Annex B

Submissions from respondents to the consultation paper on FI-FI information sharing platform for AML/CFT

S/N	Respondent	Feedback from Respondent
1	AIA Singapore Private Limited	**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.** No comment. **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.** AIA would like to suggest having a stipulated time frame instead of a reasonable timeframe to minimize the inconsistent period across the FIs. **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.** No Comment. **Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC.** No Comment. **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.** No Comment. **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.**

		No Comment.
2	Aon Singapore Pte Ltd	**General Comments:** It is unclear from the consultation paper and draft legislation on the intended scope of participating FIs in the subsequent phases. For instance, the general insurance and related intermediaries' industries have significantly lower inherent ML/FT risks. Hence, we suggest excluding FIs with inherent low ML/FT risks from the proposed framework as they will not stand to benefit or contribute much to the FI-FI information sharing on COSMIC.
3	Asia Securities Industry and Financial Markets Association	**General Comments:** 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”. **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”.* o 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. o 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. o 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. o 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. o 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. o 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). o 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. o 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> o 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. o The framework should make clear that a Request is not a mandatory course of action, whether during initial or post-initial phase. 7. Provide / Alert o 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. o 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. o 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. o 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. o 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) – o Is this list available to all participants of COSMIC? o Will there be any review undertaken when a participating FI determines that a name should be added into the watchlist? o 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? o 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:

		o 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). o 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). o 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). o 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? o 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: o 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.) o 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: o 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." o 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".

		o 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."* o 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. o If there are any other reasons not listed in the schedule where disclosure of information may be required, what should financial institutions do? o 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. o 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. o 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. o 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?
4	Association of Independent Wealth Managers	**General Comments:** The Association of Independent Wealth Managers ("AIWM") represents the interests of its ordinary members, external asset managers and multi-family offices (hereafter jointly referred to as "EAMs") in Singapore. We strongly support the efforts of the Monetary Authority of Singapore (hereafter referred to as the "Authority") to prevent money laundering, including proliferation financing, and terrorism financing. Strong AML/CFT measures contribute to the reputation of and trust in Singapore's thriving financial centre. This is crucial for the wealth management carried out by our members. **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.** The exchange of information among financial institutions on higher risk relevant persons and behaviour strengthens Singapore's AML/CFT efforts. We therefore welcome this initiative for such exchange of information among financial institutions under the auspices of the Authority. Smaller financial institutions, such as EAMs, will also need to have the opportunity to participate in this exchange of information. Excluding them will increase their exposure and may lead to money laundering or terrorism financing cases that could damage the reputation of the entire financial centre. Moreover, their exclusion may instigate other financial institutions to treat them as a higher risk and implement additional safeguards that impede collaboration among the financial institutions.

		These additional obstacles may weaken the small financial institutions and, ultimately, Singapore's wealth management sector of which they are a vital pillar. To the same extent as a strong AML/CFT framework contributes to the reputation of and trust in the financial centre of Singapore, strong safeguards of the customers are fundamental to this trust and reputation. Their privacy is of material interest to most high-net-worth individuals. Legitimate customers should not be unnecessarily exposed. We therefore also support the proposed measures to safeguard the interests of legitimate customers in the exchange of information among financial institutions, namely that information may only be shared in specified situations, i.e. when specified thresholds are met, and only to the extent that information is relevant in the specific situation. The information shared in COSMIC must remain limited to relevant information to safeguard the interests of legitimate customers and the operability of the platform. The regulations will need to be very clear on the thresholds. At the same time, access to information must be restricted on a "need to know" basis to a few designated individuals in compliance, risk management, and management. The Authority may consider allowing for Providing information in COSMIC only when the financial institution has filed a suspicious transaction report (STR). **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.** The proposed tiered approach acts as adequate safeguard to customers while allowing financial institutions to obtain and share necessary information to effectively combat money laundering and terrorism financing. We support this tiered approach with increasing thresholds for the disclosure of customer information. In case of a request, the "initiating financial institution or any of its officers may, when making a request […], disclose any risk information as may be relevant to the request made to the disclosing financial institution." (sec. X7(3) Annex B). The initiating financial institution has no obligation to disclose the information. We propose that the initiating financial institution has an obligation to disclose the risk information as an additional safeguard to ensure that the basis for the request is sufficient, but without an obligation by the disclosing financial institution to assess this, and to enable the disclosing financial institution to conduct a risk assessment themselves. The proposed statutory provisions should clarify that the disclosing financial institution has no obligation to ascertain that the request is justified. At the same time, the disclosing financial institution should have a right to withhold information of which it is confident that it is not relevant to the request. The Authority may consider further clarifying this beyond the proposed sec. X7(4) of Annex B. Sec. Y8(2)(a) of Annex B will place a great burden on initiating financial institutions for "Provide". To ensure that the risk information is disclosed to "any prescribed financial institution that has the same relevant party where the initiating financial institution knows or should have known that the relevant party that is the subject of the

		disclosure is also a relevant party of the other prescribed financial institution" will require an extensive search of the initiating financial institution's records. For example, the initiating financial institution may need to check on all accounts where an individual is the account holder, a person authorised to act on behalf of the customer, or the beneficial owner and search the transactions of all these accounts for indications of associated entities, possibly even extending to records before the obligation was introduced, to find connections to other prescribed financial institutions. Large financial institutions will certainly struggle to meet such requirement. For small financial institutions, it will be impossible to conduct the required research. We therefore advocate for the Authority to limit the extent of the "provide" obligation to relevant financial institutions involved in the transaction triggering the provision of the risk information. The disclosure to further financial institutions should not be an obligation but a possibility where the initiating financial institution is aware of common relevant parties. Financial institutions will be required to disclose information for Request, Provide and Alert in a timely manner that is to be specified in regulations (para. 4.12(b) of the Consultation Paper). Given their limited resources overall, small financial institutions, such as EAMs, will have limited resources to reply to Requests, or Provide information, or produce Alerts. While we recognise that a timely exchange of information facilitates AML/CFT measures in the ecosystem, we request the Authority to implement an adequate timeframe that does not jeopardise small financial institutions' services to their customers. Similar to the initial financial institutions participating in COSMIC, other financial institutions should also have a two-step implementation of the requirements for information sharing in COSMIC. Other financial institutions will encounter essentially the same challenges to comply with the requirements for the disclosure of information while safeguarding their customers' legitimate confidentiality. **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.** We strongly support safeguards of information shared on COSMIC: the restriction of their use for AML/CFT purposes only as well as the limited access to this information. As mentioned previously, privacy is of material interest to most high-net-worth individuals. Legitimate customers should not be unnecessarily exposed. The confidentiality of their information must be safeguarded in their interest and the interest of the financial centre Singapore. The Consultation Paper highlights technology risk management measures to safeguard access to COSMIC (para. 4.4 of the Consultation Paper). The Authority may impose requirements on the prescribed financial institutions concerning their participation on the platform (sec. X3 Annex B). While it is in the interest of EAMs to participate in COSMIC, small financial institutions, such as EAMs, have limited resources to

		safeguard their technology and their technological access to the platform. We therefore welcome the option of a web-based user interface as proposed in the Consultation Paper (para. 8.2 of the Consultation Paper) to grant them access. **Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC.** We support and concur with the proposed provisions to exclude civil liability of financial institutions that have disclosed information in COSMIC with reasonable care and in good faith. **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.** Due to their limited size and resources, small financial institutions, such as EAMs, frequently outsource functions such as compliance and internal audit. Sec. X11 of Annex B and Part II of the X11 Schedule to Annex B allow for the access of outsourced compliance service providers. The disclosure of the Authorities directions for access to and disclosure of information in COSMIC under sec. X4(3) of Annex B should be aligned for their sharing with outsourced compliance service providers. Moreover, we advocate to explicitly allow for the sharing of information with internal audit where it is outsourced. The sharing with outsourced internal audit is crucial to their control and assurance. **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.** We support the further clarification that financial institutions should not exit customer relationships without due reason. The reliability of business relations with their financial institutions is a crucial factor for customers that contributes to the trust in Singapore's financial centre. At the same time, the Authority may consider providing additional guidance to distinguish the required opportunity for the customer to address the financial institution's concerns versus the prohibited "tipping off".
5	BioQuest Advisory Pte. Ltd. TigerGraph Pte. Ltd.	**General Comments:** **<u>Introduction</u>** **BioQuest Advisory** has a business & technology advisory business with a practice in Singapore and Asian cities like Kuala Lumpur, Hong Kong. We focus on Intelligent Automation and Data Analytics. For financial services, we are working with FIs to adopt A.I. enabled automation in many operational areas and data analytics for Financial Crime Compliance (FCC) & Customer Analytics. The key data analytics technology we

