立法會
Legislative Council

LC Paper No. CB(1)960/2025

Ref : CB1/BC/5/25

Report of the Bills Committee on Banking (Amendment) Bill 2025

Purpose

This paper reports on the deliberations of the Bills Committee on Banking (Amendment) Bill 2025 ("the Bills Committee").

Background

2. In recent years, there has been a sharp increase globally in financial crime, especially digital fraud and related money laundering activities. In 2024, the Hong Kong Police Force ("HKPF") received nearly 45 000 fraud cases with a loss of over $9.1 billion. Experience shows that information sharing among banks and law enforcement agencies ("LEAs") is of paramount importance to combating such crimes. In this regard, the Hong Kong Monetary Authority ("HKMA"), HKPF and the banking sector have put in place a number of measures, including the Fraud and Money Laundering Intelligence Taskforce and the Anti-Deception Coordination Centre run by HKPF with the support of HKMA. However, with the limitations in the existing mechanism, an information gap among authorized institutions ("AIs") is being exploited by criminals to rapidly move and conceal illicit funds through the banking system.

3. Seeking to narrow the information gap, HKMA, HKPF and the Hong Kong Association of Banks ("HKAB") jointly launched the Financial Intelligence Evaluation Sharing Tool ("FINEST")[1] in June 2023 to allow rapid sharing of information on corporate accounts among the 10 participating AIs. However, about 90% of mule accounts involved in fraud-related money laundering activities are actually individual accounts. Owing to contractual and common law confidentiality obligations, as well as

---

[1] The Financial Intelligence Evaluation Sharing Tool ("FINEST") is a platform for sharing information between AIs. It is currently limited to sharing of information on corporate accounts only.

the requirements under the Personal Data (Privacy) Ordinance (Cap. 486), AIs are not able to alert each other by sharing information involving individual accounts among themselves.

4. The Administration proposes to amend the Banking Ordinance (Cap. 155) ("BO") with a view to implementing a mechanism to further narrow the information gap abovementioned. The mechanism will provide a safe harbour for AIs to share with each other information of both corporate and individual accounts on a voluntary basis, when AIs become aware of suspected prohibited conduct (i.e. money laundering, terrorist financing or financing of proliferation of weapons of mass destruction).

Banking (Amendment) Bill 2025

5. The Banking (Amendment) Bill 2025 ("the Bill") was published in the Gazette on 28 March 2025 and received its First Reading at the Legislative Council ("LegCo") meeting of 2 April 2025. The Bill seeks to amend BO to:

(a) introduce a voluntary mechanism for AIs to request or disclose information for the detection or prevention of crimes;

(b) make safe harbour provisions for AIs disclosing information under the voluntary mechanism or using information so disclosed by other AIs; and

(c) provide for related matters and make related amendments.

Bills Committee

6. At its meeting on 11 April 2025, the House Committee agreed to form a Bills Committee to scrutinize the Bill. The membership list of the Bills Committee is in **Appendix 1**. Under the chairmanship of Hon CHAN Chun-ying, the Bills Committee has held two meetings with the Administration. The Bills Committee has also invited written submissions from the public.[2] A list of organizations which have submitted views to the Bills Committee is in **Appendix 2**.

---

[2] For details, please see the written submission and the Administration's consolidated written response.

Deliberations of the Bills Committee

7. Given that FINEST currently does not capture personal account information, the Bills Committee supports the Administration's initiative to amend BO which would, in the face of rampant ML and fraud activities, enhance the regulatory mechanism. This is not only an important step to strengthen the financial security of Hong Kong, but will also significantly improve the effectiveness of Hong Kong as an international financial centre in combating fraud and money laundering.

New measures for stepping up efforts to combat fraud and money laundering activities

8. Members are pleased to note that HKMA, HKPF and HKAB announced five new anti-fraud measures on 10 April 2025, and have asked the Administration to elaborate on the implementation of these measures. The five measures include expanding the use of Scameter data, enabling bank-to-bank information sharing, sharing good anti-fraud practices with banks, conducting thematic reviews on the effectiveness of banks' anti-fraud controls, and enhancing publicity and public education on "Don't Lend/Sell Your Account".

9. HKMA has advised that it would further enhance the information sharing capability among banks, and will open up more Scameter data, including mobile phone numbers and emails of fraudsters, to banks and stored value facility operators to help them identify suspicious accounts. In addition, guidelines on best practice have been issued to the industry which suggest, among others, inviting victims to branches for interviews and approaching their families. A thematic review will also be conducted in the second half of 2025 to examine the effectiveness of the measures to help banks optimize their anti-fraud measures. HKMA will continue its publicity efforts on "Don't Lend/Sell Your Account", targeting foreign domestic helpers, new arrivals, etc., and will work with banks and the Police to step up education. HKAB has set up a task force comprising five representatives from each of the 18 banks to further strengthen publicity.

10. Members have highlighted that the Mainland and Singapore have already implemented specific legislation regarding "Don't Lend/Sell Your Account". Their legislative threshold, under which the mere lending or selling of accounts would constitute evidence of an offence, is lower than that of the existing Organized and Serious Crimes Ordinance (Cap. 455) in Hong Kong. Members have suggested that the Administration draw on international experience and consider streamlining the prosecution procedures to improve the anti-fraud legal framework. HKMA has

responded that it would study the feasibility of the proposals with the Police and would continue to draw reference from international practices.

