RESPONSE TO CONSULTATION PAPER

Please note that all submissions received will be published and attributed to the respective respondents unless they expressly request MAS not to do so. As such, if respondents would like:

(i) their whole submission or part of it (but not their identity), or

(ii) their identity along with their whole submission,

to be kept confidential, please expressly state so in the submission to MAS. MAS will only publish non-anonymous submissions. In addition, MAS reserves the right not to publish any submission received where MAS considers it not in the public interest to do so, such as where the submission appears to be libellous or offensive.

Consultation topic:	Consultation Paper on FI-FI Information-Sharing Platform for AML/CFT
Name[1]/Organisation: [1]if responding in a personal capacity	Asia Securities Industry and Financial Markets Association (ASIFMA)[1]
Contact number for any clarifications:	+65 6622 5972
Email address for any clarifications:	lvanderloo@asifma.org Laurence Van der Loo, Executive Director, Technology and Operations
Confidentiality	
I wish to keep the following confidential:	None

[1] ASIFMA is an independent, regional trade association with over 150 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, competitive and efficient Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

Dear,

ASIFMA and its members appreciate the opportunity to respond to MAS' consultation paper on *FI-FI Information Sharing Platform for AML/CFT ("Consultation Paper").* Our members take their AML and CFT responsibilities and obligations very seriously and we are supportive of any efforts to further enhance and strengthen AML/CFT capabilities in Singapore and globally. We are in principle supportive of increased sharing of AML/CFT related data and information as it will help duplicate efforts, break down information silos, encourage a collaborative approach to financial crime and help FIs to form a more complete picture of their clients and businesses. That being said, it is a complex topic and there are many other considerations around for example data privacy and "tipping-off" risks that need to be taken into account to avoid any unintended data privacy breaches, legal risks, and penalties for participating FIs as well operational aspects to make sure the platform operates smoothly and effectively. In what follows, we list our feedback to the MAS' questions listed in the Consultation Paper, as well as our feedback more broadly and some requests for clarification.

We are grateful for your consideration and hope these can be reflected in the final framework.

We would welcome the opportunity to discuss our feedback in more detail during a meeting and remain at your disposal for any follow up questions you might have,

Yours sincerely,

Laurence Van der Loo
Executive Director Technology and Operations, ASIFMA

Question 1: MAS seeks feedback on the proposed framework to strengthen the FI-FI information sharing paradigm and the measures to safeguard the interests of legitimate customers.

1. Footnote 11 states that *"MAS intends to issue the red flags and threshold criteria to participant FIs privately. FIs and their officers will be legally obliged to keep the red flags and threshold criteria confidential, to avoid unauthorised disclosure especially to bad actors. Unauthorised disclosure of the red flags and threshold criteria by FIs or their officers may be subject to penalties"*.
    - Whilst we appreciate the rationale behind this arrangement, it would be helpful if the MAS can provide some examples and scenarios, data points, templates that will clarify to FIs how COSMIC is intended to work.
    - The Consultation Paper in paragraph (7.3) requires the FI to provide an opportunity to clients to explain the transactions or behavior assessed to be suspicious, prior to exiting a client relationship. Our members fear that during these conversations with their client, FIs will have to explain what have caused a concern, which might lead to disclosure of the red flags or threshold to the client. This may result in the FI violating the confidentiality requirement as set out in Footnote 11 of the Consultation Paper.
    - We suggest that it should be made clear that such situations will not be caught under 'unauthorised disclosure'. We suggest that only "deliberate" / 'wilful" unauthorised disclosure be subject to penalties as a form of assurance to FIs.
    - Point 3.4 – "MAS will also require the FI to seek an explanation from the customer as part of its risk assessment of potential financial crime concerns" – Our members are concerned that this could be considered as "tipping off". We suggest the MAS to clarify and provide sufficient to protection to FIs.

- Internally, FIs may use these red flags communicated by MAS for risk management including adjustments to their transaction monitoring systems. For global firms, disclosure of such red flags internally is necessary for the administration of a global monitoring platform. We suggest that MAS provides more guidelines on the boundaries of confidentiality pertaining to the red flags that will be issued.
- From the wording of Annex B X4, it is currently unclear whether the set of high-risk indicators and threshold criteria will be the same for all participating FIs or whether they will be tailored and thus different for each FI? In case of the latter, we suggest that sharing of these tailored triggers with other participating FIs as part of a Request/Provide/Alert should not be deemed as 'unauthorised disclosure'. How often will the high-risk indicators be updated? Where there is an update to high-risk indicator, will this apply retrospectively?