		leverage on is the Graph technology which can drive deep linkage analysis with machine learning algorithm. We partnered with TigerGraph – a scalable, advanced analytics & machine learning platform to help FIs perform advanced analytics, especially in the area of FCC. **TigerGraph** is a leading provider of graph analytics platforms which is also the first and only distributed native graph database in the industry for advanced analytics and machine learning on connected data. Our proven technology, which supports applications such as fraud detection, anti-money laundering (AML), entity resolution, customer 360, recommendations, knowledge graph, cybersecurity, supply chain, IoT, and network analysis, has more than 1200 customers worldwide, including 8 of the top 10 global banks. Our feedback on this consultation paper would be from the technology perspective, primarily advanced analytics, to strengthen the COSMIC framework, safeguard interest of legitimate customers and provide an effective platform for detecting financial crimes. **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.** COSMIC information sharing platform is an important step towards providing visibility of activities beyond the FI's internal data, which would be critical to identify criminal networks which typically span across multiple FIs. Similar initiatives such as the UK's Joint Money Laundering Intelligence Task Force (JMLIT) has yield success stories on assets being seized and arrests made. The COSMIC framework proposed requires a good balance of information sharing for effective detection of criminal activities and protecting the privacy of legitimate customer is a delicate one. We have three points for MAS's consideration: **(1) Creating a dynamic set of risk indicators and its corresponding thresholds to reduce opportunities for exploitation** The framework proposed includes setting thresholds for risk indicators for FIs to report/request/share information on the potential financial crime. Criminals are often fast to exploit on regulations and would likely to quickly adapt to operating below thresholds and away from key risk indicators to avoid detection. Hence, the risk indicators and its corresponding thresholds should not be a static one prone to exploitation. Advanced analytics and machine learning like Graph Analytics can be leveraged to continuously monitor and discover new risk indicators that might come to be of relevance for monitoring and proposing of suitable thresholds and new risk indicators. In addition, the relationships between the risk indicators would also be importance to setting dynamic thresholds. Graph technology that focuses on tracing relationships

		and detecting patterns, communities, similarities are powerful tools in the effort to ensure risk indicators and its thresholds remains relevant and adequate to detect financial crimes. **(2) Responsibility assignment matrix access to COSMIC data to safeguard privacy of legitimate customers** Customers' confidence in their privacy with their bankers is an important one that Singapore has carefully nurtured as a leading global financial centre. For a platform like COSMIC to be effective, sometimes a significant amount of data sharing is required. Hence, there should be a good responsibility assignment matrix to control which group of users (i.e. Provider, Requester, other FIs, MAS's teams) have access to what type of data is an important one. Hence, the underlying technology (i.e. database, analytics, machine learning etc.) would need to take into consideration on each set of users having access to data as required and not in excess that the customers' privacy is compromised or in conflict with the privacy regulations we have in place. This control might be easy to implement and most often out-of-the-box for transactional systems, but in the case of advanced analytics and machine learning where data are amalgamated to produce certain estimates might increase the complexity of such controls. The selected database, analytical tool and workflow technologies for COSMIC would need to satisfy requirements for a robust responsibility matrix despite the complexities. **(3) Readiness of FI's data and systems** As most Compliance function operates on a very lean team and the additional process of providing/requesting information on COSMIC should be as automated/streamlined for efficiency and timeliness. It would be helpful if MAS can share guidance/advisory for FIs to prepare their data and systems to meet the COSMIC requirements as early as possible. The experience gained during the initial phase of the 6 banks participation would likely give an indication on what is to be expected in terms of data and system requirements to support COSMIC when more banks are to participate. **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.** In this response, we seek to offer a novel perspective on detection of criminal activities and, more importantly, another mode of information sharing based on explainable algorithmic to trigger a request for information. We will also suggest a more comprehensive set of possible interactions with COSMIC based on current practices in information technology. Finally, we intend to summarize the currently proposed modes of information sharing and explain why there is, in our opinion, two missing elements and a missed opportunity.

On the Information Sharing Mode

In information technology, information storage and retrieval is directed by a series of basic operations known under the acronym CRUD. This acronym stands for Create, Read, Update, Delete. This paradigm has held for decades and is based on the assumption that information needs to be readable and updatable. In the case of critical information systems, and sometimes for performance reasons, the Delete operation is not desirable. An example of such a requirement in the context of COSMIC could be for audit and reporting reasons. In such a case, the mechanism adopted uses a timestamp mechanism to flag information as "cancelled" instead of deleting it, ensuring continuity and traceability of information and operations history. Those basic operations are also used in the most used communication protocol: HTTP (Hypertext transfer protocol). The Hypertext Transfer Protocol (HTTP) is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. HTTP defines methods very much inspired by the CRUD basic operations: POST, GET, PUT, DELETE. There are more methods, but those are not relevant in the context of this response. The following mapping can be made:

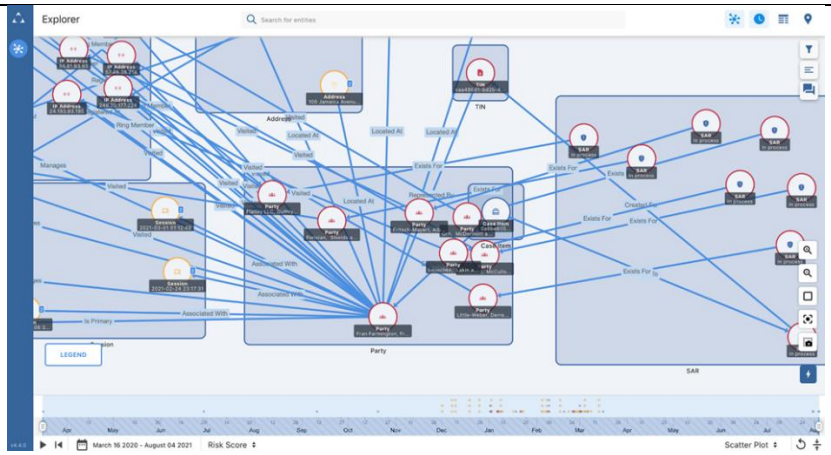
HTTP METHOD	**CRUDE OPERATION**
POST	CREATE
GET	READ
PUT	UPDATE (REPLACE)
DELETE	DELETE

As per the consultation by MAS, if we add the operations suggested, the following mapping can be done:

HTTP METHOD	**CRUDE OPERATION**	**COSMIC INFORMATION-SHARING MODE**
POST	CREATE	PROVIDE / ALERT (To FSI)
GET	READ	REQUEST
PUT	UPDATE	?
DELETE	DELETE	?

		As we can see, there are two missing sharing modes for communication completeness. As we have mentioned above, it is not desirable to simply delete a provided information, alert, or request. We are hence suggesting the following addition: 1. Update: a request to update the previously communicated information in any currently proposed information sharing modes. 2. Cancel: a request to not follow up on a previous communication mode. Those two extra information-sharing modes would complete the basic framework for complete information sharing. **Analytics Driven Extension** In addition to the previous suggestion, while COSMIC is meant for information sharing, it seems that there is an opportunity to run investigation and analysis in a more efficient manner following a REQUEST or PROVIDE request. MAS as the custodian of the COSMIC data can consider using advanced analytics including graph database and analytics to identify related individuals and entities for further investigation. Using a risk vs. privacy approach, the analysis would allow giving the requesting FI and the providing FI a holistic view of the case with enriched information linkages and insights into the case details. In our experience, this holistic approach to both data exploration and to visualization allow financial crime analysts in achieving at least 11% increase in fraud detection accuracy. Graph technology with machine learning algorithm used in investigations can yield complete explainable results. This transparency means that the audit record of the decision are fully explainable for next course of actions to be taken. With reference to our answer in question 1 above, the results from graph analytics and machine learning can be used as an input to substantiate the dynamic risk indicators and thresholds as graph analytics does its own discovery of relationships on the data provided. **Conclusion** COSMIC initiative is a significant step in the right direction in detecting financial crimes. It presents an opportunity to enhance the current proposition by adding two new sharing modes: Update & Cancel to complete the communication framework. The usage of analytics, particularly graph analytics and machine learning helps to create a holistic view of the cases in real-time and increase FIs and MAS investigative capabilities via the COSMIC platform. **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.**

		No comments **Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC.** No comments **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.** No comments **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.** Adequate review of customer relationships prior to exit is an important process to ensure that the decision of exit is a fair one and there are transparency and evidence to support the decision. On this point, we would like to make reference to Graph technology that would be helpful in mapping out all the relationships, linkages to the suspicious transactions for analysis in real-time. **Graph Analytics for Investigation** The capacity to do deep link analysis, also technically known as transversal, on data gives a deeper insights that is otherwise not visible. This analysis will also help to drive the questions to the customer for explanation. Investigators can then evaluate the answers provided by the customer to make a decision on whether to exit. One example is from the Australian Taxation Office (ATO) using Graph Analytics to fight tax evasion and investigate fraudsters who are hiding behind 10+ levels of obfuscation. The deep link investigation capabilities offered by Massively Parallel Processing graph technology allowed the ATO to investigate more than 20+ links deep in real-time on terabytes of graph data, hence exposing the fraudsters. **Explainable assessment on suspicious behaviour**