Effectiveness of voluntary information sharing mechanism

11. Members have pointed out that there are insufficient incentives for banks to participate in the voluntary information sharing mechanism, especially for small and medium-sized ones which face high costs and technical challenges. To encourage participation, members have suggested streamlining the compliance checks on participating institutions and providing tax incentives as well as technical support. Some members are of the view that voluntary participation might not fully protect the interests of the public, and suggest that the Administration consider drawing up a timetable for mandatory participation.

12. The Administration has advised that during the consultation process, HKMA has discussed with AIs the advantages of joining the information sharing mechanism on a voluntary basis, e.g. enhancing banks' anti-fraud measures and boosting customer confidence. Ten large as well as small and medium-sized AIs have already participated. As AIs have their own mechanism in place to detect suspicious transactions, there will not be much additional cost arising from their participation in the information sharing mechanism. HKMA will continue to monitor the progress closely and provide support on technical or other aspects, such as access to the system. HKMA will also enlist the assistance of the Police if necessary.

13. The Administration has added that similar initiatives in other countries are also voluntary in nature. While it is currently launched on a voluntary basis, the possibility of moving to mandatory participation in the future will not be ruled out. The Administration has remarked that more AIs would be progressively invited to participate in the future, depending on the circumstances and the readiness of the systems of individual AIs. However, the focus at this stage is mainly on retail banks of medium size and above, as past experience shows that the chance of fraudsters exploiting small banks or private banking services is relatively low.

14. Regarding the Administration's reference to the United States, the United Kingdom ("UK") and Singapore which have all introduced mechanisms to allow financial institutions to share information on a voluntary basis, members have enquired whether the provisions in the Bill, as drafted, are broadly in line with those in the legislation of other countries and regions. HKMA has advised that in drafting the Bill, reference has been drawn from the relevant legislation in Singapore, the UK, etc.

However, their standards are not fully adopted in some of the provisions in the light of the actual situation in Hong Kong.

Regulation of the information sharing mechanism and privacy protection

15. On the monitoring and transparency of the information sharing mechanism, members have suggested setting up an internal assessment system for AIs and a public complaint hotline. HKMA has responded that AIs are required to comply strictly with the regulations on the use of information, and HKMA is already vested with regulatory powers to, among others, assess the suitability of the persons-in-charge of financial institutions, restrict the scope of business where necessary and, in the worst case, prohibit non-compliant AIs from participating in the information sharing mechanism. HKMA has stressed that the sharing of information is limited to the detection of prohibited conduct and AIs will lose the protection against liability in the event of abuse. Both HKMA and the Police have set up dedicated complaint and enquiry hotlines, and the operation of the public complaint hotline is being further improved to enhance regulatory effectiveness and transparency.

16. Members are concerned how to prevent improper collection of information by AIs during the sharing process, and whether the information sharing mechanism would be extended to cover non-bank financial institutions, such as brokers and virtual asset companies. The Administration has advised the information sharing regime at this stage is voluntary and is mainly targeted at the banking sector, as over 80% of suspicious transaction reports ("STRs") come from the banking sector. HKMA plans to extend the mechanism to include individual accounts to facilitate information sharing among banks. The Administration is open to extending the information sharing mechanism to cover virtual asset institutions.

17. Noting that the Administration has consulted the Office of the Privacy Commissioner for Personal Data ("PCPD") on the Bill, members have enquired about the views of the Office of PCPD. HKMA has responded that the Office of PCPD expressed support for amending BO during the consultation in the first quarter of 2024 and raised issues relating to the interplay between Cap. 486 and BO. The focus is on how to ensure compliance with the requirements on the use of personal data under Cap. 486 through the new provisions without the need to obtain customers' consent. Over the past two years, HKMA has had in-depth discussions with PCPD on this issue. Under section 58(2) of Cap. 486, information disclosed for the purpose of detecting and preventing crime is exempt. This requirement has been strictly adhered to in drafting the Bill. As regards keeping

information, HKMA will reiterate through its guidelines that AIs are required to comply with the time limit for keeping information.

Platforms for information sharing among authorized institutions

18. Noting that the proposed new section 68AAM of BO provides that the Monetary Authority ("MA") has the power to designate a platform for information sharing among AIs, members have enquired about the regulation of the designated platform, whether it would be outsourced and how it is actually operated.

19. HKMA has explained that there are two main platforms under consideration. The first one is FINEST operated by the Police. As it is administered by the Police, its security and management can put the public at ease; the other platform under consideration is the information platform operated by the Hong Kong Interbank Clearing Limited ("HKICL"), i.e. ICLNet. ICLNet is highly secure, and the company responsible for its operation, with HKMA and HKAB each holding 50% of the shares, has absolute control over its operation. Due to information security considerations and the need to ensure complete control over the handling of information by HKMA, the chance of outsourcing the platform in the future is relatively low. As regards the actual operation, HKMA has advised that upon commencement of the amended BO, a platform for information sharing will need to obtain the consent of MA before it can be designated as an authorized platform and commence operation pursuant to BO, and AIs will be able to share information on the platform and enjoy the safe harbour protection. HKMA will continue to engage with the industry should there is a need to designate other platforms in the future.

