Submission of the Global Coalition to Fight Financial Crime regarding the Public Consultation on a Proposal for Information Sharing among Authorized Institutions to Aid in Prevention or Detection of Crime

28 March 2024

The Global Coalition to Fight Financial Crime is a public-private coalition with the aim of enhancing the fight against financial crime globally

1. Introduction

We, The Global Coalition to Fight Financial Crime, established in 2018, are a public and private international NPO member organization, with more than 30 members from public, private and third sectors, committed to improving the fight against financial crime globally. We are also organized under regional chapters. This submission in response to the HKMA Consultation is made by the GCFFC APAC Chapter, with support from the global leadership of the GCFFC.

Since our inception, the GCFFC has advocated for (and continues to do so) increased collaboration and information sharing as a key tenet in improving the effectiveness in fighting financial crime. We also support maintaining privacy and data protection and recognize a balance has to be achieved and advocate for reasonable safeguards to be considered and for mitigating steps to be taken to address any potential for foreseeable albeit unintended consequences.

We note and support the measures Hong Kong has already taken to promote collaboration and information sharing, such as the 24/7 stop-payment mechanism operated under Anti-Deception Coordination Centre (ADCC) of the Hong Kong Police Force ("HKPF") since 2017, the public-private information sharing platform Fraud and Money Laundering Intelligence Taskforce (FMLIT) established in 2017, the HKMA AML Regtech Lab launched since 2021, the anti-fraud search engine "Scameter" operated by the HKPF launched in November 2022, the Financial Intelligence Evaluation Sharing Tool (FINEST) established in June 2023, the Anti-Scam Consumer Protection Charter launched in June 2023, the establishment of the Anti-Deception Alliance announced in November 2023 and The Office of the Communications Authority (OFCA) SMS Registration Scheme announced in December 2023. Many of these initiatives are in response to the growing challenges faced from digital fraud and scams, not only in terms of the numbers of victims but also the large billions of Hong Kong Dollar losses annually incurred by Hong Kong citizens but also the laundering of illicit funds through Hong Kong.

Hong Kong is one of the world's largest international and regional financial centres attracting capital and investment from mainland China and overseas, due not least to low crime and corruption rates, the safety and soundness of its banking sector and strong financial infrastructure. Whilst these factors attract capital and wealth, they also attract criminal syndicates from overseas. These syndicates aim to exploit the city's customers and financial system for illicit activities and thereafter quickly transfer funds scammed abroad. The Hong Kong government has stated its position clearly, for example in 2022, "*The Government is committed to ensuring that Hong Kong remains one of the world's safest and cleanest cities to work, do business and enjoy life*".

In response, the HKMA having confirmed tackling digital fraud and ML/TF are included in its strategic priorities for 2024 has now made a firm proposal. The proposal is to permit AI's in Hong Kong to share information on customers, accounts and transactions strictly for the purpose of preventing or detecting financial crime by allowing AIs to alert each other to potential fraud and ML/TF concerns, thus helping to protect bank customers from losses and the banking system from being abused for fraud, money laundering and terrorist financing. This proposal must be seen in the wider fraud, financial crime and ML/TF context, and after other measures have already been taken.

The GCFFC believes the proposal:

- is a necessary and proportionate response to the heightened fraud, financial crime and ML/TF threat faced by Hong Kong;
- is very likely to have a positive effect on preventing, detecting and reporting fraud financial crime and ML/TF, and
- is very unlikely to have material unintended consequences, for example unfair financial exclusion provided the scheme is designed and operated reasonably.

The remainder of this response addresses the questions raised in the consultation using the same numbers as is used in the Consultation proposal.

2. GCFFC's Response to the Consultation Questions

2.1 Why do AIs need to share information?

Q1 Do you agree that AI-to-AI information sharing as described in this consultation paper, could help facilitate the swift identification and tracing of illicit funds and so should be established in Hong Kong to support efforts to detect or prevent crime?

The sharing of information between AI's in Hong Kong, with safeguards and strictly for the purposes of fighting fraud, financial crime ML/TF is an important contributor to raising the level of effective system wide response, and in so doing protecting citizens and systems from abuse, including financial losses and other harms. In terms of being able to improve the system wide response, it should be recognized that single AI's see only a small piece of a bigger picture, not least as a result of the many more AI's that are licensed and alternative ways to send and receive payments than in the past, so information sharing is one way to increase the visibility of AI's and to then enable AI's to better discharge their AML/CTF obligations. It is also a way for AI's to gain context in assessing its customer and or transaction, if it also has additional information that bears on the customer or transactions received from another AI. In simple terms a single AI would find repeat account openings and transactions from/to new originators/beneficiaries as something to be investigated, and so criminals tend not to concentrate their activity with one AI, but throughout the financial system. Another example could be where one AI has identified a customer of genuine serious concern and closes that account, only for that customer to open an account at another AI immediately thereafter. Whilst information shared can facilitate the prevention, detection & reporting of fraud financial crime and ML/TF, it can also support asset seizures and asset tracing.