		 [Diagram 1 above: A known Fraudster (Fran, at the bottom) is linked to several other parties using deep link analysis (common IP addresses, residential addresses, regular transactions, etc.). At the bottom of the screen, a time series of the different events allows replaying the events as they took place. The boxes are a grouping of nodes by labels (Party, SAR, Online Sessions, Addresses, IP Addresses, Transactions, etc.] From Diagram 1, the graph technology offers capabilities to the investigator to dive deeper into the relationships and also provide explanation to why an entity was assessed to be suspicious. **Conclusion** Graph analytics can be a plausible solution to providing real-time deep analysis to drive questions for the customer and also transparency and reasons for exiting a customer.
6	Etiqa Insurance Pte Ltd	**General Comments:** • To consider ability to leverage/streamline with existing reports submitted to MAS/LIA/GIA as far as possible. • To consider sufficient timeline for implementation for potential financial support especially for small FIs. **<u>Amendments under Annex B</u>** • Will reference be made to TSOFA and other relevant primary/secondary legislations under MAS Act, Insurance Act or Banking Act in addition to CDSA? • To consider making provisions for situations in which FIs are not able to meet the requirements required. **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.**

		• To ensure the provision under the proposed Framework are aligned with obligations under other regulations e.g. Personal Data Protection under PDPA. • MAS may wish to set some Guidelines to facilitate consistent treatment of the persons listed in the COSMIC platform i.e. if they should be deemed as sanctioned person or they can be accepted/retained as HRC. **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.** • With the understanding that different FIs would have different AML/CFT risk appetite and thresholds, MAS should consider aligning the reporting/alert/information request thresholds to facilitate consistency in reporting and response. • Under 'Provide', it is important to specify the scenarios under which FIs are obligated to provide the requested info and set out the circumstances wherein FIs are exempted from doing so e.g. operational and system constraints, contractual obligation. **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.** Nil. **Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC.** Nil. **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.** • On the implementation plan, to consider rolling out to non-bank FIs prior to expansion of reporting scope for initial adopters. **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.** • Will MAS/CAD be updating the COSMIC with information from the respective agency and information received from other law enforcement agencies/regulators to facilitate timely identification of suspicious actors

		• On the requirement to obtain customer explanation on potentially suspicious transactions, MAS should cater for practical constraints e.g. customers uncontactable, avoidance of tip off etc.
7	FWD Singapore Pte. Ltd.	**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.** We agree broadly on the regulatory intention to strengthen the FI-FI information sharing paradigm and measures to safeguard the interest of legitimate customers. That said, for insurers, there will be additional operational burden with every piece of regulatory instrument issued by the MAS. We note the intent is to have a fine not exceeding 1 million as well as a further fine of $100,000 for everyday or part of a day in the case of a continuing offence, where "Request", "Provide" or "Alert" are not provided in a timely manner. We suggest the MAS to relook the punitive measures as it will create operational and financial burden on insurers as a whole. **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.** • We would like to seek clarification on the following: - What constitutes a "reasonable timeframe" mentioned in paragraph 3.8, 3.10 and 3.13 of the consultation paper on FI-FI information sharing platform for AML/CFT? - What constitutes "higher threshold of red flags"? Could we limit this to circumstances where the FI has filed an STR? • We would like to suggest simplifying paragraphs 3.9 and 3.10 of the consultation paper such that information is only provided upon request. In this regard, we suggest that it may be onerous on an FI to actively send a provide message to another FI on COSMIC because there could be varying interpretations of "relevant thresholds" with due consideration on the size, scale and complexity of the operations of every FI. • We would like to suggest simplifying the regulatory expectation in paragraph 3.11 of the consultation paper where an Alert should only be placed when the FI has filed an STR on the customer. Otherwise, it may be onerous for FIs to segregate the customers based on the filing of an STR and termination of relationship. **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.** No Comments.

		Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC. No Comments. **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.** No Comments. **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.** We would like to seek MAS' guidance on how to strike a balance between this requirement of putting in place a process for reviewing customer relationships prior to exit, vis-à-vis section 48 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A).
8	Lloyd's of London Asia Pte Ltd.	**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.** • We suggest a training and certification program by the MAS for the users of the system to educate them on the issue of tipping off, protecting the confidentiality of the red flags shared by the MAS etc. • We suggest setting up a set of Terms of Reference or a Memorandum of Understanding to highlight users' roles and responsibilities within the platform. • We suggest describing the parties involved in the governance, upkeeping and maintenance of this platform. • We suggest clarifying if there any fees associated with access and use of the platform. • We suggest an avenue for the participants of the platform (e.g. insurance companies) be able to provide input into the further development of the platform and setting criteria for submissions as the platform develops and matures in future. **Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC.** We are wary of potential cross border Data Privacy issues. For example, there might be complications or local regulatory restrictions when a Compliance Officer in Singapore of Insurer A needs to extract personal data of an EU national from a

		database in Japan for Insurer B that is based in a country that does not have an equivalent Data Protection standards as the EU/Singapore.
9	Manulife (Singapore) Pte Ltd Manulife Financial Advisers Pte Ltd	**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.** **MLS**: No comment. **MFA**: Would be good if this can include FAs independently, because FAs are also required to perform ML/TF screening under regulation and file STRs. But FAs have limited access to information from providers as they are only distributors. We also see that there are more customers/corporations that buy through distributors such as FAs. This will be beneficial in the following ways: 1. Enable a wider and more robust network to prevent ML/TF/PF. 2. Enable timely detection of ML/TF/PF activities at the sales process stage and increase detection of these illicit perpetrators at the sales stage. 3. Assist the FAs to develop sharper analysis of sales and representative behaviour. 4. FAs can also then share and alert each other on situations where they come across that pose a higher ML/TF/PF risk. Another way is to include tied FAs through their parent FIs. As such, information can be shared by FIs to their FAs as well. Tied FAs can in turn share through their parent FIs. Currently, FIs are prevented from sharing information including CDD documents due to PDPA and legal obligations. The proposed framework will prevent undue concerns by the FIs for the purpose to prevent and combat ML/TF risk. FAs face challenges in obtaining additional transaction data and CDD documents of its existing and new customers from distributors. Such information is pre-requisite to perform transaction monitoring and to on-board new customers who are transferred from previous FIs. The framework will enable FAs to observe the conduct of the customer's account and scrutinize transactions undertaken throughout the course of business relations. Without further data, ongoing monitoring process is hindered by the lack of information and could eventually lead to a termination of business relationship with the customers from FAs. As FAs are not the product manufacturer and in gist an intermediary to distribute products through our FA representatives. Alternatively, the framework may consider allowing the use of third-party reliance for FAs to be the relying party on the FIs for ongoing transaction monitoring.

		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. **MLS**: With reference to section 3.8 of the Consultation Paper, it is stated that the receiving FI of a Request message should furnish the requested risk information within a reasonable timeframe if it is satisfied that such risk information may assist in the assessment and determination of ML/TF/PF risk concerns. In the event that the receiving FI is of the view that the requested information is not relevant in addressing the risk concerns, is the receiving FI expected to provide justification to the initiating FI for the non-provision of information after the initial phrase? As it can be suggestive on what is deemed a "reasonable timeframe" for the provision of information, we would recommend stipulating a timeline to make the expectations clear. This comment applies to the rest of the Consultation Paper where there are expectations to perform certain task(s) within a reasonable timeframe. With reference to footnote 15, it is stated that FIs should not reject a customer solely based on the fact that the customer is placed on the COSMIC watchlist. The customer should be provided with an opportunity to explain the unusual behaviour. This seems to suggest that FIs are allowed to share information found on COSMIS with the customer. Would appreciate MAS' clarification on this. **MFA**: Request – consider guidelines on a timeline to reply can be set e.g. 7 days because requester may be depending on this request to assess and incept the case and there should be a reply on the status. Concerned that the reply may be delayed without any status update. Provide – consider guidelines on a template to provide such that there is more consistency in provision of the information. With a predefined template, this can allow a standardised analysis and assessment for both FIs and FAs to adhere to. Alert – FAs should also be alerted on terminated relationships by FIs such that any illicit parties flagged in COSMIC do not attempt to purchase or apply through other routes. **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.** **MLS**: No comment. **MFA**: In relation to the underlined in Para 4.2, "As mentioned in paragraph 3.3, sharing of risk information on COSMIC is permitted only for AML/CFT purposes. The proposed legislative amendments will set out that sharing of risk information will be permitted only between FIs that are participating on COSMIC, and within the bounds of the

		information sharing modes of Request, Provide and Alert as outlined in paragraphs 3.6 to 3.13 above." To clarify if participating COSMIC users be extended to FAs. **Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC.** **MLS:** No comment. **MFA:** Consider whether this sharing can be put under an exception in the PDPA and whether any dispute may arise on whether the information shared relates to ML/TF/PF purposes. **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.** **MLS and MFA**: Are we able to share COSMIC platform information with our parent company's regulator in Canada i.e. Office of the Superintendent of Financial Institutions (OSFI)? **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.** **MLS:** No comment. **MFA:** Suggest that outcome of STRs filed can shared. This will enable FIs and FAs to know the next step of recourse and avoid tipping off the customer.
10	MUFG Bank, Ltd.	**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. With respect to paragraph 2.5 of the Consultation Paper, we note that the initial participants of COSMIC are the six banks who had been extensively involved in its design. In view that participation will eventually be made mandatory for all financial institutions ("**FIs**"), we would like to suggest that such other FI participants be involved at an earlier stage. This is to ensure that such other FIs have adequate time to plan design system requirements and design operational processes, both of which would take time to implement. 2. To facilitate FIs' implementation, we would like to request for more guidance on the requirements for the FI-FI information sharing process. For example, a definition of or some parameters to the terms, "reasonable timeframe" in paragraph 3.8 and