20. Members have enquired about the mechanism for introducing new platforms. HKMA has explained that the provisions in the Bill empower HKMA to designate platforms other than ICLNet and FINEST. However, there is no pressing need to designate other platforms at present. The industry has no particular concerns in, for example, ICLNet, while FINEST is already widely used by AIs at this stage. Should there be a need to introduce other platforms in the future, HKMA will carefully assess whether an AI has adequate systems of control as stipulated in the Bill (see paragraph 52 of this report for details) and will fully communicate with the Police and the banking sector before designating the platforms to ensure that the relevant mechanism can work effectively.

21. Members are concerned about how the Administration would further enhance the functions of the platform to better tackle the increasingly rampant cross-border fraud practices. HKMA has pointed out that the proposed platform would cover the sharing of individual customers'

information among banks in Hong Kong, including information of persons outside Hong Kong who have opened accounts locally. At present, banks in Hong Kong generally adopt a prudent attitude in handling cross-border remittance transactions and have put in place an enquiry mechanism to ensure the security of the transactions. When a bank finds that a customer may have been subject to fraud, it will usually halt the transaction in order to prevent financial loss. However, while these measures are effective to a certain extent, they fall short in addressing the increasingly rampant cross-border fraud activities. In view of the extensive impact of cross-border fraud, HKMA plans to explore more effective countermeasures with other regulators through international platforms or international organizations.

Security of the platforms

22. Members note that at this stage, pending HKMA's designation of the platform for information sharing among AIs, FINEST operated by HKPF is being used. According to paragraph 17 of the LegCo Brief, HKPF is carrying out system upgrading and expansion of FINEST with existing resources. While considering that both platforms, operated by HKICL or the Police respectively, meet the security standards, members are concerned about the control measures over the platforms and suggest that the list of participating banks should be made public to enhance transparency.

23. HKPF has advised that FINEST currently in use is operated strictly in accordance with the requirements of the Security Bureau and the Digital Policy Office, covering areas such as risk assessment, incident response and cloud security, and is in compliance with industry standards. Professional encryption technology is adopted for all data transmission, and the whole system is based on the Government Cloud architecture with a backup centre for real-time fault handling. In terms of access control, the system adopts dual authentication (password plus one-time passcode) and is restricted to authorized personnel of HKMA, participating banks and HKPF. In addition, the servers are located in HKPF facilities to ensure security.

24. The Administration has added that the 10 participating retail banks include the Hongkong and Shanghai Banking Corporation, Bank of China (Hong Kong), Standard Chartered Bank (Hong Kong), Hang Seng Bank, Industrial and Commercial Bank of China (Asia), Bank of East Asia, China Construction Bank (Asia), Dah Sing Bank, DBS Bank (Hong Kong) and ZA Bank. These institutions range from large banks to medium and small banks, with a 75% coverage of accounts (corporate and personal). HKMA has remarked that it will continue to expand the scope of participating AIs and is considering whether to publish the full list of participating banks on its official website.

25. As regards the control measures, HKMA has explained that one of the preparatory tasks is to require the 10 participating banks to conduct a self-examination of their existing control systems to ensure compliance with the requirements of HKMA and HKAB. The banks are required to conduct assessments and submit reports through their internal audit departments.

Interface between platforms and suspicious transaction notifications

26. Members note that at present, banks are required to report to the Joint Financial Intelligence Unit ("JFIU"), jointly run by officers of HKPF and the Hong Kong Customs & Excise Department, the details of transactions as soon as possible when they detect or suspect any suspicious financial activities. The Administration has been requested to explain how the existing FINEST can effectively interface with the suspicious transaction notification to enhance the overall operational efficiency.

27. HKMA has responded that when a bank finds that a customer may be involved in fraud or is about to be defrauded, it may enquire the payee bank for relevant information, assess the risk and take actions. If a bank has received repeated enquiries about a potential mule account or recognized that the account is involved in illegal activities, it should file an STR with JFIU as required. Before an STR is formally filed, the bank can immediately notify other participating banks through FINEST. This will fill the information gap more quickly so that other banks can be alerted in a timely manner to block suspicious transactions upon receipt of the alert. The proposed mechanism will complement the existing suspicious transaction reporting mechanism under Cap. 455.[3] AIs will be able to obtain more comprehensive information under the proposed mechanism, which will help enhance their filing of STRs.

Commencement of the Bill

28. Under clause 1(2) of the Bill, the Bill (if passed) will come into operation on a day to be appointed by the Secretary for Financial Services and the Treasury by notice published in the Gazette. The Administration has been requested to advise when the proposed mechanism will come into operation.

---

[3] Under the relevant provisions in Cap. 455 and similar provisions in the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) and the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575), AIs are required to report to the LEAs any suspected dealing in proceeds of crime.

29. The Administration has advised that it will bring the information sharing mechanism proposed under the Bill into operation as soon as possible within 2025. It is now proactively making preparations, including, among others, making adjustments to FINEST so as to cater for the expansion of its scope, expanding its capacity to cover individual accounts and preparing the guidelines to be issued by MA under the proposed new section 68AAL of BO.[4] Meanwhile, AIs participating in the proposed information sharing mechanism will also need time to upgrade or establish their systems of control for the purpose of fulfilling the requirement under the proposed new section 68AAH(1) of BO (i.e. MA may give a written approval for an AI to access a designated platform if MA is satisfied that the AI has established adequate systems of control for ensuring the AI's compliance with the relevant requirements). The Administration will determine the commencement date of the Bill taking into account the progress of the preparations aforementioned.

