HONG KONG MONETARY AUTHORITY
香港金融管理局

Conclusions of the Public Consultation on a Proposal for Information Sharing among Authorized Institutions to Aid in Prevention or Detection of Crime

September 2024

Contents

1. Introduction

1.1. This document summarises comments received in a public consultation on the Hong Kong Monetary Authority's (HKMA) proposals for information sharing among Authorized Institutions (AIs) to aid in the prevention or detection of crime and the HKMA's responses, and sets out the next steps with regard to the proposals.

2. Background

2.1. The HKMA issued a consultation document on 23 January 2024 to seek views from the banking sector and the public on proposals to facilitate sharing of information among AIs[1] of information on customer accounts (including personal customers) for the purposes of preventing and detecting crime. The aim of the proposals is to help protect bank customers and the banking system against abuse for fraud, money laundering and terrorist financing (ML/TF). The consultation document can be viewed at the HKMA website[2].

2.2. The consultation closed on 29 March 2024 and 18 separate responses were received from individual AIs, industry and professional associations, public sector and law enforcement agencies (LEAs), companies active in data and analytics or provision of data-sharing platforms, law firms, technology service providers and members of the public.

2.3. Eleven of the respondents explicitly supported the proposal, with the others offering comments and suggestions on implementation, which were generally supportive or neutral. Ten respondents provided answers to all or some of the specific questions asked in the consultation paper while others provided views on specific areas. The names of the respondents are listed in the Annex.

[1] Institutions authorized in Hong Kong under the Banking Ordinance.

[2] https://www.hkma.gov.hk/media/eng/regulatory-resources/consultations/Consultation_on_AI-AI_info_sharing_en.pdf

3. Main comments received and HKMA responses

3.1. Responses were generally supportive, although some respondents, in particular Government agencies, provided comments relevant to implementation rather than directly supporting the proposal. No respondents explicitly opposed the proposal. All respondents who directly answered question 2[3] in the consultation paper agreed that AIs sharing information for the purposes of preventing and detecting crime should be given legal protection.

Scope

3.2. One respondent suggested including proliferation financing (PF) in addition to fraud and ML/TF. The HKMA has no objection to this, while noting that PF cases are likely to be relatively rare when compared with other crimes, especially fraud. PF is also covered in comparable overseas regimes, notably that of Singapore. We will therefore include PF in the draft legislative amendments to implement the proposal.

3.3. The same respondent also suggested that the scope should include financial crime, defined as all crimes that constitute predicate offences for ML, rather than being restricted to fraud and ML. We agree with this point. While fraud is currently the most serious and prevalent form of financial crime in Hong Kong, the intention is that the proposed information-sharing regime should cover all types of crime that generate criminal proceeds to be laundered, in addition to TF and PF. This will be made clear in the proposed legislative amendments.

Voluntary vs. mandatory

3.4. The majority of respondents who commented on the issue agreed that information sharing should be voluntary. However, one respondent favoured a mandatory approach on the grounds that "*AIs play an integral part in the financial ecosystem especially in terms of supporting crime*

[3] Question 2 in the consultation paper referred to "Do you agree that AIs disclosing information under such an arrangement should be given legal protection, provided they share information solely for the purpose of preventing or detecting financial crime?".

prevention.". The respondent also felt that "*AIs should work together in obtaining any requisite consent from their customers…*". Another respondent said that, given that sharing would be "merely voluntary", it was not clear that it would make identification and trace of illicit funds more effective than obligatory filing of suspicious transaction reports (STRs). Other respondents favoured voluntary sharing "initially" with the possibility of making it mandatory later.

3.5. One respondent said that regulators should "affirmatively encourage" AIs to participate and that "*The ideal approach would be to make participation mandatory…*". Another respondent, while agreeing to voluntary sharing, suggested that AIs should be encouraged to participate with incentives such as public recognition and allowing AIs to use information on their performance in successfully disrupting criminal activities in their marketing. The same respondent said that "*On balance, making this voluntary is likely to improve the implementation…*" and that mandatory sharing would add to the compliance burden of AIs, while noting that participation in some overseas regimes where sharing was not incentivised had been less than hoped for.

