Financial Crime Intelligence and Insights
111 Town Square Place, 14th Floor
Jersey City, New Jersey, 07310 USA

March 22, 2024

VIA Email: ai-to-ai-informationsharing@hkma.gov.hk
Hong Kong Monetary Authority
55/F, Two International Finance Centre
8 Finance Street
Central, Hong Kong

RE: Public Consultation on Information Sharing Among Authorized Institutions

To Whom It May Concern:

Financial Crime Intelligence & Insights, Inc. ("FCi²") appreciates the opportunity to comment on the Hong Kong Monetary Authority's Public Consultation on a Proposal for Information Sharing Among Authorized Institutions to Aid in Prevention or Detection of Crime.

FCi² is a wholly owned subsidiary of the Global Association of Risk Professionals, Inc. (GARP), the world's leading professional organization for risk managers, offering the Financial Risk Manager (FRM)® certification as well as the Sustainability and Climate Risk (SCR)® certificate globally. GARP also sponsors the GARP Benchmarking Initiative (GBI) which provides analysis and confidential reporting for over 100 financial institutions around the world on bank capital and other financial industry studies. FCi² was established in the United States to provide a secure automated information sharing hub for participating financial institutions to proactively identify and fight financial crime.

FCi² is dedicated to the use of advanced technology to provide insight into potential AML/CFT, fraud, sanctions, and cyber-crime activities through advanced peer-to-peer and public to private information sharing approaches and methodologies. Developed in consultation with law enforcement, FCi² 's work is intended to transform the fight against financial crime from reactive to proactive, exposing illegal activity at a much earlier stage of development, and providing more informed and almost immediate investigative results.

FCi² strongly supports the Hong Kong Monetary Authority proposing legislative amendments that would provide "safe harbor" protection to Authorized Institutions ("AIs") sharing information on customers, accounts, and transactions for the purpose of preventing or detecting fraud, money laundering, or terrorist financing, with appropriate safeguards in place to protect shared information. We commend the establishment of public-private partnerships by the HKMA, the Hong Kong banking sector and the Hong Kong Police Force which are essential in the fight against financial crime.

General Comments

Much of our response is premised on over three years of meetings and consultations on fighting financial crime with law enforcement and regulators in the United States, Canada, and Europe as well as with numerous financial institutions around the globe. We have focused on addressing the growing issue of how to fight financial crime more effectively in a world where bad actors are aggressively using technology and taking

advantage of current privacy and cross-border information sharing constraints on private sector players and law enforcement.

The United States has affirmatively encouraged information sharing among financial institutions and between law enforcement and financial institutions since enacting groundbreaking legislation in 2002. But the procedures for sharing developed at that time were built around then available technology. Incredible technological advancements have been made over the last twenty-two years, and bad actors have become much more sophisticated. The world is also much more connected and integrated. And the future will only see greater connectivity, larger information flows and instantaneous money movement everywhere around the world.

The effectiveness of any legislation, including that passed in the U.S. twenty-two years ago, and the benefits gained will rapidly diminish unless more is done to modernize both public-to-private and private-to-private approaches to information sharing. Avenues for quick but studied change must be built into any current or new information sharing initiatives. They must provide the ability to respond to an unanticipated, rapidly changing and interconnected global marketplace, technological advances, and an increasingly sophisticated criminal landscape.

Recommendations

As discussed in additional detail below, this proposal for peer-to-peer information sharing contemplates a structured voluntary exchange of information. This is a very positive step toward combating financial crime. But its voluntary approach may ultimately become an impediment to realizing the proposal's full intent as it may result in uneven participation, slow and potentially incomplete information sharing and suboptimal use. And an absence of regulatory incentives "encouraging" financial institutions to share information readily and efficiently with other financial institutions to detect and prevent financial crime, coupled with any lack of clarity about either the scope of information that can appropriately be shared or with which AIs or other institutions, may undermine its potential benefits.

To assist in detecting and/or preventing the furtherance of any criminal activity an AI will need to quickly alert other potentially affected AIs. AIs who observe activity that may indicate that persons, accounts, or transactions may be involved in fraud or ML/TF should quickly request and receive information from other AIs which they reasonably believe may be able to provide information that will shed light on potential fraud or ML/TF risks, or to alert other AIs that may be at risk of being targeted by criminals. A delay in providing the requested information which could result from a voluntary versus mandatory regime or lack of clarity on applicability, will do little to proactively prevent and detect financial crime or intercept illicit funds. This leaves law enforcement and AIs in a defensive position, undermines any proactive benefits contemplated by the proposal and reduces its positive objectives.