Definitions of overseas money laundering and prohibited conduct (proposed new section 68AA)

30. The proposed new section 68AA of BO defines "prohibited conduct" and "money laundering". The Administration has been requested to clarify whether the indictable offences under the definitions are not limited to those occurring in Hong Kong. For example, if funds involved in overseas money laundering activities are transferred to accounts in Hong Kong, whether this would be covered by the proposed information sharing mechanism, and whether AIs would be allowed to intercept the illicit funds.

31. The Administration has explained that the dealing with the proceeds of a conduct that is committed outside Hong Kong but would constitute an indictable offence if it had occurred in Hong Kong is "money laundering" under BO. Even if the offence is committed overseas, a local AI may still disclose information under the proposed mechanism when dealing with the relevant property or proceeds. Moreover, the definition of "money laundering" in the Bill includes "money laundering" as defined in the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615), which means an act intended to make illicit proceeds not to appear to be such proceeds, whereas the definition of "money laundering" in the Bill includes, in addition to this meaning, the dealing of property that is the proceeds of an indictable offence.

---

[4] Under the proposed new section 68AAL of BO, MA has the power to issue guidelines on matters relating to the proposed new Part XIIAA by notice in the Gazette or in another appropriate way, and such notice is not subsidiary legislation. In addition, MA may give a written direction to an AI directing it to take or refrain from taking a specific action if MA considers it necessary to ensure compliance with the requirements of the proposed new Part XIIAA.

Scope of request for and disclosure of information (proposed new section 68AAB)

32. HKMA launched a public consultation on the proposal for information sharing among AIs for the purposes of preventing or detecting crime in January 2024 and issued the Consultation Conclusions in September of the same year. Paragraph 3.9 of the Consultation Conclusions states explicitly that information shared should be limited to what is relevant and necessary to achieve the purposes of preventing and detecting crime. Under the proposed new section 68AAB(1) of BO, information that an AI (institution A) could request from another AI must be information relating to the entity, account or transaction concerned that may assist institution A in detecting or preventing prohibited conduct as defined in the proposed new section 68AA (e.g. money laundering) as required by the proposed new section 68AAB(2)(b).

33. The Legal Adviser to the Bills Committee has expressed concern as to whether the proposed scope of information under section 68AAB(2)(b) (i.e. may assist institution A in its inquiries for detecting or preventing any prohibited conduct) really meets the criteria of being "relevant and necessary". For example, the Economic Crime and Corporate Transparency Act 2023 of the UK (as quoted in the public consultation document) explicitly limits the scope of information to "information which will or may assist institution A in carrying out its relevant actions" and sets out the specific types of actions, such as customer due diligence, identity verification, termination of business relationship or refusal to deal. The Legal Adviser to the Bills Committee has requested the Administration to further clarify the scope of application of the proposed provision to ensure its precision and necessity.

34. The Administration has advised that the proposed new section 68AAB of BO provides that an AI (i.e. institution A) may request from another AI (i.e. institution B) information that relates to, among others, a customer of institution A or an entity, account or transaction associated with that customer, for the purpose of assisting institution A in its inquiries for detecting or preventing any prohibited conduct (as the proposed new section 68AAB(2)(b) of BO refers). In practice, institution A, when making an information request to institution B, will have become aware of an activity (e.g. a transfer of funds from an account under institution A to an account under institution B) that may be involved in prohibited conduct. Upon receiving information from institution B, institution A will conduct an inquiry to determine whether there is a risk that any entity, account or transaction involved in the activity concerned may be involved in a prohibited conduct. If institution A comes to the view that the entity, account or transaction may be involved in prohibited conduct, then it may

decide to take further action including filing an STR with the relevant LEAs in accordance with section 25A(1) of Cap. 455, section 25A(1) of the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) or section 12(1) of the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575). Further actions, including possible freezing or closure of accounts, may follow after consultation with the relevant LEAs, so as to achieve the aim of detecting or preventing the prohibited conduct concerned.

Mechanism for disclosure of information by authorized institutions

35. Members have pointed out that the requirements on disclosure of information in the Bill relate to different scenarios where in particular, (a) the procedure when institution A makes a request for information to institution B under section 68AAB(3) of BO; (b) the disclosure of information to institution A by institution B upon receipt of a request under section 68AAC(1) of BO; and (c) the disclosure of information which may be made by an AI on its own initiative under section 68AAC(4) of BO. The Administration has been requested to explain the practical operational scenarios corresponding to each of these three provisions to facilitate compliance by the banking sector.

36. HKMA has replied that under the proposed new section 68AAB of BO, an AI may request customer information from other financial institutions but must provide specific background (e.g. its own customers' related information) for the counterparty to assess and decide on the details of the disclosure. This is a disclosure "on request". Under the proposed new section 68AAC(1) of BO, when institution B receives a request from institution A and discloses information in accordance with the requirements, this is a "one-to-one" disclosure. Under the proposed new section 68AAC(4) of BO, an institution may disclose "on its own initiative" information to another institution if it suspects that prohibited conduct exists, and this may be done on a "one-to-multiple" basis to alert other institutions. Thus, the three provisions correspond to three different scenarios.