Q2 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?

AI's are subject to legal obligations to protect the confidentiality of their customers data, which would be infringed without such legal protection, as changing terms and conditions and seeking customer consent is unrealistic, particularly acquiring informed consent from customers that may be the subject of any such proposed information sharing. The struggle against illicit finance is often made more difficult by conflicts between firms' other compliance and legal obligations. Resolving this conflict by giving explicit legal protection to the arrangement, provided it is used for the established goals only, will remove a blocker to adoption in Hong Kong that many other countries' legislative frameworks still have not engaged with.

Additional legal obligations also exist which require legal protection so as not to generate potential conflicts of laws and or ambiguity. As these proposals for information sharing are voluntary, any remaining legal jeopardy will likely scupper the initiative.

Q3 Do you agree that AIs should be able to participate in such information sharing on a voluntary basis?

On balance, making this voluntary is likely to improve the implementation of the proposal, with those AI's that go first able to gain valuable experience before it becomes more widely accepted and used. Referring to the experience of the United States and Australia, we are of the view that AIs' participation should be encouraged and incentivized.

I. United States

Under the USA PATRIOT Act Section 314(b), financial institutions are permitted, upon providing notice to the United States Department of the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity. Such information sharing is voluntary, that is – financial institutions are permitted but not incentivized to share information. There is a noted lack of uptake from financial institutions as a result – BSA officers (AKA MLRO's) are not always able to advocate for opting in, as the "business case" is lacking. 314(b) participation comes with requirements, and costs additional compliance resources.

II. Australia

This is similarly noted in Australia in terms of the well-respected "FinTel Alliance," a public private partnership that entails larger players in the financial services field. The FinTel Alliance has had major wins against serious and organized crime and produced insightful intelligence products, but it cannot extend to every provider of financial services (and intelligence) in Australia as it is costly. This is again replicated in the newly established Australian Fraud Reporting Exchange ("AFCX"), which comes with specific undertakings to adhere to Service Level Agreements and is a costly endeavor. AFCX is an independent, not-for-profit organization that was formed by the four major Banks to assist businesses combat financial-related crimes. It operates independently of government, law enforcement and its members, although it is funded by its members. The AFCX has the support of the Commonwealth Attorney-General's Department and is a key limb in the Australian Government's National Organized Crime Response Plan.

The alternative of mandating information sharing, though, could be worse: imposing greater compliance burdens on financial institutions already encumbered with AML and fraud and other compliance and operational costs and concerns. Mandating information sharing between different regulated entities with no intermediary is, at the least, a sub optimal approach as data security, counterparty due diligence and customer privacy are all legitimate concerns of financial institutions, as is the potential use of the underlying information for unstated purposes.

As such, the GCFFC recommends adopting an approach of making participation optional, but encouraged and incentivized. Such encouragement could take the form of allowing participating institutions which stimy criminal efforts to use this information in targeted public relations and marketing campaigns, reduced levies and fees on the financial service sector, or public acknowledgement from regulatory bodies of firms' commitment to disrupting financial crime.

2.2 What information would be shared and how?

Q4 Do you have any comments on the scope of information to be shared for the purposes of preventing or detecting financial crime?

Consideration could be given to the following areas:

I. Suggest the scope to include Fraud, Financial Crime and ML/TF

The proposal refers to fraud and ML/TF, but we prefer the scope to include Fraud, Financial Crime and ML/TF. We suggest "Financial Crime" be defined by all crimes that are predicate offences to money laundering. We also suggest that "PF" also be included, and that sanctions and sanctions non-compliance be included. In terms of information to be shared, the proposal should focus less on prescriptively listing what can be shared, and more on providing a safe harbor against customer confidentiality and data protection obligations, as not all information that can be shared between AI's in connection with fraud financial crime or ML/TF investigations, is restricted. This could include for example information on non-customers or a customers' customer. A point to consider is the model in the UK as set out in Page 22 of the Proposal which limit's information sharing in the b) Economic Crime and Corporate Transparency Act 2023, to information the sender believes, will "assist (direct or indirect) recipients in relation to customer due diligence and determining risk-mitigating actions with regard to business relationships or products and services". We believe this unfortunately limits information sharing unnecessarily and in some cases is interpreted as "post suspicion information sharing", which is unfortunate and unhelpful as it then has potential consequences for the treatment if that information by the recipient.

II. Whether victim details should be specifically excluded from information sharing

This includes victims of crime (e.g. fraud) or those who have had their identities compromised (through ID theft or account takeover). Where it is not fully clear that a person or entity is actually involved (as opposed to, for instance, having their account compromised), an explicit requirement that this should be shared also should be considered to reduce the "contamination" of victims' reputations and the accidental 'co-mingling' of accounts controlled genuinely by a victim with accounts controlled by an impersonator.

