Speech by SJ at plenary session of 15th China-ASEAN Prosecutors-General Conference (English only) (with photo)
****

Following is the speech by the Secretary for Justice, Mr Paul Lam, SC, at the plenary session of the 15th China-ASEAN Prosecutors-General Conference today (September 23):

Your Excellencies, distinguished delegates, ladies and gentlemen,

Hong Kong is one of the least corrupt places in the world. However, money laundering remains a serious issue because of other types of financial crimes such as deception. The proceeds of financial crimes, whatever they are, become the subject matter of money laundering. In 2024, there was a 2.3-fold increase in the number of persons prosecuted for the offence of money laundering compared with 2023, and 648 individuals were convicted of money laundering offences. We applied for court orders to restrain over HK$360 million of suspected serious crime proceeds under police investigation. Our anti-corruption agency, the Independent Commission Against Corruption, also applied to restrain over HK$400 million of suspected crime proceeds under investigation. By the end of 2024, around HK$2 billion remained restrained.

To prevent and combat money laundering effectively would require the co-ordination and co-operation among the general public, the financial institutions, the law enforcement agencies and regulatory bodies, the prosecution and also the judiciary. Further, while money laundering usually and traditionally involves funds in bank accounts, virtual assets are now being used for such purposes. I would like to highlight recent Hong Kong developments in four areas, which are relevant to "Combatting Money Laundering and Corruption, and Recovering Assets in the Technological Age".

Deterring members of general public from acting as money mules

The use of "mule accounts" is common in money laundering. "Mule accounts" refer to accounts suspected of being sold or rented out for laundering crime proceeds, and money mule is someone who transfers illegal money on behalf of others. The purpose of using mule accounts is to make it more difficult to trace the funds, and to identify and prosecute the true criminals committing the underlying offences. We use two main ways to deter people from acting as money mules.

First, public education. In April 2025, it was announced that the Hong Kong Monetary Authority (HKMA), the Hong Kong Police Force (HKPF) and the banking industry will strengthen publicity and education efforts to disseminate messages to customers regarding "Don't Lend/Sell Your Account" including outreach activities to targeted segments, and enhance industry co-ordination through the formation of the Anti-fraud Education Taskforce by the Hong Kong Association of Banks (HKAB) comprising 18 major banks. The purpose is to remind and warn people that they should not be tempted by quick money and lend or sell their bank accounts to anyone laundering money;

otherwise, they run the risk of being convicted of money laundering offences.

Second, heavier penalties. The HKPF would apply to the Court for enhanced sentencing, namely, to impose a more severe penalty, in money laundering cases in order to produce a stronger deterrent effect. By early April 2025, the sentences of 95 mule account holders had been increased by 13 per cent to 33 per cent, with sentences ranging from 21 to 75 months of imprisonment. In a very recent District Court case, HKSAR v Luo Jiayou [2025] HKDC 1334, decided on August 5, 2025, the money mule opened three bank accounts for his friend and received RMB4,000 as a reward; the total sum received by the three bank accounts was HK$9 million odd. The prosecution applied for an enhanced sentence pursuant to specific provisions in the Organized and Serious Crimes Ordinance (Cap.455). The Court held that: first, there is clear and cogent evidence that money laundering using bank accounts opened by "ML Stooges" is still widespread and commonly being practised in Hong Kong today; second, what true criminals need are gullible scapegoats like the defendant in that case who would take the blame for them when the law enforcement takes action; third, the court must send a clear message to the general public that people who play the role of "ML Stooge" will receive severe punishment, so that there is a deterrent effect; and when there are fewer or no willing "ML Stooges", the criminal activities which rely on their bank accounts would fail. At the end, the Judge increased the original sentence of 40 months by 25 per cent to 50 months.