37. Members have enquired whether a disclosing institution must have reasonable grounds to believe that the relevant entity or account is involved (or may be involved) in prohibited conduct in order to make a disclosure. HKMA has responded that there are two types of procedures under the information sharing mechanism depending on the scenarios: the first one is the "request/response" procedure, which is applicable when AIs have identified suspicious activities but the level of reasonable suspicion is not yet reached. They seek to make clarification through communication with other AIs. If no suspicious transactions are identified, the procedure will come to a close, but if found suspicious, an STR will be filed, and the relevant information will be made known only to the AIs involved before the

filing of the STR. The second type is the "notification on one's own initiative" procedure, whereby AIs proactively alert multiple AIs (on a "one-to-multiple" basis) when the threshold of reasonable suspicion is reached (usually having filed an STR or possessing law enforcement intelligence), even if the correlation has not yet been fully recognized. The purpose of this alert is to provide a quick early warning to disrupt suspicious movement of funds. This classification is designed to strike a balance between risk management efficiency and customer privacy protection.

Information that relates to an entity, account or transaction associated with an occasional transaction

38. Under the proposed new section 68AAB(1) of BO, when institution A (an AI) needs to investigate a suspicious transaction, it may request institution B (another AI) to provide relevant information in two scenarios: the first scenario (section 68AAB(1)(a)) in respect of a suspicious transaction involving institution A's own customers and the second scenario (section 68AAB(1)(b)) in respect of a suspicious transaction involving institution B's customers. The Legal Adviser to the Bills Committee has pointed out the difference in the scope of information to be obtained on suspicious transactions in these two scenarios and sought clarification on the legislative considerations and specific basis for the different scope of information to be obtained in respect of suspicious transactions of institution A's own customers and those of institution B's customers.

39. The Administration has advised that the difference in the language of the proposed new section 68AAB(1)(a)(ii)(B) and section 68AAB(1)(b)(ii)(B) of BO (i.e. an occasional transaction that "institution A has been requested by entity A to conduct" in the former and an occasional transaction that "institution B may have conducted for entity B" in the latter) reflects the Administration's intent. In practice, institution A will know whether it has been requested to conduct an occasional transaction for entity A, whereas institution A will not necessarily know whether institution B has been requested to conduct an occasional transaction for entity B (if that occasional transaction ultimately did not proceed). Institution A will only either (a) know that institution B has conducted, or (b) suspect that B may have conducted, an occasional transaction for entity B. Under the proposed new section 68AA of BO, "occasional transaction" is defined as a transaction conducted between an AI and an entity, with which the AI does not have a business relationship (i.e. an entity that is not a customer of the AI). In reality, such occasional transactions are nowadays rarely conducted by AIs, given the high risks of money laundering or other illicit activities. The scenarios involving occasional transactions are included in the Bill for completeness.

Correction of inaccurate information (proposed new section 68AAE)

40. Under the proposed new section 68AAE of BO, if an AI that has disclosed any information under section 68AAB(3), 68AAC(1) or (4) or 68AAD(2) (disclosing institution) to another AI (receiving institution) becomes aware that the information is or has become inaccurate, the disclosing institution must correct the inaccuracy as soon as reasonably practicable after becoming aware of the inaccuracy. Members have enquired about the specific time frame for "making correction as soon as reasonably practicable", the liability for disclosure of inaccurate information by an institution, and the handling of subsequent requests for supplementing or updating information by the institution. HKMA has advised that the time frame for making correction would be specified in the guideline, which would in principle range from one to two days, with flexibility depending on each case. If an AI needs to provide supplementary information and acts "in good faith and with reasonable care" in doing so, it may provide such information on the platform. The safe harbour provisions in the proposed new section 68AAG of BO cover disclosures made "in good faith and with reasonable care", and AIs are not liable for unintentional mistakes.

Safe harbour provisions (proposed new section 68AAG)

41. Regarding the safe harbour provisions under the proposed new section 68AAG of BO, the Legal Adviser to the Bills Committee has sought clarification as to whether it is the Administration's intent that the information to be disclosed pursuant to the relevant section(s) under the proposed new Part XIIAA of BO would be subject to the safe harbour protection even if the information concerned is information protected by legal professional privilege; if so, of the justification(s) for such proposal; if not, whether the Administration would consider making appropriate amendment(s) to reflect the legislative intent.

42. The Administration has advised that as the information sharing mechanism proposed under the Bill is voluntary, an AI may decide whether or not any information so requested should be disclosed. In practice, it is envisaged that the information to be shared under the proposed mechanism (e.g. bank account numbers, personal data of customers and counterparties, and transaction details) will unlikely be subject to legal professional privilege (i.e. unlikely to include confidential legal advice or documents prepared for litigation). In the light of the above, the Administration considers that no amendment to the current formulation is needed.

43. The Legal Adviser to the Bills Committee has requested the Administration to clarify what "other provision" (i.e. other than contract,

enactment or rule of conduct) would be as referred to in the proposed new section 68AAG(1)(a) of BO.

44. The Administration has advised that the wording of the proposed new section 68AAG(1)(a) of BO is consistent with the safe harbour provisions for STRs in section 25A(3) of Cap. 455, section 25A(3) of Cap. 405 and section 12(3) of Cap. 575. The Administration's policy intent is to provide a safe harbour for AIs to disclose information under the proposed mechanism without being treated as breaching "other provision", which is intended to cover any unforeseen restrictions not imposed by any contract, enactment or rule of conduct.

