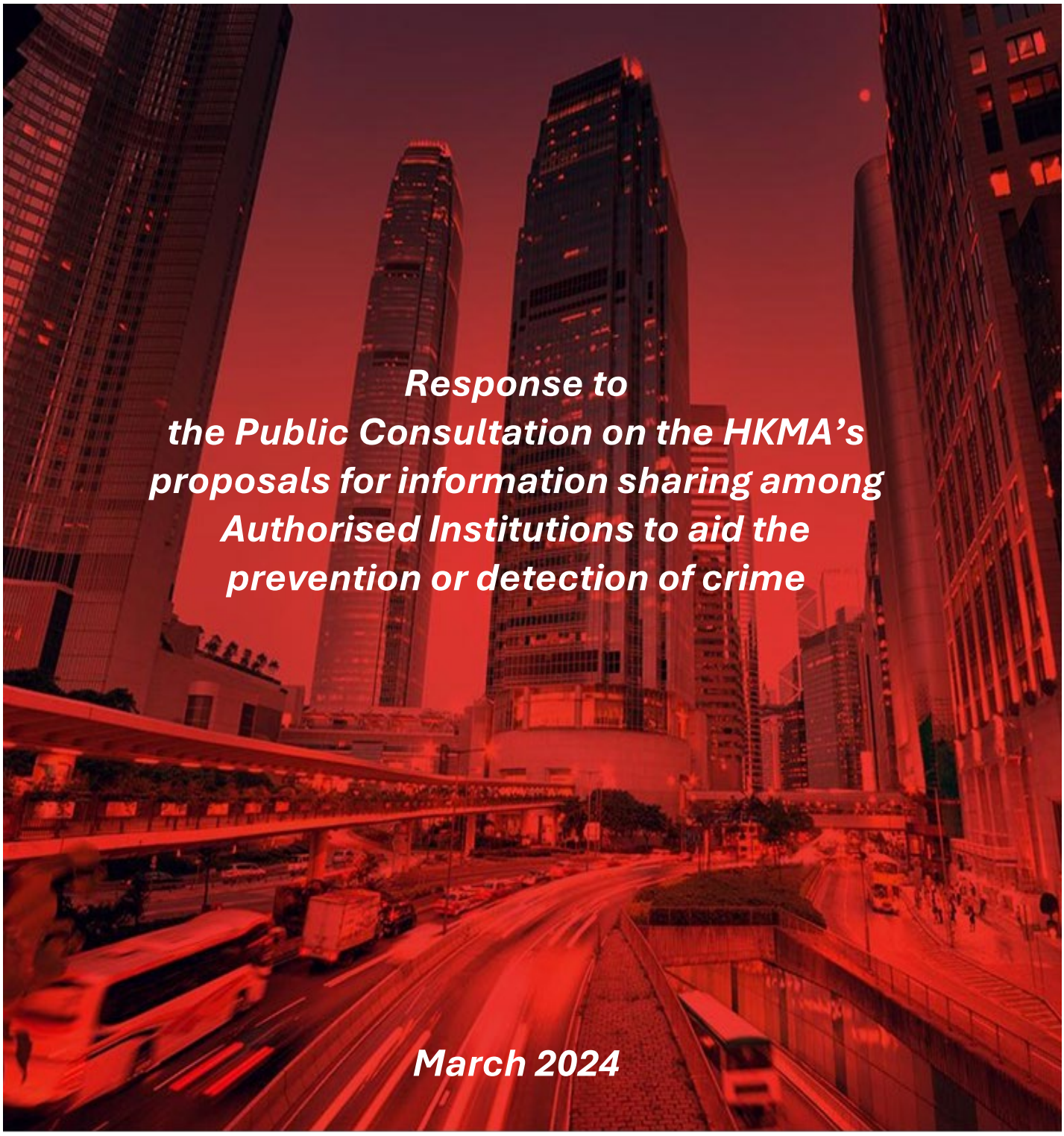
FINTECH ASSOCIATION OF HONG KONG

FINTECH ASSOCIATION OF HONG KONG LIMITED
(Incorporated in Hong Kong as a company limited by guarantee)
(the "Association" or "FTAHK")
Company No.: 2534398
www.ftahk.org



Response to the Public Consultation on the HKMA's proposals for information sharing among Authorised Institutions to aid the prevention or detection of crime

March 2024

Address: 23/F, One Island East, 18 Westlands Road Quarry Bay, HK

FINTECH ASSOCIATION OF HONG KONG

FINTECH ASSOCIATION OF HONG KONG LIMITED
(Incorporated in Hong Kong as a company limited by guarantee)
(the "Association" or "FTAHK")
Company No.: 2534398
www.ftahk.org

The FinTech Association of Hong Kong (FTAHK) is a **member-driven, independent, not-for-profit, & diverse organisation** that is the voice of the FinTech community in Hong Kong. It is organised and led by the community, for the community, through a series of committees and working groups.

Our objective is to promote Advocacy, Communication and Education in the wider FinTech ecosystem.

Build the community.
Be the connector.

FINTECH ASSOCIATION OF HONG KONG LIMITED
(Incorporated in Hong Kong as a company limited by guarantee)
(the "Association" or "FTAHK")
Company No.: 2534398
www.ftahk.org

The FinTech Association of Hong Kong ("**FTAHK**") welcomes the continued endeavours of the Hong Kong Monetary Authority ("**HKMA**") to enhance the measures in place to prevent and/or detect financial crime, and further strengthen Hong Kong's position as an international finance centre of repute.