2. Under current arrangements, FIs would file an STR on suspicious activities and the authorities (CAD / MAS) could carry out investigations accordingly. Where additional information is needed, the authorities rely on a Production Order or informal sweeps to get information from more FIs. This protects FIs from breaching banking privacy regulations as their interaction is currently confined to only regulators and enforcement agencies. The new proposal mandates sharing of suspicious transactions amongst FIs on COSMIC. In doing so, FIs are now subject to additional litigation risks by customers and the authorities (if triggers are inadvertently shared with bad actors, if customer information is shared without threshold/triggers being met, the nature of information shared is inappropriate etc).
   - Has MAS considered a middle ground whereby MAS/CAD, upon receiving STRs, follow up with the filing FI and decides whether and what to load onto COSMIC? This allows FIs to side-step the litigation from customers, penalties from MAS and minimizes the risk of tipping-off.
   - Alternatively, another option would be a network of designated officers to share/receive information within a secured and monitored platform. Access to the platform should align with that of SONAR (i.e. authorized persons logging in via Singpass/Corppass such as MLRO/Head of Compliance/Legal/Risk). CAD being the central party of STR information should be an active contributor to the platform."

Question 2: MAS seeks feedback and welcomes suggestions to enhance the proposed three modes of information sharing, i.e., Request, Provide and Alert, to better support FIs' detection and assessment of potential illicit actors.

1. FIs should respond to Request messages, send Provide messages and place Alerts within a reasonable time period. Given that substantive penalties and fines are linked to lateness, we encourage the MAS to provide more detail on what is considered as a reasonable time period.
2. For Request and Provide, an FI should only initiate risk information sharing with another FI, where the customer had transacted with customer(s) of the other FI and/or where its customer is also a customer of the other FI. Our members are unclear on how they can determine these other relevant FIs that are linked to the customer or its activities.
3. For a variety of reasons - including "tipping off" considerations or when the FI does not know which other FIs the client banks with - an FI may decide not to send a Request / Provide message even when thresholds are met. The FI may decide to file an STR instead. The alternative of filing an STR over sharing the information on COSMIC should be made

a valid option in view of such constrains. In such a scenario, MAS/CAD can in turn put the necessary information on COSMIC, if deemed appropriate.

4. As penalties can apply if information is shared between FIs prior to complying with the requirements of "Request, Provide and Alert", we suggest that there is a carve-out from any liability when parties are acting in consortiums or syndicates and materials (POAs, board resolution extracts, etc) are shared amongst institutions."
5. Would it be possible/ necessary to include disclosure of connected persons to the customer, given that illicit actors often function within a group to avoid detection? i.e. Where the inquiry relates to a customer, would the respondent FI also be required to include information on the connected persons (to the customer) where such information is available from the respondent FI.
6. <u>Request</u>
    - With regards to making it mandatory for receiving FI to furnish requested information, this should be subject to the receiving FI being satisfied that the information will assist in assessment and determination of ML/TF/PF risk concerns. We suggest the MAS provides guidance on how assessments can be made to minimise 'fishing expeditions' by requesting FIs. This will also provide legal protection (by customers) for the receiving FI. We suggest the receiving bank should have the right to deny to respond if the receiving bank is suspecting that the requesting FI is fishing or if they have established that they might disclose competitive or price-sensitive information by responding to the Request. We suggest MAS clarifies the conditions subjects to which a receiving FI can deny to respond to a Request.
    - The framework should make clear that a Request is not a mandatory course of action, whether during initial or post-initial phase.
7. <u>Provide / Alert</u>
    - A client termination is often based on a balancing of risk vs reward factors and may not solely be due to suspicion. Is an FI obligated to file an STR in such a scenario? If yes, the FI should not be obligated to disclose such financial or commercial reasons.
    - There might be "tipping off" triggers under the requirement to provide details in "Alert" should an STR be filed, or a relationship terminated and also the requirement to first ask the client to explain certain red flags or suspicious behaviour. While the intent is sound in the name of providing better risk information to other FIs and to treat customers fairly, our members need more guidance on how they can manage the risk of "tipping off" at the same time.
    - Following the receipt of information provided by another FI (under Provide) and an internal risk assessment, is there an expectation for the receiving FIs to provide the outcome of the risk assessment to the initial FI or file STRs given the information provided by the initial FI? We submit that any ongoing obligation to continually provide updates to the initial FI will be onerous.
    - We suggest the MAS clarifies that FIs are not required to exit the relationship if its internal risk assessment does not throw up any suspicious transactions.
    - In giving the customer an opportunity to explain, and then the firm decides to exit, does it constitute information that firms would also need to include in the Alert and share with other FIs?
8. Section 3.11 (Watchlist on COSMIC) –
    - Is this list available to all participants of COSMIC?
    - Will there be any review undertaken when a participating FI determines that a name should be added into the watchlist?

