GIBSON DUNN

Hong Kong Monetary Authority Consults on Information Sharing Among Authorized Institutions to Prevent Financial Crime

Client Alert | February 21, 2024

The proposed information sharing system will help to bring Hong Kong in line with global trends and enhance the effectiveness of its mechanisms to combat fraud, money laundering and terrorist financing. On January 23, 2024, the Hong Kong Monetary Authority ("**HKMA**") published the "Public Consultation on a Proposal for Information Sharing Among Authorized Institutions to Aid in Prevention or Detection of Crime" ("**Consultation Paper**").[1] In short, the Consultation Paper proposes to facilitate information sharing among Authorized Institutions ("**AIs**") in respect of personal bank accounts for the purpose of preventing or detecting fraud or money laundering and terrorist financing ("**ML/TF**"). The proposal also considers the introduction of legislative amendments to provide "safe harbor" protection to AIs which share information for the purposes of preventing or detecting fraud or ML/TF, provided the AIs comply with appropriate safeguards. **I. Why encouraging information sharing between AIs?** While information sharing among AIs and law enforcement agencies has been successful in combatting a wide range of financial crimes, the HKMA recognizes that such arrangements may not, by themselves, be sufficient to fully address the risk of ML/TF via networks of accounts maintained or controlled by criminals (commonly referred to as "**mule account networks**"), since information might not be shared quickly enough to intercept illicit funds. Delays in information sharing provides an opportunity for criminals to exploit information gaps between AIs to rapidly move and conceal illicit funds. For example, by the time one AI has frozen the accounts maintained or controlled by criminals, those responsible may have already succeeded in moving their illicit funds to their mule accounts in another AI, which the first AI may not be able to quickly alert. Therefore there has been a global trend towards encouraging information sharing among financial institutions to combat crime and related ML/TF. In Hong Kong, participating AIs can share information on corporate accounts with one another through the Financial Intelligence Evaluation Sharing Tool ("**FINEST**") launched in June 2023. However FINEST currently does not support information sharing on personal accounts due to concerns over data privacy. The Consultation Paper points out that FINEST's ability to prevent and detect crime would be enhanced if information sharing were extended to personal accounts because a significant portion of mule account networks involve bank accounts held by individuals. As such, the importance of safeguarding data privacy and customer confidentiality should be balanced against the need for information sharing among AIs to detect or prevent crime and facilitate the interception of illicit funds. **II. What is the effect of the "safe harbor"?** The HKMA proposes to introduce legislative amendments to provide "safe harbor" protection to AIs which share information on personal accounts with other AIs solely for the purposes of preventing or detecting fraud or ML/TF. The "safe harbor" would provide AIs with legal protection from breach of legal, contractual or other restrictions on disclosure of information, and AIs also will not be held liable for claimed loss arising out of disclosures made. However the "safe harbor" will only apply if the AI complies with the safeguards discussed below. **III. What is the scope of information that could be shared between AIs?** While the scope of information to be shared will vary on a

Related People

William R. Hallatt

Arnold Pun

case-by-case basis, the Consultation Paper proposes that it could generally include:

- Bank account numbers;
- Personal data (e.g. name, date of birth, identity card number) of a customer or counterparty who is a natural person;
- Personal data of any beneficial owners or connected party (e.g. a director, partner, or trustee, as applicable) of a customer who is a legal person, a trust, or a legal arrangement similar to a trust;
- Personal data of any person purporting to act on behalf of a customer (e.g. acting under power of attorney, or an account signatory);
- Details of relevant transactions including counterparties;
- Reasons why the transactions or activity may be involved in fraud or ML/TF.