The changes proposed in the consultation are essential to addressing many of the information sharing issues noted above, and others, and should be welcomed by all. However, we respectfully recommend that as you decide on your approach that you consider the speed at which technology advances and create ways forward that are flexible enough to take advantage of innovation and technological advances, and which do not result in information sharing provisions that quickly become obsolete or present unintended barriers. The need to analyze data using such tools as machine learning and artificial intelligence given the amount of data that will need to be analyzed and how quickly funds flow between and among institutions and across borders will be important for any information sharing regime to be effective.

FCi² Response to HKMSA Public Consultation on a Proposal for Information Sharing Among Authorized Institutions to Aid in Prevention or Detection of Crime

Specific Responses to Questions Presented

Question 1.

We agree that AI to AI information sharing is essential to the swift identification and tracking of illicit funds and should be established in Hong Kong to help detect and prevent crime and address the issue of risk displacement. However, we would suggest that the institutions permitted to engage in information sharing for these purposes be expanded to include more than just AIs as defined in the consultation document.

While we understand the HKMA's authority under the Banking Ordinance extends to the Ordinance's defined list of authorized institutions, criminals use a variety of institutions other than deposit taking institutions to launder funds and conceal illicit activities, including casinos, insurance companies, crypto exchanges which have become important to movers of illicit funds across the blockchain, broker-dealers, investment advisors, credit card companies and others. By limiting information sharing to the defined list of AIs, Hong Kong's view into criminal activity will similarly be limited and its ability to detect and combat crime will be constrained. Bad actors will quickly take advantage of any system weaknesses and will move their illicit activities to areas where they can hide and where law enforcement finds it difficult to operate. Allowing non-deposit taking institutions to voluntarily take advantage of the safe harbour being considered may assist in closing this information gap.

Question 2.

We agree that AIs (and any other institutions that may be included as suggested above) disclosing information for the purpose of detecting and preventing financial crime should be given legal protection from liability. The safe harbour described in the consultation paper is consistent with the protections provided in other jurisdictions, including the United States. We believe that without such protections, many, if not all, institutions will refrain from sharing any personal information despite their desire to combat financial crime, for fear of being held liable for a breach of legal, contractual, or other obligations and any claimed losses resulting therefrom.

Additionally, we have seen that fear of litigation or liability resulting from alleged violations of privacy regulations or confidentiality obligations that relates to the disclosure of information often leads legal departments of institutions to read any permissive legislation very narrowly. It is less risky not to share information if there is any question as to whether the sharing of information falls within the scope of the safe harbour.

In the United States, for example, the rule provides a safe harbour for information shared relating to anti-money laundering or the prevention of terrorist financing. It does not explicitly provide for fraud. Although the Financial Crime Enforcement Network (FinCEN) clarified in a subsequent FAQ its intent to include fraud within the safe harbour, many banks still will not allow information relating to fraud to be shared absent a formal rule change.

We recommend that any safe harbour provision be written as clearly as possible to include all suspected criminal activity meant to be prevented and detected by the sharing of information, including fraud, money laundering, and terrorist financing.

FCi² Response to HKMSA Public Consultation on a Proposal for Information Sharing Among Authorized Institutions to Aid in Prevention or Detection of Crime

Question 3.

While we generally agree that voluntary information sharing among private institutions is preferable, what we have seen with voluntary information sharing, in those jurisdictions that have implemented such legislation, is that many eligible organizations do not participate in the information sharing regime. Their rationale may vary from, among other things, resource allocation, risk averseness, fear of regulatory scrutiny, or lack of awareness or incentives. Organizations also have differing levels of commitment to fighting financial crime. Some are passionate about it while others do not see the value vis-à-vis other internal initiatives vying for resources so do the minimum.

We've regularly found that when participation is voluntary, inquiries requesting information from another institution believed to have information that would be helpful to the inquiring institution's investigation of suspected illicit activity go unanswered, are answered in part, or are responded to too late to be helpful. There is little incentive for the institution being inquired of to respond to a request or to prioritize a request for information.

A solution may be for regulators to affirmatively "encourage" AIs to participate in a voluntary information sharing regime, to include their compliance in audit findings, and regard it as a customer protection measure.

Further, a technologically advanced approach could be considered, allowing for literally immediate information flows. In this scenario, every participating institution, irrespective of how they view their level of participation, would be linked technologically, and *required to timely respond* to any valid request made by any other institution that has volunteered to collaborate to fight financial crime. Essentially, once you're "in", you're committed to fully engaging with your activities being reviewed considering that commitment.