- Will the name remain in the watchlist indefinitely, or is the participating FI expected to undertake a review after a period to determine if it should remain?
- Who determines if the name can be removed from the watchlist?

9. Participant FIs should check if a prospective or existing customer is on the COSMIC watchlist. The name of these clients will need to be formatted in such a way that it can support screening by different systems used by FIs. If there is an expectation to screen new and existing clients against COSMIC Watchlist, FIs will need to be able to export the names in COSMIC for backend screening. Operationally, it is not feasible for FIs to screen the names manually, one by one. Also, downloaded info will have to be shared with a relevant support team to support such regular screenings. Section 3.13 (Material networks of suspicious actors and activities escalated to MAS for further analysis and follow-up) – Will the outcomes eventually be shared by MAS on COSMIC or published through a document?
10. Will the Request/Provide/Alert be of a specified format or free text?
11. Is the response limited to text only or is there a possibility for FIs to share documents?
12. Will the disclosing FI receive any e-mail notification if a Request/Provide/Alert has been received?
13. Can Requests be sent to more than 1 participant FI and if so, will COSMIC allow for all the FIs to view the information that has been provided to the requesting FI?

Question 3: MAS seeks comments on the proposed legislative amendments, to permit the disclosure of risk information on COSMIC for AML/CFT purposes only, and to require FIs to put in place measures to safeguard the confidentiality and appropriate use of the shared risk information.

1. While MAS is the owner and operator of COSMIC, the proposed framework places the responsibility on FIs to (a) ensure that alerts and criteria shared by MAS is not inadvertently made known to bad actors (b) ensure that the circumstances/scenarios under which information is shared on COSMIC meets MAS' listed criteria/threshold (c) ensure that the information shared on COSMIC is appropriate and accurate. As the criteria/threshold/conditions for (a) – (c) above are new and untested, can FIs run their assessments by MAS before providing risk information via COSMIC in the initial few years, especially since there are penalties if FIs get it wrong?
2. Alternatively, as mentioned further above, given the penalties to be imposed on FIs for the above, MAS should issue clear guidelines with regards to the above including examples of scenarios when sharing on COMIC would be appropriate and inappropriate, standard template with specifications on the actual data to be provided etc. In providing data points, MAS should also take into account that the KYC information collected may differ depending on the nature of relationship with client.
3. Section 4.3 – "… *FI may be subject to penalties if it discloses risk information to another FI without first satisfying the requirements and conditions for Request, Provide and Alert after the initial phase…*" Is the disclosing FI expected to ensure that when a Request is received, that the requesting FI had satisfied the requirements and conditions of the Request (i.e., that the customer's behavior had crossed the relevant threshold) before responding to the Request? Otherwise, will the disclosing FI be deem liable as it had disclosed risk information?
4. Section X7(4) and Y7(4)- a FI will be required to disclose "*if the disclosing financial institution is satisfied that the disclosure of such risk information may assist in determining any matter in connection with money laundering, terrorism financing, or the financing of the proliferation of weapons of mass destruction*". This may be subjective in determination. FIs may opt to readily release information to avoid any prosecution under section Y10(3).

5. Under the 'any individual that fails to secure FIs' compliance with requirements' that may be subject to penalties, is the MAS referring to the MLRO of the firm or persons appointed in charge of COSMIC?
6. Section X1(1) – It is unclear what "class of persons" will form a "relevant party". Will this also include connected persons to a customer (spouse/ family/ business associates)?

Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC.