		"reasonable time period" in paragraph 3.13, would be helpful to FIs in their planning and allocation of resources. 3. Further, we would also appreciate some guidance on the time period that information entered into COSMIC would be retained and displayed, as well as the frequency that such information displayed on COSMIC will be refreshed, if any. **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.** No Comment. **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.** No Comment. **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. We understand that FI-FI disclosure and sharing of risk information on COSMIC, where customer consent has not been obtained, may result in possible liability under: i. Section 47 of the Banking Act ("BA"), for disclosure of customer information to other FI(s); and ii. Section 13 of the Personal Data Protection Act ("PDPA"), for disclosure of personal data to other FI(s). Therefore, we would like to clarify whether FIs would be able to rely on any existing exceptions for disclosure of customer information and personal data without consent, such as under Part II of the Third Schedule to the BA and Section 13(b) of the PDPA. Alternatively, would there be any amendments to the BA and PDPA (in addition to the introduction of FSMA), so as to afford similar statutory protection to FIs for disclosing customer information / personal data via COSMIC? 2. We would like to share that there are circumstances where we would receive customer risk information from overseas affiliates. An STR would then be filed, if the customer risk information provided by the overseas affiliate and the Bank's internal assessment warrants an STR filing. We understand that FIs may be required to share such customer risk information on the COSMIC platform. However, there may be legal or regulatory requirements in the jurisdiction from which the information was originally shared, which disallow the onward sharing of such customer risk information.

		Therefore, we would like to suggest that MAS consider availing exemptions to FIs, such that banks are permitted to not onward share customer risk information on COSMIC or to only share such information in a limited manner (e.g. anonymised), in the abovementioned scenario. **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.** No Comment. **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.** No Comment.
11	NICE Actimize	**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.** • The proposal has similarities to the United States FinCEN 314b in which financial institutions have the ability to share information between themselves for purposes of fighting financial crime. The big differentiator with this proposal, in our mind, is that this also provides a platform to facilitate the storing and sharing of the data. That is a significant benefit. • Based on feedback from several financial institutions, FinCEN's 314b isn't always successful because the FIs are not required to respond and in many cases, some financial institutions don't respond to requests. This could occur for a couple of reasons: - What is the benefit for a financial institution to respond? There is work involved to respond to these requests and it ultimately assists their competitors. It does not necessarily provide a competitive advantage; however, it does not have a direct benefit either. It is a greater good for fighting financial crimes; however, sometimes that is not enough. - There is a potential fear of releasing too much information or the information released could misinterpreted. The financial institution with the information requested may not want to legal risk involved. • The major deficiencies in nearly all information sharing frameworks is the non - inclusion of positive feedback incentives for sharing valuable actionable information as against disincentives/penalties for non-disclosure of suspicious activity or defensive SAR filings. Legislatively, this is similar to a "joint and several" legal approach while providing some safe harbour to participating data sharing members.

		• Voluntary systems do not tend to be as successful as regulated systems. It is our belief that if MAS had more control, it may be managed better. **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.** • The proposal is relying on financial institutions to decide when and what to share and then MAS is going to monitor it. It is assumed that if suspicious activity occurred that is deemed valuable to share, it is more than likely that a STR would also be filed. It may be more operational efficient to have MAS determine what should be shared and when it should be shared. This would also aide in maintaining consistency of data sharing since it is controlled by one entity (MAS). • The sharing of data will have specific thresholds that are set by MAS and can change as time changes. Financial Institutions have to ensure they are abiding by current guidelines. We note that initially, the plan is to pilot COSMIC with limited details. As the pilot progresses, more details will be allowed to be shared. MAS will be controlling the guidelines of what can/cannot be released. If MAS defines controls the data that is shared, they can control what and when data is shared. This also allows them to release historical data on customers that was previously limited during the pilot. MAS would have complete control of the data and can be the "gatekeeper" • Pertaining to 3.1 (a) Misuse of Legal Persons and separate legislation governing Ultimate Beneficial Ownership Registry, mandating linkage of UEN to internal banking entity IDs and accounts will improve detection, assessment of potential illicit actors, as well as minimize risk of sharing legitimate customer information. **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.** • The framework should contain positive financial incentives for sharing risk information with MAS, other participating FIs and potentially non-COSMIC members as well to promote sharing between FIs and MAS. Given that no FI is perfect operationally, the "sharing" credits could potentially offset penalties or fines. Portions of any fines paid to MAS should also be committed to funding COSMIC platform enhancements. **Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC.** No Comment

		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. • Several of the initial COSMIC members share Actimize solutions and can leverage their respective existing configuration risk event types and thresholds to provide POC conditions to alert each other in accordance with local and cross-jurisdiction data sharing policies. • Most technology platforms, including Actimize, will have the ability to label risk events, transaction data, and entity level data with confidentiality levels to either hide or mask data to different user permissions settings. **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.** • We are unsure about the following statement: *"As there may be legitimate explanations for such red flags, MAS will also require the FI to seek an explanation from the customer as part of its risk assessment of potential financial crime concerns"*. Isn't this going to tip the customer off that they are being investigated? Typically, during AML investigations, customers are not contacted. This is different with fraud. In fraud there can be customer outreach because they may be a victim of fraudulent activities; however, in money laundering, typically, the customer is the aggressor in the activity. • In the US a publicly listed company was created in the early 2000's by a consortium of US FIs to essentially alert each other of fraudsters and attempts of fraud. Persons who have had their accounts frozen or closed have the opportunity to respond and defend the legitimate and legal use of their banking accounts consistent with the US Consumer Financial Protection Bureau requirements. (Sample: 201602_cfpb_checking-account-consumer-report-dispute-sample-letter.pdf (consumerfinance.gov)) • Related to the exiting of a client relationship, there was another area of question: *"Where a customer's activities exhibit the higher threshold of red flags, and the FI has filed an STR on the customer and decided to terminate the relationship, the FI should place an Alert on this customer on the "watchlist" in COSMIC".* - Every organization has different risk tolerances. What's not acceptable at one financial institution, may be acceptable at another. This could open up a way for those with higher tolerances to a "shopping list" of new prospects. - Another issue is that the person/entity may be watchlisted from banking at those large institutions. This forces bad actors to use smaller institutions with potentially less controls, and no visibility to the data in COSMIC. Ultimately it may force de-risking

		which has shown to have negative results in areas like correspondent banking. This should be limited to large losses, not every type of client exited. - In order to minimize the unintended impact of exiting and "de-risk" entities from a more effective financial crime framework to a more vulnerable and ineffective FIs, it may be worthwhile exploring a more gamified approach where riskier entities access is restricted, reduced, and limited while simultaneously revealing more of their identity, associations and financial activities within the COSMIC platform. Actively promoting and embedding legal language in each bank's terms and conditions will potentially dissuade bad actors from engaging with COSMIC FI members • The ideal framework will embed a shared standard to identify and classify a legal person and associated parties to view the financial crime risk consistently across the COSMIC participants. This foundation should exist as a prerequisite for the COSMIC participants to align identification of risk events and thresholds across all participating FIs. Risk events should reflect a holistic view of entity risk that includes Know Your Customer elements, AML screening and transaction monitoring elements, fraudulent behaviour, and perhaps 3rd party fraud attacks. The ability to proactively monitor risks, update, maintain, and align AML & suspicious activity typologies is also an essential component of the COSMIC solution. Risks can change over time; therefore, changes in risk should also be communicated to financial institutions to ensure they are monitoring their customers effectively.
12	Quantexa Pte Ltd	**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.** We believe that logging and auditing of all requests will be needed to safeguard the interests of legitimate customers. This auditing mechanism will also need to make it easy for an MAS analyst or investigator to verify that the system is being used in a proportionate manner. This auditing mechanism will need to be able to show the different data sharing actions (i.e. requests, provisions, alerts), the resulting networks of transactions and social relationships, the stated suspicions of the FIs and any AML risks detected by MAS' systems. **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.** Quantexa agrees that the collaboration of multiple FIs is key to detecting money laundering. We believe that the Request, Provide, Alert framework is fit for purpose. 1. We believe that speed of execution and timeliness of the FIs to react and respond to data that is shared regarding money laundering risk will be crucial in ensuring that COSMIC effectively disrupts financial crime. The money laundering networks that COSMIC uncovers will be inherently complex, and their complexity will increase for larger networks. The workload of the FIs will grow accordingly as they expand their