3.6. Given that most respondents, including those from the banking industry, favour voluntary sharing, the HKMA does not propose to impose a statutory obligation on AIs to share information. As noted in paragraph 5.12 of the consultation document, we believe this is more appropriate between private sector institutions, in contrast to the legal requirement to report suspicious transactions to LEAs. There is also a concern that a mandatory approach would be likely to lead AIs to share information in every case where the obligation could be triggered. This could generate large volumes of low-value STRs, which would work against the overall objective of improving the quality of STRs and intelligence in the system.

3.7. However, noting that a significant minority of respondents either favour mandatory sharing or some form of encouragement for AIs to participate, we will consider issuing guidance to the industry on when information sharing is appropriate and encouraging participation. The HKMA will also monitor use of designated platforms and may intervene

in the course of supervisory work if AIs are found not to be participating actively.

Scope of information to be shared

3.8. One respondent suggested including digital footprint information in the scope of information to be shared. Another considered that there should be no statutory limitations on the information to be shared since crime typologies change rapidly, while another stated that information shared should be kept to a minimum "*with regard to the type of action that is documented as suspicious criminal activity*". Another respondent suggested that information on victims of financial crime should be specifically excluded.

3.9. We agree that there is a need for a degree of flexibility in the types of information to be shared, which will vary depending on the circumstances of individual cases. The list in paragraph 6.1 of the consultation document was intended to be illustrative rather than exhaustive and we do not intend to impose statutory limitations on the types of information that may be shared. That said, we agree that information shared should be limited to what is relevant and necessary to achieve the purposes of preventing and detecting crime. This will be made clear in the proposed legislative amendments and guidance to the industry.

Relationship with the STR regime

3.10. There was general agreement that information sharing among AIs should not constitute "tipping off" (disclosing that an STR has been filed) under the relevant legal provisions. We will include a provision to this effect in the legislative amendments.

3.11. One respondent stated that the proposed information-sharing arrangement should be seen as complementary to the STR regime, which is in line with our intention. Another suggested that the HKMA should encourage joint STR filings by AIs. We agree there may be scope for collaborative STR filing and will consider this further with the banking sector and the Hong Kong Police Force (HKPF).

3.12. One respondent suggested that the consent status, i.e. whether an authorized officer has given consent for the AI to deal with property believed to be the proceeds of crime under relevant legal provisions, should be included in the information to be shared. We have consulted the HKPF, who do not support this suggestion given that, where consent has been granted, it would only apply to the AI to which it is given and not to AIs receiving information. In addition, the consent status is dynamic and could change as new information surfaces. This could lead to confusion and additional workload if the updated consent status has to be shared again. We therefore do not intend to adopt this proposal.

Safeguards

3.13. There was general agreement on the need for safeguards. Multiple respondents stressed the need for clear rules and guidance surrounding the circumstances in which information may be shared. The HKPF suggested that only authorized officers[4] and AIs should have access to information on designated platforms. One respondent suggested that information should attract the same level of protection at the receiving AI as at the originating AI. Other respondents suggested defining a maximum retention period for shared information and arrangements for deletion of information in cases which turned out to be false positives. One respondent supported giving customers an avenue to appeal.

3.14. The purposes for which and circumstances under which information may be shared will be clearly set out in the legislative amendments, supplemented by statutory guidance issued under the Banking Ordinance. There will also be positive obligations to maintain the confidentiality of shared information. We will consider further and discuss with stakeholders the points about maximum retention periods, treatment of false positives and victim data.

[4] i.e. authorized officers for the purpose of receiving STRs filed under relevant legal provisions. In practice, this refers to the Joint Financial Intelligence Unit (JFIU).

3.15. One respondent sought clarification on whether data shared via the Financial Intelligence Evaluation Sharing Tool (FINEST)[5] platform would be seen by the HKMA and HKPF. Both the HKMA and HKPF currently have access to FINEST and this would continue following the legislative amendments. Information on FINEST is invariably the subject of STRs filed by disclosing AIs. In many cases, receiving AIs will post information in their turn and also file STRs. In some cases, for example where posting on FINEST is a matter of urgency to facilitate the interception of funds, there may be a gap between posting and filing the STR. Since this information is likely to be relevant to ongoing investigations, we intend to include a provision giving the HKPF (in practice, the JFIU) access to cover any gaps. The HKMA's access will be for analytics and any necessary supervisory action.