1. Given that information sharing between FIs is contemplated, antitrust must be considered. If necessary, the statutory amendments should incorporate a carve-out from application of any antitrust liability for actions taken in connection with this initiative.
2. It is not usual for clients to request an attestation from FIs that onboarding/refresh information are used for only KYC or formal investigation purposes. As information sharing on COSMIC would not fall under the latter (unlike STRs), statutory amendments should address such attestations.
3. Depending on the booking model of an FI, there could be trades handled in Singapore booked to an affiliate/HQ in another location. Will the proposed statutory protection extend to such transactions when the KYC may be conducted by a non-Singapore team?
4. Under the 'any individual that fails to secure FIs' compliance with requirements' that may be subject to penalties, is the MAS referring to the MLRO of the firm or persons appointed in charge of COSMIC?
5. Privacy laws are very much embedded into most client contracts. FIs with European clients are also subject to laws like the GDPR. These present a significant challenge particularly for smaller FIs to comply with the "Request", "Provide" and "Alert" mechanisms while adhering to contractual clauses and global privacy laws that might apply. This is particularly as the risk information shared with external FIs may then be further shared within the FI's Group of companies and affiliates. The framework for COSMIC should be carefully designed to address these challenges. For instance, consideration should be paid to whether there may be conditions under which FIs are able to "abstain" from the "Provide" requirement e.g., FIs without the requisite contractual protection (due to lack of bargaining power to negotiate) or which are subject to opposing laws.
6. In relation to Sections X6 and X11 of Appendix B:
    - Please consider making an amendment to the Banking Act to expressly provide for and permit disclosure of (without specific customer consent) Customer information for the purposes contemplated in and/or in accordance with the Financial Services and Markets [Act] (FSMA) (including any disclosure of information where further disclosure is not prohibited under the FSMA, such further disclosure).
    - Please consider making an amendment to the Personal Data Protection Act to expressly provide for and permit collection, use and disclosure of personal data about individuals without consent, for the purposes contemplated in and/or in accordance with the FSMA (including any disclosure of information where further disclosure is not prohibited under the FSMA, such further disclosure).
    - Please consider making an amendment to the Personal Data Protection Act, with respect to Section 26 of the PDPA (and related provisions in the subsidiary legislation) to expressly provide for and permit transfer of personal data outside Singapore without consent/restrictions, for the purposes contemplated in and/or in accordance with the FSMA (including any disclosure of information where further disclosure is not prohibited under the FSMA, such further disclosure).

- Does an individual's right to access/correct personal data under Part V of the Personal Data Protection Act apply to information that Financial Institutions collected from the COSMIC platform?
- Section X6 and X11 use the term 'disclosure' [of information]. Please consider also including the terms 'collection' and 'use' [of information] which are terms used under the Personal Data Protection Act, in order to provide statutory protection to FIs vis-à-vis the obligations under the PDPA on disclosure, collection and use of personal data. (eg. When a FI receives information from the platform, it will also be 'collecting' data.)

7. In relation to X13 of Appendix B:
   - Section X13 uses the term 'disclosure' [of information]. Please consider also including the terms 'collection' and 'use' [of information] which are terms used under the Personal Data Protection Act, in order to provide statutory protection to FIs vis-à-vis the obligations under the PDPA on disclosure, collection and use of personal data. (eg. When a FI receives information from the platform, it will also be 'collecting' data.)
   - Can the immunity under Section X13 extend to disclosure in accordance with Section X11.
8. We seek MAS' confirmation that the statutory protection would cover FIs in the event that the information shared by these FIs was inadvertently disclosed by other participants FIs. Additionally, we would suggest that comments from the Personal Data Protection Commission be sought to ensure that FIs would not be subject to undue legal liabilities from such sharing of personal data.

Question 5: MAS seeks comments on the scenarios and related conditions that have to be met before an FI may share COSMIC platform information with local and overseas affiliates of FIs, and third parties.

1. Footnote 31 states that "*In relation to the persons to whom platform information can be disclosed to for performance of ML/TF/PF risk management: (a) Where the participant FI is incorporated outside Singapore, (i) any officer of the head office/parent company of the FI who is designated in writing by the head office/parent company, (ii) any officer of any branch of the FI outside Singapore who is designated in writing by the head office/parent company, and (iii) any officer of any related corporation of the FI who is designated in writing by the head office/parent company of the FI. (b) Where the participant FI is incorporated in Singapore, (i) any officer of the head office/parent company of the FI who is designated in writing by the head office/parent company, and (ii) any officer of any related corporation of the FI who is designated in writing by the head office/parent company of the FI*."
2. As it is common for clients to have multiple relationships with HQ as well as affiliates, Financial Crime Risk teams generally work with their counterparts in other regions to holistically assess a client's risk, taking into consideration the various relationships maintained globally. It is proposed that sharing of COSMIC information with Financial Crime Risk teams within the same FI be allowed. This avoids the problem of delay in risk management reviews due to designated persons being on leave or having left the company over time.
3. Table A (Disclosure of platform information) – Person to whom platform information may be disclosed, point (ii): "Any officer designated in writing by the head office or parent company of the participant FI". We suggest it would be a heavy lift for FIs that does not add much value in case FIs have to maintain a list of names designated by the head office/parent company before the information can be shared. We therefore propose that MAS consider aligning this table with the Banking Act 3rd Schedule, where there is no

requirement for "officer designated in writing" if the disclosure is for the purpose of risk management –