		network investigations and the investigations become more complex. We believe that the manual work required by the submitter and receiver will quickly become the bottleneck of the system. Therefore, we would suggest designing the system so that this manual task can be achieved by an AI-application which can automatically combine network analytics and risk scoring. This would require that element of the request and answer to use a standard data scheme. This data scheme should be network based in order to capture the complexity of a money laundering case. This will enable the system to generate networks of suspected money laundering spanning multiple FIs in a few seconds. It would also make it possible for a bank to suspend a transaction before it is executed. Quantexa would be happy to share more thinking on the best way to create these interfaces and handle the different requests consistently with MAS. 2. In order for the system to be comprehensive, the submitter and receiver will have to share a rich context of information around the persons/accounts/companies of interest. We recommend that this happens in the form of a network model such that each data sharing action results in a network being generated from all historical data available within COSMIC (i.e. historical submissions, alerts, STRs, transactions, ACRA records, etc). This will mean that for every submission from an FI which contains customer, related party and counterparty information (and every request for details of one of these entity types), COSMIC will automatically create a network which includes other connected entities (connected via shared addresses, businesses, additional transactions, etc.). Thus other FIs will be able to find direct connections between their internal data and the submitted details, as well as indirect connections via the extended network for the submitted entities. Entity resolution technologies will be key to identify the data of interest. High risk cases will need to apply a very high level of fuzziness when retrieving internal data in order to make sure that no potential information of interest is missed by the receiver. 3. Some scenarios will not be identified by a Request, Provide and Alert framework. Example 1, a U turn scenario will most likely not be detected if the cycle degree is not high enough (e.g. superior to 4). In order to still detect these scenarios, MAS could either implement transaction patterns detection as a central detection function (this will require to pool all of the historical data) or implement a detection engine that can be executed on multiple data indexes that would remain with the different FIs. As above, timeliness will be critical, so any network pattern detection will need to be capable of running in real-time, leveraging the full volume historical data. Quantexa would be happy to share more information on how to implement this with MAS. 4. The routing of the request will be a challenge when the requestor cannot identify all the FIs involved with the persons/accounts/companies of interest. In order to properly route these requests, MAS could implement a central entity resolution function (this will require to pool all of the historical data) or implement a detection engine that can be executed on multiple data indexes that would remain with the different FIs. As above, timeliness will be critical, so any entity resolution will need to

		be capable of running in real-time, leveraging the full volume historical data. Quantexa would be happy to share more information on how to implement this with MAS. **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.** No Comments **Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC.** No Comments **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.** No Comments **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.** No Comments
13	R3	**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.** We commend MAS's intent to strengthen the FI-FI information sharing paradigm to safeguard the interests of legitimate customers and prevent illicit actors. Today, each step in a banking transaction is viewed in isolation. But financial institutions (FI) require a holistic view of customers to understand the context of the customer's relationships and risk. Therefore, it is essential to create a data-sharing mechanism amongst FIs to better track such illicit activities by identifying the original sender, the in-between steps, and the destination. Historically, there has been resistance amongst FIs to share data with one another due to bank secrecy, data privacy issues and regulatory uncertainty around liability – we note that MAS intends to confer statutory protection from civil liability to FIs which participate on COSMIC. We also note that MAS will introduce a legislative framework to govern the sharing of risk information on COSMIC, whereby a customer must exhibit multiple high-risk behaviours or indicators that suggest serious financial crime before an FI is required to or may share risk information on that customer with other participant FIs.

		In such a situation, the efficacy of the system has a few dependencies. Firstly, accurate tracking of illicit activities is dependent upon the risk assessment framework used by the FI. This framework must be robust in order to ensure that no high-risk activities go undiscovered. Secondly, in a system where data is shared between parties, if there is a security breach due to operational failure or other reasons, this could be a problem for client confidentiality. Lastly, if an FI obtains proprietary information of another company's client data, this could arise in a situation of unfair data sharing. Newly developing viable technologies could potentially rebalance these dependencies by offering greater security together with more access to data. Some solutions include the use of Homomorphic Encryption, Secure Multi-Party Computation, Secure Enclaves, Zero-Knowledge Proofs, and Federated Learning all of which provide differing solutions and implementations to address data access and controls. Parties providing information can remain in control of the data, have it stored on-premise and access it in real time. Such privacy preserving technologies enable data to be shared to identify illegal activity within the banking system, without a need for trust amongst participating FIs, all while remaining in compliance with privacy regulation. This is in contrast to the situation today where there are only regulatory and legal impediments to prohibit any participant in the network from disobeying data rules, but no technological protection. Conclave is an R3 developed confidential computing platform that enables transactions to be aggregated in an encrypted form, without revealing the actual transactions to any of the other participating FIs. Leveraging confidential computing techniques, data is protected in transit, at rest and in use (rather than merely in transition) by performing a computation in a hardware-based Trusted Execution Environment (TEE). Using Intel SGX, TEEs allow programmes to run inside secure enclaves which are isolated from the rest of the computer on which they run. TEEs ensure that data and code can be processed without the owner of the computer gaining access to the raw data. As a result, programmes are resistant to physical and software attacks by the owner or operator of the computer, as well as by outside parties. This means that Customer data will be protected and cannot be viewed by the service provider or even cloud vendor. We strongly believe that Conclave can serve as an additional layer of technological protection to COSMIC and preserve customer confidentiality, information security and privacy. **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.** We commend MAS' initiative to propose an information sharing mechanism to support FIs' detection and assessment of potential illicit actors. Flagging suspicious activity often involves transactions between banks that are confidential.

		Solutions like Secure Multi-Party Computation (SMPC) protocols enable these transactions to be shared in an encrypted form, to allow them to remain hidden to the other parties. It offers Remote Attestation, a type of digital key, so parties involved may each audit how the data is being used and ensure that unauthorized entities cannot access it. With a Secure Enclave (solutions built into the CPU, thus providing hardware security) and blockchain, all parties providing information remain in control of the data at all times, as the data remains stored on-premise. Therefore, we suggest including such solutions into the information sharing system to provide technical assurance on how the requested and provided data will be processed in order to better encourage FI participation. **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.** We agree with MAS's imposition of 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. At the same time, we note that these legislative amendments are added security measures on top of the security features to be built in COSMIC. It is stated that COSMIC's security features will be in compliance with MAS, government-wide and government specific information and communication technology security policies and standards, and include the appropriate user-authentication mechanism, data encryption both in transit and at rest, as well as monitoring of security vulnerabilities. We would recommend going a step further and embedding COSMIC with confidential computing technology that permits data encryption in transit, at rest and whilst in use. This is possible with Conclave, R3's proprietary developer platform, that enables the development of applications that prove how data is used. Conclave allows application builders to develop new applications – or enhance existing – that aggregate sensitive data from multiple parties and provide technical assurances the data remains protected. As soon as the data leaves the FI's environment it is encrypted in transit, at rest and most importantly, in use. Conclave is a standalone platform but can also be used with R3's proprietary blockchain platform – Corda. **Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC.** No response.

		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. We agree with MAS's guidelines on permitting FIs to disclose information to overseas affiliates and third parties on a need-to-know basis and in compliance with the conditions put forth in Table A. We believe that distributed ledger technology (DLT) can be instrumental in ensuring these conditions are met. Corda is R3's signature permissioned DLT software and is used in a range of industries to record, manage and execute institutions' financial transactions in perfect synchrony with their peers. Corda is unique in the blockchain space by offering a platform modelled with open-source technology at its core alongside privacy, settlement finality, and scalability. The fundamental design decision of Corda, which was made at the very beginning, is that Corda allows for limited data sharing on a need-to-know basis, which facilitates compliant transactions between regulated institutions subject to reporting and data privacy regulations. We have also witnessed most governments' concerns around cross border data sharing arising as a result of data residency laws. Crucial for regulators, TEEs have a feature called Remote Attestation, where the TEE provides cryptographic proof that data will be protected, analysis of customer data conforms to regulations and that data will not be misused but processed as intended. By using TEEs, businesses can be sure that customer data is not misused by providing technological proof of how that data is protected when collected, shared and analysed. **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.** No response.
14	SALV OY	**General Comments:** Salv would like to congratulate MAS on their initiative in developing the framework for the COSMIC platform. Data and intelligence sharing in AML/CTF-PF has the potential to fundamentally disrupt finance crime on an unprecedented level. Over the past year, in collaboration with the Estonian Ministry of Finance, Financial Supervisory Authority, Data Protection Inspectorate, Financial Intelligence Unit and four leading Estonian banks (by market share: 90% of domestic market), Salv has been building a FI-FI data sharing platform and network across the Baltic States called AML Bridge. This has been operational now for four months. Designed to become Europe's first region-level AML information exchange network, the first cross-border exchanges between

		institutions in Estonia, Lithuania and the UK are set to take place in coming months. It is through the experience gained building the AML Bridge network that we believe Salv can offer some insights to assist MAS and COSMIC – after all, crime doesn't stop at the borders, and dedicated crime-fighters need regional, and eventually global, solutions. **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.** Salv commends MAS on the proposed framework and its safeguard messages – it is our belief that the COSMIC platform, as currently outlined, would be highly effective in reducing financial crime. Here are some additional observations for your consideration: 1. The regulatory framework drafted by MAS will give strong confidence to FIs within the network, removing concerns over the fundamental legality of information exchange – something that is repeatedly cited as a concern in Europe in projects such as AML Bridge. It is imperative however that this regulatory framework is drafted with the greater Asia-Pacific region in mind, not just Singapore, as different nuances in local AML/CTF legislation may act as a barrier for wider expansion with key regional banking partners and institutions. 2. In addition to ML, TF and PF, the COSMIC information sharing platform could be considered for a fraud or scam prevention use case. In Estonia, banks are preventing approximately €400K/month in scam proceeds using AML Bridge; given the relative size of Singapore this could easily be $3-5m SGD/month. As fraud or scam is often a predicate crime of money laundering, it has been our experience that the technology required for fraud/scam prevention is not radically different from AML/CTF-PF, so this could be a consideration for MAS. 3. We do not recommend that MAS become overly-prescriptive on red flag risk thresholds, as this might decrease the effectiveness of the network by limiting the flexibility and responsiveness of FIs. While it is key that any data exchanged be both necessary and proportionate, individual risk appetites within FIs vary (as do the quality of data inputs that determine these risk appetites). 4. We strongly agree that it is important to set consistent parameters around specific data formats exchanged. This plays an important role a) in preventing inadverted PII exposure, and b) in providing cleaner, more accurate inputs for centralised analytical tools. 5. Salv understands the political importance of MAS being the proprietary owner of COSMIC, but it is our suggestion that restricting this only to MAS could limit the potential scalability of the platform. As Europol's recent 2021 SOCTA report detailed, 7 out of 10 serious criminal gangs operate in at least three countries globally, and a globally-connected network will be critical to better protecting Singapore from AML/CTF-PF threats.