Regulatory incentives should be regarded as a major key to ensuring the success of a voluntary regime.

The ideal approach would be to make participation mandatory but ensure information requests are fully defined and controlled with automation encouraged to lessen any financial burden of compliance.

Question 4.

We agree that the scope of information shared for the detection and prevention of financial crime should be determined by the AIs, be as comprehensive as may be reasonably warranted and not proactively limited. We do not believe there should be statutory limitations imposed on the information permitted to be shared as crime typologies change rapidly. To have to change restrictive statutory or other rule-imposed limitations in response to those changes would be difficult and time consuming. Pre-defined limitations may also serve to delay sharing while internal approvals are sought at the responding AI to ensure only permissible information is shared. And there would likely also be differences in interpretation or risk tolerance, which would enable some AIs to share more than others, potentially resulting in information gaps relating to transactions or activities indicating fraud, terrorist financing or money laundering.

Question 5.

In the United States, if a financial institution suspects money laundering or terrorist financing activity, it may, as part of its internal investigation into that activity, make a Section 314(b) request to another financial institution who has registered with FinCEN to participate in the information sharing program[1]. If the other institution responds in a timely manner, the information obtained from such an inquiry may aid the investigation and allow for more a complete and accurate SAR (the equivalent of a STR) filing.

In the US, financial institutions are not permitted to disclose that a SAR filing has been made, however, they can share the same information contained within the SAR with other financial institutions, as appropriate. This does not constitute tipping off in the US. However, the prohibition against disclosing a SAR filing has had a chilling effect on financial institutions collaborating on joint SAR filings. Joint SAR filings would be beneficial to law enforcement because the information would be more encompassing and provide cost benefits to participating filing institutions. FCi² supports making it clear in the legislation that sharing information among AIs will not constitute "tipping off" and, that the HKMA encourage joint SAR filings, especially if they can be automated (see response to Question 6).

Question 6.

Given the speed with which criminals can move money, coupled with the lack of transparency across the financial institutions being used to move that money, we strongly support an approach to information sharing that would allow for better suspicious activity information flows and quicker action. The sharing of information relating to suspicious activities among AIs can provide greater transparency into fund flows, as well as better insight into the underlying possible illicit activities. Allowing AIs to share information and collaborate, when appropriate, on joint STR filings could provide law enforcement with more complete and concise information. We also believe that automating aspects of the STR, for instance enabling essential information to be auto populated, would greatly enhance the efficiency and effectiveness of the filings.

Question 7.

We agree that to protect personal data privacy and customer confidentiality, information sharing among AIs regarding customers and customer activity should be limited to cases where the purpose is to detect and prevent financial crime. In the US to fall within the safe harbour from liability, a financial institution must have a suspicion of possible money laundering or terrorist financing activity. Because such sharing would take place at a time when an investigation was being initiated and information gathered, a higher standard would likely dissuade sharing under the safe harbour for fear of failing the test and being subject to legal and/or contractual liability. It would also greatly mitigate against developing a more proactive approach to detecting illicit activity, a stated objective of the proposed legislation, in addition to investigating financial crime, and reduce the effectiveness of the use of technology and future technological advancements.

[1] Prior to sharing information, financial institutions also must have provided notice to FinCEN under 314(b) and verify that the financial institution with whom it wishes to share information has also submitted the requisite notice to FinCEN. This administrative requirement has been noted to be an unnecessary burden by many financial institutions.

Question 8.

Protecting privacy should be part of the foundation for any information sharing regime, especially one that ultimately will have to consider cross-border information flows as most are highly concerned about privacy issues. Using privacy enhancing technology to address this issue is something that should be considered by the HKMA as it finalizes its rulemaking.

Conclusion

FCi2 appreciates the opportunity to provide its views to the Hong Kong Monetary Authority regarding its Proposal for Information Sharing Among Authorized Institutions to Aid in the Prevention and Detection of Crime. We understand the difficulty in attempting to both protect customers' rights to privacy while simultaneously protecting the financial system from being used as a tool to further criminal activity. The best way to balance those interests is through the smart use of technology which allows for a quick exchange and analysis of information in a secure and transparent way. Allowing financial institutions to alert each other about suspicious activity will help to arm them and law enforcement with more complete information. The ability to share and collaborate quickly is an important tool in detecting criminal activity, protecting customers from fraud, and the banking system from abuse. We commend your proposal.

Respectfully submitted,

/s/Richard Apostolik
_____
Richard Apostolik
President & CEO

/s/Rachel Lerner
_____
Rachel Lerner
General Counsel