Requiring and empowering bank and other institutions to detect and then report suspicious transactions

Banks are on the frontline of global efforts against money laundering. This is necessarily so because the targeted funds pass through their hands and generally only banks are positioned to detect and scrutinise suspicious transactions. Only they have knowledge of their customers and their banking activities. Accordingly, our statutory and regulatory rules (for example, the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)) require banks to have in place a working system to conduct customer due diligence; to maintain continuous monitoring of customer accounts; to investigate suspicious transactions; to cease dealing with the account holders and to freeze the funds where suspicions are unresolved; and to report suspicions to the Police. There are four points I wish to make concerning our efforts to ensure compliance of these obligations on the part of the relevant institutions and to enhance their capabilities to do so.

(i) Strict enforcement of legal and regulatory duties

In case of contravention of the relevant legal and regulatory obligations, apart from potential criminal liabilities, the bank in question may be subject to disciplinary actions resulting in reputational damage. As an example, on July 22, 2025, the HKMA announced that it had taken disciplinary actions against three banks under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance: the penalties included a reprimand; an order to conduct a look-back review of past transactions, and develop and

implement a remedial plan to address the contraventions; and pecuniary penalties. But these are very exceptional cases because banks in Hong Kong take compliance issues seriously. In the first eight months of 2025, over 120 000 suspicious transactions were flagged by the financial sector and professionals.

(ii) Use of artificial intelligence

On September 9, 2024, the HKMA issued a circular on the Use of Artificial Intelligence for Monitoring of Suspicious Activities. It is taking various initiatives to further support and accelerate the use of artificial intelligence in suspicious activity monitoring: to give two examples, first, sharing experience and success stories of AI by organising experience sharing forums with speakers from the industry and technology firms; and, second, providing targeted guidance and support by a dedicated team with an external consultant.

(iii) Enabling information sharing among banks

One of the challenges of combatting money-laundering is the "information gap" exploited by criminals to rapidly move and conceal illicit funds through the banking system, because banks that detect illicit activities cannot alert other banks owing to contractual and common law confidentiality obligations and statutory data privacy requirements. Hence, in June 2023, the HKMA, the HKPF and the HKAB jointly launched the Financial Intelligence Evaluation Tool to allow rapid sharing of information on corporate accounts among 10 participating financial institutions. However, about 90 per cent of mule accounts involved in fraud-related money laundering activities are actually individual accounts, rather than corporate accounts.

To plug this loophole, on June 4 this year, the Banking (Amendment) Ordinance 2025 was passed, and it will come into effect on a date later this year to be announced. The new law provides authorised financial institutions with a voluntary sharing mechanism to request or disclose information on the detection or prevention of crimes whether the account holders concerned are corporate or individual. More importantly, the law makes safe harbour provisions for institutions disclosing information under the voluntary mechanism or using information so disclosed by other institutions so that they will be immune from potential prosecution or civil liability for breach of confidence.

(iv) Extending legal and regulatory requirements to virtual assets

A new licensing regime for Virtual Asset Trading Platforms (VATPs) took effect back on June 1, 2023, which included the coming into effect of the Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Ordinance 2022 (Cap. 615). One of the purposes of the statutory amendment was to apply customer due diligence and record-keeping requirements to virtual asset service providers. Pursuant to the statutory amendment, the Securities and Futures Commission (SFC), responsible for supervising the VATPS, has published the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset

Service Providers).

Stopping dissipation of funds in money laundering

Upon detection of suspected money laundering, the important thing is to stop the funds or property in question from further dissipation as soon as practicable. This is essential in order to enable the victims to recover the assets upon the conclusion of the relevant legal proceedings. In Hong Kong, where a bank has identified suspected transactions, it is obliged to submit a Suspicious Transaction Report to the Joint Financial Intelligence Unit (JFIU), which is operated primarily by the HKPF and the Customs and Excise Department. At the same time, the bank will freeze the account provisionally. The JFIU will decide within two working days whether the bank should receive consent to deal with the funds in question. If consent is given due to unsubstantiated suspicion, the JFIU will issue a Consent Letter to the bank which will enable it to deal lawfully with the funds.