III. Guideline should be provided on the "detail of relevant transaction(s) to ensure AI staff can input the relevant information by providing clear right annotation in the new platform

For example:

- Bank account transaction
- Credit card transaction
- Wealth Product Transaction
- Insurance Product Transaction

2.3 How will this affect the existing STR regime?

Q5 Do you agree that information sharing among AIs as described in this paper should not constitute "tipping off" under the relevant legislation?

The proposal limits the sharing of information from one Hong Kong AI to another. Both are subject to tipping off obligations and so the sharing of information should not of itself increase the risk of the customer, or other party being tipped off as a result. STR information should not be shared as that would amount to tipping off, and anyway relates to subjective judgements in underlying data and not "information" relevant for sharing. Nevertheless, the sharing itself between AI's should not legally constitute tipping off and if there is any risk that it might, then this potential legal jeopardy will scupper those who would otherwise likely be interested in this voluntary scheme.

In addition, the GCFFC submits that the legal protections extended to cover financial institutions should explicitly allow financial service firms to collaborate without tipping off – putting the issue "beyond doubt," as phrased, is ideal.

Q6 Do you have any other views on how the proposed information sharing arrangement should interface with the STR regime?

The information sharing and STR regimes should be kept entirely separate. Sharing STR filings is inappropriate, and information shared should be focused on the information on customers and transactions and not on the opinion of any other AI in relation to its assessment of that information. It follows that so called super STRs, referencing other STR's from other AI's etc are out of scope. Nevertheless, STRs filed based in whole or in part based on information on customers or transactions at another AI should be included and referenced in the STR narrative, in order to inform the JFIU.

2.4 Safeguards

Q7 Are the proposed safeguards appropriate?

Yes. This proposal is not a tradeoff between fighting fraud, financial crime ML/TF and customer confidentiality, as is often portrayed. A customer has a legitimate right to his/her financial affairs remaining confidential, because if made public or shared with third parties, intrude into the personal sphere of the customers private life, in the same way that third parties can't intrude into someone's home and take a look around. A person's financial activities reveals much about that person, their lifestyle and lifestyle choices and customers are entitled to have these protected from public state of third-party scrutiny. Where though an AI is proposing to share customer related data with another AI in the same jurisdiction, that is subject to the same obligations, there is no prospect that the customers data will become public or handed over to the state or to other third parties unless there is a lawful reason to do so, for example in case an STR is filed, in which case the wider interests of the public and fighting fraud, financial crime and ML/TF should rightly prevail.

In addition, we suggest HKMA to provide guidance via HKAB to see if the HKAB template of the Data Policy Notice will be revised.

Q8 Do you have any other suggestions for safeguards that may be imposed to protect the interests of legitimate customers?

For information that is subject to customer confidentiality protection at one AI, that is then shared with another AI, is customer information at the originator AI but not at the recipient AI. That information should though attract the same level of protection at the recipient AI as it does at the originator AI.

In addition, the HKMA have clearly considered carefully the desired outcomes of information sharing and possible secondary impacts such as "de-banking" or "de-risking." The consultation paper shares several good suggestions, such as the prevention of "fishing expeditions" or use of information exchange to essentially "tip off" other AI's who aren't reasonably expected to be involved with a customer. The adoption and supervision of a risk-based approach is sound. However AI's will need guidance on when and how they can, through careful and proper consideration, determine a customer relationship to present unreasonable risk as a result of information sharing. Put simply, industry will need to know how to handle this when offboarding is the best approach.

2.5 Other comments

I. Information sharing channel

Regardless of whether the HKMA choose to use the FINEST or another new platform for this information-sharing initiative, the HKMA should be aware that AI may require more time for in-depth analysis of the technical requirements and relevant system development to fulfill new data exchange protocol.

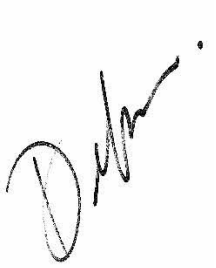
II. Mode of information sharing

We agree that the mode of information sharing would consist of two parts - (i) AIs request information from other AIs ("request and response") and (ii) AIs disclose information to alert other AIs ("push notification").

However, we suggest HKMA to provide further clarification on (i) the definition of "a person, account or transactions may be involved in fraud or ML/TF"; and (ii) the scenarios that AIs should share information through "request and response" or "push notification".

The GCFFC APAC Chapter welcomes the opportunity to provide its response to the HKMA consultation and looks forward to the proposals becoming operative in 2024 which would represent another important tool to add to the toolkit Hong Kong is using to tackle fraud, financial crime ML/TF and be an example to third countries and a path that others should follow.

Yours Faithfully



GCFFC APAC Co Chair Debra Au

GCFFC APAC Co Chair Jodie Arthur

GCFFC Chair John Cusack