4. In relation to X11 Schedule:
    - Please consider including the equivalent of the Banking Act Third Schedule (Disclosure of Information) Part I: Section 8 "Where the bank is a bank incorporated outside Singapore or a foreign-owned bank incorporated in Singapore, the disclosure is strictly necessary for compliance with a request made by its parent supervisory authority."
    - In relation to Part II Section 1: Please consider including disclosure to "a lawyer, consultant or other professional adviser appointed or engaged by the bank in Singapore under a contract for service".
    - Please consider including the equivalent of the Banking Act Third Schedule (Disclosure of Information) Part II: Section 2 *"Disclosure is solely in connection with the conduct of internal audit of the bank or the performance of risk management."*
    - Please consider including the equivalent of the Banking Act Third Schedule (Disclosure of Information) Part II: Sections 4, 4A, 4B where they contemplate that disclosure of existing data in the bank's possession may be required as part of a restructuring/business change.
    - If there are any other reasons not listed in the schedule where disclosure of information may be required, what should financial institutions do?
    - Please consider including the equivalent of the Banking Act Third Schedule (Disclosure of Information) Part I: Section 1 "*disclosure is permitted in writing by the customer*" under the condition that the FI has anonymised the identities of the platform participants that had provided the information. In case the customer has provided a broad consent for disclosure of his information, the limitations as provided in the "conditions" column may make the disclosure more restrictive than under the customer written consent.
    - Please clarify the requirement of filing the STR as a condition for disclosure of platform information in Part II section 2. Please consider removing this condition so that the disclosure is permitted on a similar basis as under the Banking Act Third Schedule (Disclosure of Information) Part II: Section 2.
    - Please clarify the requirement to designate the officer in writing – does it mean a designation of a particular person by name? Please consider a change to designation of the branch or related corporation instead of the officer.
    - Please advise how to distinguish FI's ML/TF/PF proprietary information from the platform information if such platform information pertaining to a particular customer will be matched with the FI's proprietary information of such customer and may need to be disclosed outside of the FI.
5. There should be sufficient guidance to ensure protection to FIs around any data privacy issues, especially when it comes to overseas offshore data sharing with head office or overseas affiliates for various purposes (such as internal and external audits).
6. Given that the third parties may be in jurisdictions with high AML/ CFT risks, or maybe unregulated, the "conditions as may be specified in a notice or direction issued by the Authority or otherwise imposed by the Authority" should be strict to protect against abuse or unauthorized access to FI's customer's information.
7. Table on pg. 16 – 2nd row – Alignment required so there is no need to identify 'designated officers' individuals themselves.
8. Table A 3rd row – We note that the disclosure of information to outsourced parties is subject to conditions as may be specified in a notice or direction issued by the MAS. As FIs would already have in place existing agreements with the outsourced vendors, it would

be time-consuming and challenging to introduce new conditions in the form of additional contractual clauses. In this regard, we respectfully ask that MAS consider this carefully and add only what is necessary, taking into account what is already required under the existing outsourcing guidelines.

Question 6: MAS seeks feedback on introducing a requirement for FIs to put in place a process for reviewing customer relationships prior to exit, which would include providing the customer adequate opportunity to explain the activity or behaviour assessed to be suspicious.

1. As mentioned above, a mandatory requirement for FIs to engage the customer on a suspicious activity or behaviour prior to exit of relationship could increase the risk of tipping-off as well as unauthorised disclosure of the thresholds or red flags. MAS may wish to consider making such engagement a best effort requirement instead, subject to the assessment of FIs on the risk of tipping-off. As firms may need to explain why they are suspicious and explain to them the thresholds/red flags etc.
2. Before exiting a relationship, FIs would typically take other actions first, such as cutting credit lines, reducing limits. Is that not caught by this?

Other comments and questions:

1. How long would the data be stored in COSMIC? What would be the criteria for removal?
2. Can participating FIs access/request for historical info on COSMIC, will there be search function or is it real time?
3. Can the MAS further clarify how they intend to use the information on COSMIC and for what purposes?
4. Does the MAS have any intentions to share any COSMIC data with other APAC regulators/enforcement agencies, (e.g. HKMA/JFIU)?
5. Following this initial phase, MAS intends to make the risk information sharing requirements mandatory. MAS will also consider when to expand the scope of participant FIs and the key risks to be targeted by COSMIC.
6. Can the MAS further expand on the expected timelines to expand membership and also the key risks, which in the initial phase is only limited to 3 areas: “misuse of legal persons”, “trade-based ML” and “proliferation financing”.