45. Under the proposed new section 68AAG(1) of BO, an AI disclosing information under the proposed mechanism in the Bill will be protected from liabilities in relation to the disclosure (i.e. safe harbour protection). Under the proposed new section 68AAG(2)(a), one of the conditions for obtaining the safe harbour protection is that the AI that made the disclosure acted in good faith and with reasonable care in making the disclosure. As "reasonable", "care" and "good faith" are not defined under the Bill, members have asked whether the Administration will consider issuing guidelines and providing examples to help AIs meet the above condition. The Administration is also requested to provide relevant court cases for reference.

46. The Administration has explained that HKMA will issue guidelines under the proposed new section 68AAL of BO, which will cover, among other things, the need for AIs to, and examples on how AIs may, make disclosures in good faith and with reasonable care to benefit from the safe harbour protection under the proposed new section 68AAG(2)(a). The guidelines will also illustrate with examples how AIs should fulfil the above requirements. With respect to court cases, the following cases discuss those terms in other contexts:

(a) With reasonable care: There are no hard and fast principles of law to determine whether the AIs have made certain disclosures "with reasonable care"; the same depends on the facts and context of each particular case. In the context of whether a bank has breached its duty of care owed to its customer, *Dex Asia Ltd v DBS Bank (Hong Kong) Ltd & Anor* [2009] 5 HKC 289 notes that "whether a person exercises reasonable care depends on consideration of all relevant circumstances" (at paragraph 56 of the judgment); and

(b) In good faith: In the company law context on whether a court application made by members of a company to examine the

company's records is made in good faith, *Wong Kar Gee Mimi v Hung Kin Sang Raymond* [2011] 5 HKC 361 considers that "good faith" means honestly and with no ulterior motive (at paragraph 16 of the judgment). As far as the Bill is concerned, for AIs to benefit from the safe harbour protection under the proposed new section 68AAG(2)(a), it is the policy intent that the AIs must make the disclosures as permitted under the proposed new section 68AAB(3), 68AAC(1) or (4), 68AAD(2) or 68AAE(3), among other things, without any ulterior motive.

Duty of confidentiality of employees of authorized institutions

47. Under the proposed new section 68AAG(1)(b) of BO, a disclosure of information made under the proposed new Part XIIAA of BO would not render the AI that made the disclosure liable in damages for any loss arising out of the disclosure or any act or omission in consequence of the disclosure if specified conditions are satisfied. Also, under the proposed new section 68AAG(4) of BO, an AI's disclosure of information under section 68AAF(3)(a) or use of information under section 68AAF(3)(b) would not be treated as a breach of any obligation of confidence owed by the AI.

48. As an employee of an AI may also be similarly liable for a breach of confidentiality if he or she improperly discloses or misuses the information knowing of its confidential character (paragraph 72 of Volume 19 of *Halsbury's Laws of England* (fifth edition, 2011)), the Legal Adviser to the Bills Committee has expressed concern as to whether it would be necessary to extend the application of the proposed new section 68AAG(1)(b) and 68AAG(4) of BO to employees of AI to immune them from civil liabilities. For instance, section 28I(b) (i.e. the safe harbour provisions) of the Financial Services and Markets Act 2022 of Singapore (as added by the Financial Services and Markets (Amendment) Act 2023 quoted in the public consultation document) provides that both a prescribed financial institution and its officer (e.g. a director, secretary or employee of the institution) authorized to act for the prescribed institution are not liable for any loss arising out of the disclosure or publication of information etc. if certain conditions are satisfied.

49. The Administration has advised that under the proposed information sharing mechanism, a disclosure will be made by, or under the authorization of, an AI. As an AI will be permitted to disclose information within its ownership and control under the safe harbour as provided for by the proposed new section 68AAG of BO, there will be no unlawful disclosure on the part of the AI's personnel fulfilling their duties as employees within the authorization of the AI. This approach is in line with

that adopted in section 188(2) of the Economic Crime and Corporate Transparency Act 2023 of the United Kingdom and section 314(b) of the Patriot Act of the United States which provide safe harbour protection to a financial institution making a disclosure. In contrast, section 28I of the Financial Services and Markets Act 2022 of Singapore provides that a disclosure or publication may be made by a financial institution or an officer of a financial institution authorized to act for the institution or both. This is different from the approach adopted by the information sharing mechanism proposed by the Bill, under which a disclosure will be made by an AI in the name of the AI. In the light of the above, the Administration does not consider it necessary to extend the scope of application of the proposed new section 68AAG(1)(b) and 68AAG(4) of BO.

Access to designated platforms by authorized institutions (proposed new section 68AAH)

50. Members have enquired whether "access a designated platform for the purposes of this Part" in the proposed new section 68AAH(1) of BO would include an AI making a disclosure request or a disclosure on a designated platform under the proposed new sections 68AAB(4)(a), 68AAC(6)(a), 68AAD(5)(a) or 68AAE(4)(a) of BO such that the relevant AI should have adequate systems of control for ensuring the AI's compliance with the requirements under the proposed new Part XIIAA of BO in order to obtain the written approval from MA for making a disclosure request or a disclosure on the designated platform. The Legal Adviser to the Bills Committee has also sought clarification on what "adequate systems of control" would be and asked the Administration to consider whether the criteria for "adequate systems of control" should be provided for in the Bill or guidelines for the sake of clarity.

51. The Administration has explained that an AI would need to access a designated platform for both making a request for information and disclosing information under the proposed mechanism under the Bill. Under the proposed new section 68AAH(1) of BO, access to a designated platform will require the written approval of MA to be granted on the condition that MA is satisfied that the AI has adequate systems of control for ensuring its compliance with the requirements under the proposed new Part XIIAA of BO. The AI shall comply with the said condition on a continual basis, failing which MA may withdraw the approval.