But if there are good reasons for suspicion requiring further investigation, the JFIU will issue a Letter of No Consent (LNC) to the bank, which generally will continue to freeze the account. The LNC is usually valid for six months. When the LNC is in force, the JFIU shall use its best endeavours to obtain a restraint order from the Court under the Organized and Serious Crimes Ordinance or procure the victim to seek an injunction from the Court to formally freeze the funds in the bank. It is most significant that, on April 10, 2024, the Court of Final Appeal of HKSAR in Tam Sze Leung and others v Commissioner of Police [2024] HKCFA 8 confirmed that the scheme of issuing LNCs is lawful and constitutional and does not infringe the right to property and other rights protected by our Basic Law.

It should be noted that LNCs have been issued not only against funds in bank accounts but also virtual assets. In a case decided back in 2021, Yan Yu Ying v Leung Wing Hei [2021] HKCFI 3160, the HKPF had issued LNC to virtual asset service providers to prevent the dissipation of 999 Bitcoins. In a more recent case HKSAR v. Tam Lai Yin [2025] HKCFI 2116, the Police seized or froze the tainted cryptocurrency with a cold wallet to prevent dissipation.

It is equally important to bear in mind that the victim may also apply for injunctions in civil actions to restrain the further dissipation of the relevant funds. This is particularly useful when, for whatever reasons, the Police is unable, or no longer able, to freeze the funds in question. In such event, the Police would usually inform the victim and advise him to take civil proceedings to safeguard his position. As an example, in a recent case decided on August 28, 2025, Shan Jau Chan and another v. Yuloong Trading Co Ltd and others [2025] HKCFI 3888, upon an application by the victim of a cyber-fraud, the Court granted an interim injunction to restrain dissipation of the funds in question when the Police indicated that they could no longer maintain the LNC upon legal advice.

The Court has adopted various innovative measures, likely to be among the first in the world, in assisting victims when the property involved cryptocurrencies. As example, in a

recent case decided in April 2025, BP SG Investment Holding Limited v. Chen Shanxian and others (HCA 533/2025), the fraudster transferred assets of the victim into non-custodial cryptocurrency wallets. Non-custodial wallets are anonymous, decentralised and non-regulated; and therefore, it is almost impossible to identify the persons behind such wallets who perpetrated the relevant fraudulent transactions. This also makes it difficult to conduct effective service of the court documents on the defendants, such as an injunction order, which is usually essential in civil proceedings. To resolve this practical difficulty, the Court permitted the injunction order to be served firstly, through a tokenised injunction order, secondly, through a messaging platform between virtual asset wallets, and thirdly, through airdropping a non-fungible token (commonly known as NFT) containing a hyperlink to the court order. Putting aside the technicalities involved, these methods of service effectively "taint" the relevant wallets in the sense that all subsequent transactions that follow the service can be traced to the blockchain and the existence of the injunction can be seen, effectively deterring others from transacting with these wallets. Furthermore, the Court ordered the transfer of the suspected fraud proceeds to a custodial wallet to be held in escrow by a cryptocurrency custodian pending the final outcome of the case. These arrangements ensured the effective preservation of virtual assets.

Enhancing prosecution's capability to handle technological crimes

Enhancing our prosecutorial capability to deal with technological crimes is, of course, vital. To this end, in 2023, the Department of Justice set up the Technology Crime Sub-division under the Prosecutions Division. This division comprises counsel with specialised knowledge and built-up experience in prosecuting sophisticated and syndicated technology crime cases. Their duties also include providing legal advice to law enforcement agencies, active involvement in new legislation on cybersecurity and technology crimes, and exchange of knowledge and experience in combatting technology crimes with law enforcement agencies and other stakeholders.

What I said above are merely examples and highlights, but I believe they serve as cogent evidence that Hong Kong will indeed spare no effort in preventing and combatting money laundering and corruption, and recovering assets in the technological age. We also look forward to strengthening our collaborations with other jurisdictions, including of course member states of ASEAN, in this respect. Thank you very much.

Ends/Tuesday, September 23, 2025