		6. A phased approach is heavily recommended, allowing MAS's engineers and development partners time to eliminate inefficiencies, align partners, and periodically review progress and assemble feedback. Salv has adopted this process with AML Bridge, and having concluded the first four months of information exchange, we have begun conducting participant workshops to help improve platform efficiency ahead of our phase two rollout and function expansion in 2022. **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.** It is Salv's opinion that, as currently outlined, COSMIC's three modes of information sharing provide an excellent basis, both for a) promoting immediately impactful collaborations within the three priority target areas, and b) for future expansion of the platform's scope and ambition. Some notes we would add: 1. That MAS has already considered use cases and scenarios is very positive, but Salv would also invite you to consider further how COSMIC will integrate with existing compliance processes within FIs. When initiating AML Bridge Estonia, Salv started with a long list of 15 potential use cases, but operational challenges from within FIs helped us fine tune what was a) realistic and b) most effective to implement immediately. 2. With FIs already conducting customer due diligence, screening, transaction monitoring etc across multiple compliance teams, the case management or case prioritisation mechanisms needed to optimise these processes for FIs using the COSMIC platform requires consideration. What teams are responsible for giving input for each request, provide, and alert? How does it link to their current work processes? What teams are the counterparties for each? Answering questions such as these will help optimise daily information-exchange processes. 3. It is Salv's recommendation to begin the process of information exchange between participant banks manually at first – as this helps reduce initial integration friction and also to better understand the needs and working processes of various internal teams. 4. It was our finding based on the AML Bridge Estonia experience that a prerequisite to building trust in the use of an information-exchange platform is physically bringing together participants in the network. No matter how sophisticated the technology is, ultimately investigative collaborations rely on a human element so building this trust face-to-face (or remotely as circumstances dictate) is key. **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.** Without a detailed study into the local characteristics of Singapore's AML/CTF legislation, Salv is limited in its ability to offer constructive feedback for MAS on

		COSMIC's domestic application. We can however present some insights from a European perspective: 1. That MAS is closely considering the legality of information sharing is very important; across the Baltic States and in other markets across the EU uncertainty arising out of seemingly contradictory legislative environments has been one of the key blockers to rapid network expansion – especially for FIs spanning multiple legal jurisdictions. 2. The recent September 2021 opinion statement from the European Data Protection Supervisor confirms the legality of data and information exchange across the EU, on the provision of strict data minimisation, in line with the principles of necessity and proportionality outlined in the General Data Protection Regulation (GDPR). 3. Salv commends MAS on the high standards outlined around the sharing of risk information. Any FI that wants to do business with EU-based institutions must meet GDPR standards. It is our opinion that MAS even surpasses these standards. **Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC.** Exposure to legal liability is a big concern for many FIs, especially for DPOs and MLROs, who are often held responsible within their organisations – despite the absence of clear guarantees from relevant legislation in this area. It is Salv's view that MAS's approach is more than adequate to protect FIs from undue legal risks; here however are some additional suggestions that could help build confidence on the part of FIs: 1. For the AML Bridge Estonia validation, the direct participation of the Estonian Data Protection Inspectorate (AKI) in outlining the scope and parameters of initial use cases was key to building the confidence of FIs, as was the creation of a AKI-approved demo environment for banks to familiarise themselves with a new process. That MAS is able to provide a regulatory green light for COSMIC is a major advantage over other legislative environments, but once again raises issues regarding the participation of FIs that are registered in other legal jurisdictions. 2. Salv commissioned numerous legal analyses before entering new jurisdictions – these have had a beneficial effect in providing assurance to participant banks. In a market such as Lithuania, for example, legal precedent of regulatory fines for improper data exchange created extra hesitance – working closely with participant DPOs in a sustained fashion has helped alleviate these concerns. 3. On a very general level, some protection is offered to networks such as COSMIC by the fact that globally, FIs are already exchanging large volumes of AML-relevant data through mechanisms such as Swift messaging. Which means, ensuring that the framework of COSMIC is more robust than existing information-exchange practices can only positively position COSMIC and MAS.

		4. The global recommendations of FATF also support the case for more ambitious information-exchange platforms. As a participant in FATF's recent data pooling report, Salv has had an active role in helping frame a more positive global environment for FI-FI information sharing. **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.** We should look at information sharing outside of Singapore in two different categories: 1. Sharing of information, related to performance or audit with entities outside of the network or outside of Singapore. 2. Sharing of information between the transacting parties in the global chain, taking into consideration all transacting parties are also part of the network. As for the first point we fully agree that information sharing, with third parties or overseas subsidiaries that are not part of the transaction chain, should be extremely limited and only allowed either for investigative purposes or group wide performance analysis and audit. But if we take the second category, during which overseas information sharing is happening between the parties in the transaction chain, then we see that the possibility to communicate with receiving parties or source parties has great effect in limiting cross-border money laundering. If information-sharing is happening between transacting parties, then customer data is exchanged already during the transaction. As detailed in Europol's 2021 SOCTA report, ML/TF/PF and fraud are mainly conducted across borders, which means limiting information-sharing only within individual nations will greatly reduce the possibility of tracking and stopping illicit actions. For Salv, the most important distinction therefore is whether information exchange is happening *inside* a controlled and restricted platform such as COSMIC or AML Bridge, or *outside*, rather than whether the exchange is happening across borders. **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.** Salv commends MAS for looking to mitigate the risks of potential financial exclusion to legitimate customers through unintended "de-risking". But mandating that every customer offboarded should be provided with "an adequate opportunity to address its concerns" *prior to offboarding* could have considerable operational implications for participating FIs.

		1. It is Salv's experience (during the time in which key Salv personnel built TransferWise's AML teams and products) that significant resources are already committed inside FIs to handling complaints processes involving offboarded customers – the large majority of whom often demonstrated clear and well-evidenced grounds for offboarding. 2. Any offboarded customer already has due process through the relevant financial supervisory body to go through an official complaints process; this provides the necessary and appropriate recourse for any wrongfully-handled customers to be given fair process. Adding additional operational costs for participating FIs will only de-incentivise participation in networks such as COSMIC, which are so important to the global fight against ML/TF/PF.
15	Sumitomo Mitsui Banking Corporation Singapore Branch	**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.** We seek clarification on how the framework will interact with STRs eg should information received via the framework be included in an STR and should the responding FI and information it provided be identified in the STR? If an FI lodges an Alert and STRO subsequently notifies there is insufficient evidence or that no further action is needed of the FI, should the Alert be removed or updated to reflect the response of STRO? Will there be any liability to the FI for not removing an Alert in those circumstances? The criteria for providing information via the framework may involve subjective interpretation of that information. Levels of analysis will also differ among different people. Will inadequacy of information or analysis invalidate the protection from liability? Will disclosure to prospective/existing customers of information contained in Alerts be permitted in order to get explanations from them on the transactions that led to the Alert? Otherwise is it the intention that FIs should not continue to deal with persons that have Alerts against them **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.** Will guidelines be provided on the timeframe to respond to Request messages, send Provide messages and place Alerts on customers and on what types of customer information can be shared and under what scenarios (how extensive information sharing can be) in order to avoid violating customer confidentiality **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. Will guidelines be provided as to the information security measures to be taken or will this be left to each FI to decide? **Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC.** It should be made clear that FIs are not obliged to provide platform information to the customers on whom information is lodged on COSMIC. The disclosure provisions are based on the Banking Act under which informing customer of its own information is not precluded. If the intention is for platform information sharing not to be disclosed to the customer concerned, it should be expressly provided for in the regulations. **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.** No comments **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.** We seek guidance on the extent to which we are allowed to inform the customer that the information was obtained from another FI especially in situations where it is obvious that we could only have got the information for which we are asking for explanation from another FI
16	Tokio Marine Life Insurance Singapore	**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.** We agree on the proposed framework and the measures as they will help to identify potential trends of illicit activities across different FIs. For clarity and better understanding, would this framework be stated as an exception within the PDPA regulations, as the current exception within PDPA under “Legitimate Interest” only highlights the collection, use and disclosure of personal data for investigation or proceedings as well as vital interest of individuals. This sharing of information does not seem to fall under the definition of investigation nor vital interest of individuals. “investigation” means an investigation relating to — (a) a breach of an agreement;