IV. Is information sharing mandatory or voluntary? Under the proposed system, information sharing by AIs will be made by participating AIs on a voluntary basis. **V. Will changes be made to the STR regime?** The HKMA proposes to introduce a legislative provision that will make clear for the avoidance of doubt that information sharing among AIs under the proposed arrangements will not constitute the offence of "tipping off" under the Organized and Serious Crimes Ordinance (Cap. 455) ("**OSCO**") and the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405) ("**DTROP**").[2] The obligation to file STRs will remain unchanged. **VI. What safeguards will be implemented?** The HKMA recognizes the importance of protecting the data privacy and customer confidentiality of legitimate customers. The HKMA therefore proposes that the "safe harbor" should only apply where appropriate safeguards are complied with, as summarized below:

- The information is shared solely for the purpose of detecting or preventing financial crime;
- AIs receiving information are required to treat it in the same manner, and to the same standards of confidentiality, as other confirmation information;
- Onward sharing of information received by an AI to another AI is only permitted if is for the purpose of detecting or preventing financial crime, and subject to the same requirements regarding confidentiality;
- Information sharing will only be permitted via secure channels such as FINEST (and AIs will need to demonstrate that they are technically and operationally ready and have implemented appropriate systems and controls in order to be permitted to access such platforms);
- An AI should only request for information from another AI where the requesting AI has reasonable grounds to believe that the other AI is able to provide information which will assist with preventing or detecting financial crime (including in deciding whether to file an STR);
- To prevent "fishing expeditions," requests for information must be specific and identify the subject of the request, relevant transactions and reasons for suspecting that an activity is connected with financial crime;
- Sharing of information will be on a need-to-know basis, i.e. an AI will only be permitted to request or disclose information where they have observed suspicious activity that may indicate that a person, account or transaction may be involved in fraud or ML/TF;
- AIs need to adopt a risk-based approach with respect to information shared under the "safe harbor", e.g. AIs should not terminate a customer relationship merely because the customer is included in information shared or requested (instead, an AI should always conduct its own risk assessment before deciding on the appropriate action to take).

The HKMA proposes to set out the specific requirements in the legislative amendments and the HKMA will also issue statutory guidance setting out its expectations on complying with the relevant requirements. The information sharing mechanism would be supervised by the HKMA, and the HKMA proposes to have the power to impose penalties on AIs that fail to comply with the relevant requirements. **VII. Conclusion** The proposed information sharing system will help to bring Hong Kong in line with global trends and enhance the effectiveness of its mechanisms to combat fraud and ML/TF. The HKMA notes that the United States, United Kingdom and Singapore have already introduced legislation to allow financial institutions to share information concerning individuals and entities where financial crime is suspected. While the specific requirements under each jurisdiction differs, they all provide a safe harbor for financial institutions which disclose information where financial crime is suspected. The HKMA aims to issue its consultation conclusions and prepare the necessary legislative amendments in the second half of 2024. Interested parties are encouraged to provide feedback by March 29, 2024. _____ [1] Available at: https://www.hkma.gov.hk/media/eng/regulatory-resources/consultations/Consultation_on_AI-AI_info_sharing_en.pdf. [2] Under section 25A(5) of OSCO and DTROP, a person commits an offence if, knowing or suspecting that an STR has been filed, the person discloses to another person any matter which is likely to prejudice any investigation which might be conducted following the filing of the STR.

The following Gibson Dunn lawyers prepared this client alert: William Hallatt, Arnold Pun, and Jane Lu*.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. If you wish to discuss any of the matters set out above, please contact any member of Gibson Dunn's Global Financial Regulatory team, including the following members in Hong Kong and Singapore: William R. Hallatt – Hong Kong (+852 2214 3836, whallatt@gibsondunn.com) Grace Chong – Singapore (+65 6507 3608, gchong@gibsondunn.com) Emily Rumble – Hong Kong (+852 2214 3839, erumble@gibsondunn.com) Arnold Pun – Hong Kong (+852 2214 3838, apun@gibsondunn.com) Becky Chung – Hong Kong (+852 2214 3837, bchung@gibsondunn.com) **Jane Lu is a paralegal (pending admission) in the firm's Hong Kong office who is not yet admitted to practice law.*

Related Capabilities

Financial Regulatory

Financial Institutions