Personal data privacy

3.16. The Office of the Privacy Commissioner for Personal Data (PCPD) provided a number of general observations from the perspective of protection of personal data privacy under the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO).

3.17. With reference to Data Protection Principle (DPP) 3 of Schedule 1 to the PDPO, the PCPD noted that personal data shall not be used (including disclosure or transfer) for a purpose other than the original purpose of collection or a directly related purpose, unless prescribed consent of the relevant data subject has been obtained, or any of the exemptions under Part 8 of the PDPO is applicable. To the extent that the exemption relating to the prevention or detection of crime, etc. under section 58 of the PDPO is relevant, the burden of proof is on AIs as data users to properly invoke the exemption and justify for each case that the non-disclosure of personal data to other AIs would likely prejudice the purposes of the prevention or detection of crime (or any other purposes referred to in section 58 as the case may be). Also, in making any disclosure and/or transfer of personal data, it is for AIs to assess and justify

[5] FINEST is a platform for sharing information on bank accounts, where crime is suspected. The pilot phase was launched on 20 June 2023. Currently, FINEST only covers information on corporate accounts suspected to be involved in fraud.

in each case the scope and extent of information sharing necessary for attaining the intended purpose.

3.18. The PCPD suggested that the HKMA provides guidance to AIs with respect to the maximum retention period for AIs to retain the customer information, received under the proposed information-sharing arrangement to take heed of DPP2(2) of Schedule 1 to the PDPO.

3.19. To ensure that the proposed information sharing is conducted via secure channels, the PCPD also recommended the HKMA and AIs to constantly review the technology deployed to ensure that personal data is securely kept against any unauthorized or accidental access, processing, erasure, loss or use in accordance with DPP4 of Schedule 1 to the PDPO.

3.20. The HKMA welcomes the PCPD's comments. It is the HKMA's policy intent to include specific provisions on the circumstances in which information, including personal data, may be shared in the legislative amendments, supplemented by statutory guidance issued under the Banking Ordinance. AIs will be expected to ensure that the relevant requirements are met in each case and to be able to demonstrate the grounds on which decisions are made. It is also the HKMA's intention 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. We also intend to restrict data subjects' access to specified data to guard against the risk of alerting criminals to the fact that their activity has been noticed. We will keep the technological aspects of platforms used for information sharing under regular review and consider the need for a maximum period for data to be retained.

3.21. The HKMA is continuing discussions with PCPD on the interaction between the proposed legislative amendments and the operation of the provisions of the PDPO.

Technical matters

3.22. A number of respondents made suggestions with regard to technical and operational aspects of the proposed information-sharing arrangement. These included the possibility of leveraging data from credit reference

agencies, and restricting access within AIs to minimise the possibility of data leakage. We will review all of these suggestions with relevant stakeholders and consider including them in the legislative amendments and/or statutory guidance as appropriate.

4. Next steps

4.1. The proposed amendments will be taken forward as part of an overall review of the Banking Ordinance and will be included in a Bill to be introduced into the Legislative Council tentatively in 2025. In the meantime, the HKMA is engaging stakeholders, including the PCPD, the banking sector and the HKPF, on practical matters relating to implementation of the proposals.

Annex - List of respondents

(in alphabetical order)

1. Clifford Chance
2. Consumer Council
3. Dun & Bradstreet
4. Financial Crime Intelligence and Insights
5. FinTech Association of Hong Kong Limited
6. Global Coalition to Fight Financial Crime
7. Hong Kong Police Force
8. Hong Kong Professionals and Senior Executives Association
9. LexisNexis
10. Office of the Privacy Commissioner for Personal Data
11. The DTC Association
12. The Hong Kong Association of Banks
13. Toronto-Dominion Bank
14. TransUnion Limited

Three respondents are individuals.

The name of one other respondent is withheld from disclosure at its request.