		(b) a contravention of any written law, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or (c) a circumstance or conduct that may result in a remedy or relief being available under any law; **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.** We would like to clarify on the following under the three modes of information sharing: Request – The Consultation Paper (CP) states that "Where a customer …., it may request for risk information on the customer from other FIs which are linked to the activity." We would like to clarify, assuming we have no knowledge of which FI the customer has relationship with, are we able to utilise this mode to request for information from any FI? Provide - We would like to clarify whether MAS plans to standardize the turnaround time across all FIs. Alert - The CP states that FIs need to provide the reasons for placing a customer under "Alert" status and we assume that this will be subjected to approval by MAS. We would like to seek clarification if MAS (due to certain reasons) rejects to place the customer under "Alert" status, will MAS provide the reason(s) for rejection and should the FI then re-classify this customer to be of a lower risk. **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.** We would like to clarify the extent of sharing i.e. whether there is a limit to the risk information sharing to those persons who are permitted under Annex B. Also, a possible concern is that if a red flag and threshold criteria is not known to a wider spectrum of the FI's employee base, this may limit the effectiveness of the information sharing and reporting of suspicious activity by FIs on the COSMIC platform. However, we also understand that MAS wishes to limit access to such information and criteria, in order to avoid circumvention by bad actors. Therefore, we propose that the qualifying criteria be further tightened for the officers who shall be privy to the red flag and threshold criteria. Under Annex B Part II, there seems to be a contradiction between second and third column. Second column states that we are allowed to share information with "officer designated in writing by the head office or parent company of the prescribed financial institution". However, if a designated officer is based outside Singapore, information

		shared to the officer has to be anonymised. That being the case, it may dilute the purpose of such information sharing. Lastly, will there be guidance on the measures required by FIs to put in place to safeguard the confidentiality as this may help to standardise the requirement across all FIs. **Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC.** In principle, we agree that the proposed statutory protection is generally sound. However, we note that the draft provision is worded quite broadly to exclude civil liability in its entirety and it also makes it clear that any such disclosure shall not constitute a breach of any restriction upon the disclosure of information as imposed by any written law, rule of law or contract. It would be good if MAS is able to illustrate some examples on this. Secondly, we propose to include the sentence highlighted in yellow in Annex B - X13. As this section makes reference to Section 39 of CDSA, it would be good to include the statement below to align to Section 39(6) of CDSA. (screenshot reproduced below) **Immunity for disclosure** X13.—(1) No civil liability shall be incurred by a prescribed financial institution or any of its officers for disclosing any information in accordance with sections X7, X8 or X9, including liability for any loss arising out of the disclosure or any act or omission in consequence of the disclosure, if he had done so with reasonable care and in good faith. (2) A prescribed financial institution which discloses any information in accordance with sections X7, X8 or X9 shall not be treated as being in breach of any restriction upon the disclosure of information imposed by written law, any rule of law, any contract or otherwise. **Section 39 (6) of CDSA** (6) Where a person discloses in good faith to a Suspicious Transaction Reporting Officer – (a) his knowledge or suspicion of the matters referred to in subsection (1)(a), (b) or (c); or (b) any information or other matter on which that knowledge or suspicion is based, The disclosure shall not be treated as a breach of any restriction upon the disclosure imposed by law, contract or rules of professional conduct and he shall not be liable for

		any loss arising out of the disclosure or any act or omission in consequence of the disclosure. **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.** We would like to seek clarity on the extent of sharing with permitted persons in Annex B. For e.g. if the FI has a customer who falls under the alert list, we may need to seek advice from head office on the treatment of this customer and sometimes external counsels may be engaged. Also, parent company may request for extensive information from the FIs as part of the reporting obligation. Certain AML/CFT functions may be out-sourced to service providers outside Singapore. It would therefore be helpful if MAS would elaborate on the conditions that would be imposed in such circumstances in X11 Schedule Part II(3). **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.** We agree that it will be beneficial for customer to explain the activity or behaviour as this will shed some insight and assist in the assessment by the FIs. However, it may not be a common practice yet to ask for justifications during off-boarding of customers. This is because contractually, under certain circumstances, customers are allowed to exit or FIs are allowed to end the relationship without going through this step. The requirement may thus have the unintended consequence of alerting customers of potential suspicions by the FI and/or authorities.
17	Wise Asia-Pacific Pte. Ltd.	**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.** Wise Asia-Pacific Pte Ltd (Wise) welcomes the opportunity to provide comments on the consultation paper on FI-FI Information Sharing Platform for AML/CFT. By way of background, Wise is a global technology company, building the best way to move money around the world. With the Wise account people and businesses can hold more than 40 currencies, move money between countries and spend money abroad. Large companies and banks use Wise technology too, an entirely new cross-border payments network that will one day power money without borders for everyone, everywhere. However you use the platform, Wise is on a mission to make your life easier and save you money. Wise fully supports smart intelligence sharing initiatives as a means to prevent 'information silos', support FIs to disrupt criminal activity and strengthen the integrity of the Singapore Financial System.

		We would like to highlight two potential policy concerns: exclusivity of the platform and mandatory penalties that we believe will reduce the impact of the initiative. **1. Exclusivity of the platform** Wise encourages MAS to consider in the pilot allowing a broader range of financial institutions (FI) to participate. The initial phase of the program will only have bank participants. By only allowing banks, the systems and processes will be bank-centric. The platform would have more impact with a variety of FI perspectives and data sets. By allowing other FI to apply initially, sharing protocols that get established would be fit for purpose for more FIs at a later stage. We share MAS' concern, articulated in section 5.2 of the consultation, where illicit actors may shift their activities to FIs that are non-participants within the FI-FI sharing platform. This appears to be counter-intuitive to the overall objective. As such we have the following questions / comments: a. We suggest Major Payment Institutions to have the option to participate initially. As Trade-Based Ml and Proliferation Financing are MAS' priority targets, including larger volume payments, FI would be useful since both of these targets heavily involve cross border wire transfers. Further to this, MPI are required to meet a higher standard of technology risk management standards and cyber hygiene. b. New participants to the platform should be given a 'grace period,' to integrate and share information without penalty. This will allow FIs time to adjust, forecast and engage resources to fully support information sharing. c. We strongly recommend FIs have an option to opt-out of the platform. The aim is to encourage information sharing for the benefit of the Singapore Financial system, however, there may be operational or resource constraints that inhibit participation. The framework should allow FI to make that determination. d. Non-participating FIs would be in a disadvantaged position. All FIs are part of the same ecosystem, where any given payment likely involves multiple local banks and non-bank FIs. Participating banks will be able to communicate suspicion easily, allowing those FI to effectively handle a customer. Non-participants, however, are disadvantaged as we would not have access to the same information and therefore consume resources investigating why a participating bank is not cooperating on a transaction and / or potentially execute transactions with another non-participant that should be disrupted. e. In section 5.2, MAS states that it, '...step up our supervisory engagement of FIs that are not on COSMIC, to warn them of such instances and provide guidance to tighten their AML/CFT controls'. Wise welcomes input and engagement from MAS. For the purpose of information sharing, we strongly recommend warnings are able to be distributed and consumed via application programming interface (API). For example,

		where intelligence is received via .pdf or email it cannot be easily consumed into systems without a high degree of manual intervention. Exclusion of payments FI and non-bank FI will be counter intuitive to the aims of information sharing initiatives and jeopardise the integrity of non-participants the Singapore financial system as a whole. **2. Mandatory requirements for participants with penalties** Wise supports minimum standards and requirements of data sharing to enable participating FI to receive timely data requests. At a time when non-bank FI can participate, further consideration should be given to making the timeliness and penalties proportionate to size of the participating FI. For example, mandatory 'Provide' responses would disproportionately allocate resources to support non-bank FI. We are also concerned about how onerous the requirements might be as well as the severity of the underlying penalties. As it stands, these provisions provide a disincentive to sharing of data to combat financial crime. We have the following comments: a. Data sharing "Request", "Provide" or "Alert" should be on a voluntary basis. The requirement for mandatory submissions that have to be within a specific timeframe are potentially restrictive and may be a barrier for entry for FIs as there is no way to estimate whether or not it is pragmatically possible a non-bank FI to be able to meet the relevant minimum standards and requirements that MAS may set for this. The FATF Recommendation of Private-Sector Information Sharing also suggests voluntary sharing in Para 83. In the US and in the UK(JMLIT), FI cooperation is voluntary. Further to this, JMLIT has extended membership to non-bank FI, as they are key players in the UK financial ecosystem. b. We ask MAS to share data on volumes of information sharing requests to help non-bank FI determine whether participation is feasible. c. Resulting penalties for not meeting the minimum reporting requirements are extreme and disproportionate to the size and scale of non-bank FI. We fully agree that penalties for confidentiality, information security and privacy are logical and necessary, however we view the proposed penalties for reporting timelines are excessive. Wise strongly recommends MAS consider a membership model, where a requirement of membership is timely responses to requests for information. Non-compliance with timeliness provisions would result in exclusion from the platform. We believe this approach will achieve the result MAS is looking for, where participants are incentivised to share information but does not disenfranchise non-bank FI who may not have capacity, resources or risk appetite to join.