52. The Administration has further explained that the systems of control of an AI under the proposed new section 68AAH of BO should cover, among others, (a) cyber security and other measures in the AI's systems to make sure that the AI's access to the designated platform will not compromise the security and integrity of the designated platform; (b) policies

and procedures for ensuring that the information requests made and information disclosed or received through the designated platform would only be dealt with by designated staff within the AI; (c) record-keeping arrangements; and (d) appropriate governance and management oversight. MA will issue guidelines under the proposed new section 68AAL of BO to set out the detailed requirements after consultation with the banking sector.

Proposed duration of keeping records and information (proposed new section 68AAI)

53. Under the proposed new section 68AAI(1)(a) and (b) of BO, an AI would be required to keep, for a specified period, a record of any request for information that it makes or receives under the proposed new section 68AAB(1) of BO, and any information that it discloses or receives under the proposed new Part XIIAA of BO. If the record or information relates to an entity with which the AI maintains or has maintained a business relationship, the specified period would be the duration of that relationship and an additional period of at least five years beginning on the date on which the relationship ends (the proposed new section 68AAI(2)(a) of BO). If the record or information relates to any other entity, the specified period would be a period of at least five years beginning on the date on which the request or disclosure is made (the proposed new section 68AAI(2)(b) of BO). The Legal Adviser to the Bills Committee has sought clarification on how these proposed requirements on keeping records and information (insofar as the information contains personal data) would comply with the Data Protection Principle 2(2) of Schedule 1 to Cap. 486 which provides that all practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is or is to be used.

54. The Administration has advised that when formulating the record keeping requirements in the proposed new section 68AAI of BO, reference has been drawn from Part 3 of Schedule 2 to Cap. 615. It is envisaged that the majority of the information to be disclosed or received under the proposed information sharing mechanism under the Bill will likely be relevant to the customer due diligence and other requirements under Cap. 615. In addition, such information to be disclosed or shared under the proposed mechanism may be included in STRs which would form the basis of law enforcement investigations and related prosecutions. In the light of the above, the Administration considers the record-keeping requirements in the proposed new section 68AAI of BO reasonable.

55. The Administration has also pointed out that MA will issue guidelines under the proposed new section 68AAL of BO to remind AIs to ensure that no personal data will be kept for longer than is necessary in

accordance with Data Protection Principle 2(2) in Schedule 1 to Cap. 486, subject to the record-keeping requirements under the proposed new section 68AAI of BO.

Production of records and information to the Monetary Authority

56. Under the proposed new section 68AAI(6) of BO, an AI would be required to produce to MA any record or information that it keeps under the proposed new section 68AAI of BO at MA's request. The Legal Adviser to the Bills Committee has sought clarification on whether it is necessary, for the sake of clarity, to provide that the production of such record or information would be subject to the safe harbour provisions under the proposed new section 68AAG of BO (currently no reference to the proposed new section 68AAI(6) has been made) to ensure that the AI would be immune from civil and criminal liabilities for the production of such record or information to MA.

57. The Administration has advised that MA is empowered to request AIs to provide information under BO for the exercise of his statutory functions (e.g. sections 63(2) and 72A(2) of BO). The approach under the proposed new section 68AAI(6) of BO is consistent with other parts of the BO. As far as personal data is concerned, section 60B(a) of Cap. 486 provides for an exemption from Data Protection Principle 3 in Schedule 1 to Cap. 486, if the use (which is defined in Cap. 486 as including disclosure or transfer) of the personal data is required or authorized by or under any enactment (i.e. the proposed new section 68AAI(6) of BO in this case).

<u>Designation of platform (proposed new section 68AAM)</u>

58. The Legal Adviser to the Bills Committee has sought clarification on why it is considered appropriate that the notice to designate a platform for the purposes of the proposed new Part XIIAA of BO under the proposed new section 68AAM(1) of BO would not be subsidiary legislation (i.e. not subject to the negative vetting procedure of LegCo under section 34 of the Interpretation and General Clauses Ordinance (Cap. 1)). The Legal Adviser to the Bills Committee has also noted that a notice to designate an "electronic MPF system" (i.e. eMPF Platform) pursuant to section 19I(1) of the Mandatory Provident Fund Schemes Ordinance (Cap. 485) is subsidiary legislation (see the Mandatory Provident Fund Schemes (Designation of Electronic MPF System) Notice (L.N. 48 of 2024) gazetted on 19 April 2024).

59. The Administration has responded that it notes that the use of the eMPF Platform is mandatory for the trustees of mandatory provident fund schemes for performing their scheme administration functions under

Cap. 485. As such, it has legislative effect, being of general application to a class of persons and of binding effect. In contrast, the proposed information sharing mechanism under the Bill is voluntary. Whilst AIs participating in the proposed mechanism will be required to disclose and receive information through platform(s) to be designated by MA, the designation of platform(s) does not have general application to the public or a class of the public and is relevant only to the AIs that choose to participate in the proposed mechanism. Therefore, the notice does not have legislative effect, as the act of designation is administrative in nature seeking to effect the relevant requirements under the Bill (e.g. under the proposed new section 68AAB(4)(a) of BO). Examples of designation notices that are not subsidiary legislation include notices relating to designation of retail payment systems under section 4(1) of the Payment Systems and Stored Value Facilities Ordinance (Cap. 584) and notices relating to designation of trading platforms under section 101K of the Securities and Futures Ordinance (Cap. 571).

