtual asset services provider
VBs	Virtual banks

ANNEX B – LIST OF FIGURES/TABLES/BOXES

Figures/Tables

Boxes