		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. Wise has no comments on the proposed model of 'request, provide and alert'. With reference to our response in '1. a.' to question 1, MAS should consider API warnings to non-participants in the event that non-participants are connected to a case. This would assist non-bank FI to assess alerts in a timely and cost-efficient manner. **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.** Wise has no comments on the proposed legislative amendments to permit the disclosure of risk information 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. However, Wise views that requirements relating to making the mandatory submission and the timing / timeframe of submission are restrictive and will be a barrier for other FIs to participate. **Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC.** Where MAS considers sharing of warnings via API to non-bank FI connected to a case, we ask MAS to extend statutory protection to those same non-bank FI. **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.** No Comment **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.** Treating customers fairly is central to the Wise mission. The current proposal requires further consideration of compliance with tipping-off provisions in section 48 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act. As an issue of fairness, we take the view customer fairness should already be a consideration for FIs. This issue could be further considered by MAS holistically as part of a review of de-banking within Singapore.
18	Respondent A	**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. The proposed provisions applied to "prescribed financial institutions" as prescribed by MAS under section X14, as defined in section X1. AML/CFT requirements does not apply to Exchanges and Clearing Houses as these AML/CFT requirement are performed by the members of the Exchanges and Clearing Houses. As such, we would like to clarify if Exchanges and Clearing Houses will not be prescribed as a "prescribed financial institution".
19	Respondent B	**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.** Broadly, we agree with MAS' approach to provide a platform for FIs to share information about high risks customers to sharpen our ML/TF/PF awareness. We understand that MAS will set out high-risk indicators and threshold criteria for FIs, who will be mandated to "Request", "Provide" or "Alert" accordingly. We would like to clarify if the FI will have the discretion to take the required actions on COSMIC depending on the number of indicators that were breached, or would actions be required as long as any indicators has breached the threshold. Furthermore, MAS has set out examples of such high-risk indicators. We note that indicators may be qualitative in nature (e.g. providing evasive or giving inconsistent replies) and may not be easy to determine a "threshold" for such indicators. Broadly, we think the COSMIC system will be useful in enhancing the gathering of information on high-risk customers. However, as ML/TF/PF activities may be carried out under different names and amongst groups of people, we would like to clarify whether there will be any functionality on COSMIC to share information based on groups of related names instead of individual name. **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.** We note that FIs can seek information through a "Request" message to another FI should there be red flag(s) observed. We would like to clarify if a "Request" message will also warrant the FI to also submit a "Provide" message to other relevant FIs as certain high-risk indicators may have been triggered. Paragraph 3.12 of the consultation paper states that 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. Will there be any controls to prevent FIs from requesting for information of a person who is not its existing customer?

		Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC. We agree that statutory protection from civil liability provides confidence for FIs to share information through COSMIC. We would like to clarify if MAS will also provide an exemption for FIs from the requirement to obtain the respective individual's consent for disclosure of personal data (under the Personal Data Protection Act) via COSMIC.
20	Respondent C	**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.** •Unlevel playing field if only selected banks are invited to participate in COSMIC, as legitimate clients who may have concerns about their information being shared may move their accounts to non-participating banks. This would be a real concern for private banks and we hope that MAS will take this into account should COSMIC be extended in the next phase. •If the information sharing is resulting from STRs filed by FI, MAS or the central party would already have the relevant BO/RP and transactional information. How the STR information is to be shared can be centrally managed. Shouldn't any FI be able to query this centrally managed information to check if a prospect/client has any concern? As a consideration, MAS can also include those that cross threshold into alert list to be included in FI name screening engine. **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.** De-risking of legitimate customers: While MAS is proposing to introduce requirements for FIs to provide for an opportunity for customers to be heard, query whether this is sufficient to eliminate de-risking risk as an FI would be put on the defensive should it choose to retain a customer flagged on COSMIC. As MAS/STRO will also be following up on information leads from COSMIC, perhaps there could be process of refreshing info on COSMIC. If the authorities have "closed" a case, that could be indicated on COSMIC.
21	Respondent D	**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.** We applaud this COSMIC initiative. The sharing of insight and information among the crime fighting ecosystem is necessary to combat the ever-evolving criminal landscape. We were compelled to make this submission before the MAS and the FIs embark on this strategically important and economically critical system design journey in order to

		share our deep experience of data sharing systems design, development and implementation. **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.** The design of the proposed COSMIC Platform assumes that information/data must be (a) centralised and (b) shared outright. We seek to challenge this design decision for the following reasons: 1. Centralisation has time and again been proven to increase the risk, duration and cost of projects. Risks are increased primarily because one entity is designated as the custodian of the new data. Costs are increased for numerous reasons: data is unnecessarily duplicated (also has a negative environmental aspect), the transformation of data into a new centralised format increases the costs for FIs and consequently increases the time needed to implement the system and reduces the voluntary adoption of the platform. 2. Sharing the data outright increases the risk to FIs and therefore ultimately reduces the effectiveness of the COSMIC platform. In practical terms, before an FI decides to share data (even if the sharing is mandated by law), the FI must satisfy itself that the sharing of information is compliant. This will require FIs to develop and implement new policies and procedures in writing and then implement them through systems. 3. Finally, this design approach achieves the following negative effects: a. Any extension of the initial data sharing assumptions will require the participants (FIs and MAS) to conduct the same process again for the new data (new system design, new legislation, new policies and procedures etc.) b. It is well known that the information needed to fight financial crime is not just present with the FIs. Indeed, the best analytics usually comes from combining the data of FIs with law enforcement agencies. The current proposal does not immediately include law enforcement agencies. c. The current proposal does not enable analytics of patterns of fraudulent transactions. Criminal activities are ever evolving. New criminal patterns emerge all the time. AML/CTF analytics usually requires the continuous development and improvement of models which should have access to data continuously in order to address model decay. d. Finally, the current design assumes that all relevant information and players who must provide information are present within the jurisdiction of Singapore. Financial crime is cross-border. 4. If the design approach is a simple messaging system rather than a centralised data platform, then the proposed COSMIC platform will not enable analytics but rather sharing of specified limited information in a manner that is heavily FI dependent. The

		MAS could be missing an opportunity to implement a data sharing platform that enables the achievement of all the FATF recommendations around data sharing. We felt compelled to make this submission to bring a new perspective to the attention of the MAS and the FIs. While centralisation of data remains a common model, the technology industry is moving away from it at pace because it is highly inefficient. More time and resources are spent on the centralisation infrastructure than on the analytics. While the reason for the centralisation is in fact the analytics (inform FIs and the MAS of criminal activities). Coronavirus 'track and trace' technology is one well known application of this decentralised approach to analytics. A simple messaging system would not achieve the policy intent of data sharing initiatives as it does not enable data sharing in a scalable manner. **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.** The outright sharing of data is always risky for FIs and will merit case by case analysis of whether they are legally able to or compelled to share information. Usually, such matters are dealt with at a global level and through internal policies and procedures of FIs which will certainly be different as regulation is usually principle based. Accordingly, there is a high likelihood that at least one FI will, at some point, not agree to share information. The sharing of insight rather than private information would reduce this risk.
22	Respondent E	**General comments:** Just to clarify, I note that paragraph 13.4 under MAS Notice 626 already gives FIs the power to share customer information to third parties without obtaining customer consent, if it is in relation to AML/CFT issues: *13.4 For the purposes of complying with this Notice, a bank may, whether directly or through a third party, collect, use and disclose personal data of an individual customer, an individual beneficiary of a life insurance policy, an individual appointed to act on behalf of a customer, an individual connected party of a customer or an individual beneficial owner of a customer, without the respective individual's consent.* Thus, I would just like to clarify how the above paragraph would interact with COSMIC, and the proposed legislative framework proposed. This is because it seems like the new legislative framework may not take into consideration paragraph 13.4. For example, can a FI share customer information with another FI <u>today</u> for the purposes of AML/CFT, relying on 13.4? If so, then how would the new legislative framework apply vis-à-vis 13.4 (e.g. would MAS Notice 626 take precedence)?

		If 13.4 can be applied today, then theoretically, COSMIC can be launched without the need for any further legislative amendments since COSMIC will help FIs comply with 626?
23	Respondent F	**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.** Nil **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.** Nil **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.** Nil **Question 4: MAS seeks comments on whether the proposed statutory protection adequately covers FIs against undue legal risks arising from disclosing information via COSMIC** Nil **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.** Nil **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.** • In most cases, the bank would have checked discreetly with the customer on the unusual activities or transactions prior to determining if the activities or transactions are suspicious and the resulting decision to file a STR and exit the customer relationship. However, there are certain scenarios which will pose operational challenges/practical difficulties to the banks to review the relationship before the exit: i) The customer is uncontactable and therefore the bank may not be able to obtain the information or explanation

		ii) the customer is in the retail banking segment where there is no dedicated relationship manager. • We would suggest the Authority to allow certain exceptions/situations where the bank may not be required to review the relationship to ease the operational burden. • We are also concerned that the bank may risk tipping off the customer and contravene the regulations governing tipping off and hence, we would suggest to have regulatory safeguards to protect the bank against such legal risks. • Alternatively, the Notice may be revised to provide flexibility to the bank to determine and document the reason NOT to provide the customer with an opportunity to address its concerns. This is because in some cases, it may be relatively straightforward that the unusual activities and transactions are suspicious or highly possible to have contravened other regulations based on our understanding of the customers' business / adverse media and thus the bank has decided to exit the relationship without checking with the customer so as to avoid risk tipping off the customers.