Sharing of information otherwise than on designated platform

60. The Legal Adviser to the Bills Committee has expressed concern on what factor(s) MA would take into account in approving AIs to make a disclosure request or a disclosure otherwise than on a designated platform as referred to in the proposed new sections 68AAB(4)(a), 68AAC(6)(a) and 68AAD(5)(a) of BO; and whether such factors would be provided for in the guidelines to be issued by MA by notice published in the Gazette or in another way that MA considers appropriate under the proposed new section 68AAL(1) of BO.

61. The Administration has advised that it is envisaged that there may be circumstances where it is necessary or expedient for AIs to share information other than via a platform designated under the proposed new section 68AAM(1) of BO. For instance, an AI that has access to a designated platform may wish to disclose information to another AI that has no access to the designated platform for the purpose of alerting the latter of possible prohibited conduct. In such cases, MA will liaise with the AIs concerned to ensure secure transmission and processing of information as appropriate. MA will issue guidelines under the proposed new section 68AAL of BO to set out the relevant procedures and considerations.

Proposed enforcement provisions

62. As stated in paragraph 3.20 of the Consultation Conclusions issued by HKMA, HKMA intends to include enforcement provisions in the legislative amendments in relation to requirements for AIs to keep shared information confidential and to have adequate systems and controls. The

Legal Adviser to the Bills Committee has enquired what "enforcement provisions" that HKMA intends to refer to (e.g. provisions imposing offences or liability for damages), and how this legislative intent has been reflected in the Bill.

63. HKMA has advised that while the proposed new Part XIIAA of BO does not carry any explicit enforcement provisions considering the voluntary nature of the proposed information sharing mechanism, there are appropriate measures to provide adequate safeguards to the information shared under the proposed mechanism. Specifically, the Bill stipulates that AIs can only disclose or use relevant information for detecting or preventing prohibited conduct, and the information will only be disclosed via secure channels. If an AI fails to comply with the conditions, the AI will lose the protection of the safe harbour. MA may also revoke its approval for the AI concerned to participate in the information sharing mechanism, or take other supervisory actions as provided for in other parts of BO (e.g. requiring the AI concerned to submit reports prepared by auditors under section 59 of BO for providing an assessment of the adequacy of the AI's systems of control).

Drafting issues

64. Members have suggested amending the term "轉傳" in the heading of the proposed new section 68AAD of BO to more accurately reflect the meaning of its English equivalent "onward disclosure" (e.g. by changing it to "轉披露").

65. The Administration has advised that the English term "onward disclosure" is only used in the heading of the proposed new section 68AAD of BO, and is not used in its content. Under section 18(3) of Cap. 1, a section heading to any provision shall not have any legislative effect. According to the drafting conventions in Hong Kong, a section heading should succinctly and accurately set out the content of the provision. Having considered the above principles, the term "轉傳" is a suitable equivalent of the English term "onward disclosure" in the relevant section heading.

66. Members have questioned whether "記錄" in the proposed new section 68AAI(5)(b) of BO should be amended as "紀錄". The Administration has advised that it will propose a committee stage amendment to replace the term "記錄" with "紀錄" in the proposed new section 68AAI(5)(b).

67. Members have suggested whether "JFIU officers" and "designed platform operators" in the heading of the English text of the proposed new

section 68AAJ of BO should be changed to "officer" and "operator" (i.e. in singular form) to better align with the references in the proposed new section 68AAJ(2) and (3) of BO, and to enhance consistency with the expression of the proposed new section 68AAF(2) of BO.

68. The Administration has highlighted that according to the drafting conventions in Hong Kong, English provisions are generally drafted in singular form, so as to avoid the provisions being interpreted as applicable only to circumstances where the plural form applies. One of the exceptions is the headings of provisions. A heading seeks to succinctly and generally summarize the gist of the provision, rather than to point to any particular person or thing. The heading of the proposed new section 68AAJ in the English text follows this principle, and the way it is drafted is in line with other new sections proposed by the Bill (e.g. the proposed new section 68AAB refers to an "authorized institution" in singular form, whereas the plural form "authorized institutions" is used in the heading in the English text).

Amendments to the Bill

69. Apart from the amendment mentioned in paragraph 66 above, the Administration will also propose another textual amendment to the Bill. The Bills Committee has considered the draft amendments and raised no objections. The Legal Adviser to the Bills Committee has not identified any difficulties relating to the legal and drafting aspects of the draft amendments. The Bills Committee will not propose any amendments to the Bill.

Consultation with the House Committee

70. The Bills Committee reported its deliberations to the House Committee on 16 May 2025.

Council Business Divisions
Legislative Council Secretariat
30 May 2025

Appendix 1

Bills Committee on Banking (Amendment) Bill 2025

Membership list

Chairman	Hon CHAN Chun-ying, BBS, JP
Members	Hon Robert LEE Wai-wang Hon CHAN Hok-fung, MH, JP Hon Carmen KAN Wai-mun, JP Dr Hon TAN Yueheng, JP (Total：5 members)
Clerk	Ms Joyce KAN
Legal Adviser	Mr Mark LAM

Appendix 2

Bills Committee on Banking (Amendment) Bill 2025

List of organization that has submitted views to the Bills Committee

1. China Dream Think Tank