The FTAHK is a not-for-profit ecosystem builder that has over 1,100 members and is the largest independent FinTech association in Asia. Our wide-ranging membership comprises of global and domestic FinTechs, Financial Institutions, Technology Service Providers, Consultancies, and members of Academia. We are grateful to have the opportunity to respond to this public consultation, the scope of which is focused on the sharing of information relating to non-corporate accounts, with a view to combatting financial crime by targeting related money-laundering.

This response has been prepared in consultation with FTAHK members representing a broad range of experience and backgrounds. Overall, our response draws on the following two themes for the consideration of the HKMA:

(1) Limited purposes for which information is (a) to be shared; and (b) to be used.

The FTAHK is generally supportive of this initiative, noting that effective information sharing is one of the foundations of a well-functioning anti-money laundering ("**AML**") and counter-terrorist financing ("**CTF**") framework. We agree with the stance of the HKMA that information sharing plays a vital role in allowing financial institutions and supervisory and law enforcement authorities to better deploy resources on a risk-based approach to combat money laundering and/or terrorist financing. We also note that this initiative of the HKMA is in-line with similar efforts made in other international financial centres[1].

As recognised by the Financial Action Task Force in its 2017 report on private sector information sharing[2], a key issue to be addressed in respect of information sharing is the legal constraints around data protection and privacy across jurisdictions (a data-minimalist approach), and the balance of these the significant national and public security interests of AML/ CTF goals (a data-maximalist approach).

[1] As examples, see the work of the Financial Crimes Enforcement Network (FinCEN) in the United States and the administration of the provisions of the Bank Secrecy Act; and the AML and CTF frameworks within the EU which require reporting of suspicious transactions, implementation of customer due diligence procedures and information-sharing with competent authorities.
[2] See: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf.coredownload.pdf

The FTAHK recommends that the scope of information that is shared amongst authorised institutions ("**AIs**") is kept to a minimum, with regard to the type of action that is documented as suspicious criminal activity, and also with reference to an AIs capability with respect to fraud detection: without the necessary tools, technologies and processes to support secure and beneficial data sharing, such an exercise may be seen to "lack teeth". We agree with the HKMA's position that information sharing only be permitted among AIs and, only then, for the purposes of detecting or preventing financial crime.

To facilitate this, we recommend the HKMA establish clear guidance for AIs to assist them in understanding whether a situation warrants any form of information sharing, (i.e., establishing whether there a strong legal and documented basis for a suspicious transaction meeting the threshold of a potential crime prior to sharing any information) and look to adopt similar standards, systems and controls as those adopted in other international financial centres in relation to when information can be shared, the types of information that can be shared, how any such information is then handled and how long it is retained.

We note that, whilst the information measures will be designed to flag those transactions that are suspicious in nature, not all flagged transactions will actually be determined as suspicious (i.e., a false positive finding). In these instances, we recommend measures be implemented for the full deletion of any such data for unsubstantiated cases, upon notification no longer suspicious or in the absence of confirmation of a case, after a specific period of time.

Relatedly, the FTAHK is also of the view that the HKMA mandate that AIs update their privacy notices and disclosure statements, explaining that information may now be shared amongst AIs for AML/CTF purposes. This, together with any awareness raising exercises undertaken by the HKMA (e.g., seminars, online resources, workshops on privacy rights, data protection and the importance of fraud prevention measures) may serve to allay any public concerns around the proposed information-sharing measures. We also recommend the HKMA consider including an individual's right to access any such data under the Personal Data Privacy Ordinance (whether the access is by an individual themselves, or by the HKMA) as part of a complaint investigation, particularly in instances where an individual has alleged that the basis of being denied *bone fide* banking services is linked to a prior instance of information sharing between AIs.

(2) Proposed legal protections for AIs sharing information

As provided above, we believe it prudent for the HKMA to provide (i) detailed guidance on the situations that warrant information sharing between AIs (i.e., a strong legal and documented basis for why an account or transaction has been flagged as suspicious *prior to* any

information sharing); and (ii) the protocols around the handling and management of any such information. An example can be seen in the United States, where Section 314(b) of the Patriot Act requires firms to safeguard any shared information, and only to use information in limited circumstances, i.e., (i) identifying and/or reporting on activities that may involve terrorist financing or money laundering; (ii) determining whether to establish or maintain an account or engage in a transaction; or (iii) assisting in compliance with AML requirements.

We also recommend that any guidance require strict separation of data from instances of information sharing from the normal banking data that is held by an AI on a customer – in an instance where a suspected transaction does not amount to criminal activity, this data separation would contain the risk of inappropriately flagging legitimate transactions from other banking customers or denying services to *bone fide* customers with a false positive flag.

Provided that any information-sharing between AIs is conducted in limited instances/ for a limited purpose, the FTAHK agrees with the position of providing legal protection to those AIs that engage in information sharing. We recommend that the in addition to the proposed guidance on systems and controls for handling information, the HKMA also specify that staff who may be involved in information sharing undergo training on the limited use-case(s) for information to ensure that data privacy rights of individuals are respected to the greatest extent possible.

As a final comment on "tipping off", we agree that AIs are likely to need protection from the criminal risk of "tipping off", and we recommend that any such protections be developed in conjunction with the relevant law enforcement divisions to ensure a balance between the various legal regimes.

Conclusion

In conclusion, the FTAHK supports the proactive approach taken to further protect the interests of legitimate banking customers in Hong Kong. We trust that this Response will be received in the constructive way it is intended, and we are open to any further discussion on any aspect of the above, as may be required.

FTAHK
27th March 2024
https://ftahk.org