CONSULTATION PAPER

P013 - 2021

October 2021

FI-FI Information-Sharing Platform for AML/CFT

Monetary Authority of Singapore

Contents

1 Preface

1.1 The Monetary Authority of Singapore ("MAS") is consulting on the introduction of a regulatory framework and platform for financial institutions ("FIs") to share risk information with each other to prevent money laundering ("ML"), terrorism financing ("TF"), and proliferation financing[1]("PF").

1.2 MAS invites comments from FIs and other interested parties on the proposed regulatory framework and information-sharing platform.

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

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

(ii) their identity along with their whole submission,

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

1.3 Please submit written comments by **1 November 2021** to –

Anti-Money Laundering Department
Monetary Authority of Singapore
10 Shenton Way, MAS Building
Singapore 079117
Fax: (65) 62203973
Email: amlcft_consult@mas.gov.sg

1.4 Electronic submission is encouraged. We would appreciate that you use this suggested format for your submission to ease our collation efforts.

[1] Proliferation Financing refers to the raising, moving or making available funds other assets or other economic resources, or financing, to individuals or entities for the purpose of weapons of mass destruction proliferation, including the proliferation of their means of delivery or related materials.

2 Introduction and Background

2.1 Singapore's anti-money laundering and countering the financing of terrorism ("AML/CFT")[2] defences have strengthened in recent years, through sharpened ML/TF/PF risk awareness amongst FIs, greater use of data analytics by FIs and MAS, and closer public-private partnership, to identify and disrupt criminal activities and networks. However, a remaining weakness is that FIs are not permitted to warn each other about potentially suspicious activity involving their customers. As such, each FI's understanding of their customers' risk profile is limited by the information the FI collects. Criminals have been able to exploit this weakness by conducting transactions through a network of entities holding accounts with different FIs, such that each FI by itself does not have sufficient information to detect and disrupt illicit transactions in a timely manner. Allowing FIs to share information on customers that cross certain risk thresholds enable them to break down these "information silos" and more effectively detect and disrupt criminal activities, reducing any harm done to the integrity of Singapore's financial centre.

2.2 FIs are required to file a suspicious transaction report[3] ("STR"), if they have reasonable grounds to suspect that a customer is involved in ML/TF/PF activities. Such STRs have played a key role in the detection of a number of significant cases. Allowing FIs to query and alert each other on potential illicit behaviours will enhance the quality of STRs filed by enabling FIs to better assess for suspicion. It will also scale more timely detection of illicit actors, and allow MAS, law enforcement agencies and FIs to act early to disrupt criminal networks, to stem material damage to Singapore's financial system.

[2] AML/CFT controls includes counter proliferation financing controls. A failure or refusal to comply with the various regulations or direction issued or made under section 27A of the MAS Act to discharge or facilitate the discharge of any obligation binding on Singapore by virtue of a decision of the Security Council of the United Nations is a serious offence under the Corruption, Drug Trafficking and Other Serious Crime (Confiscation of Benefits) Act ("CDSA").

[3] Under section 39(1) of the CDSA, where a person knows or has reasonable grounds to suspect that any property –

(a) in whole or in part, directly or indirectly, represents the proceeds of;

(b) was used in connection with; or

(c) is intended to be used in connection with,

any act which may constitute drug dealing or criminal conduct, as the case may be, and the information or matter on which that knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment, he must disclose the knowledge, suspicion or the information or other matter on which that knowledge or suspicion is based to a Suspicious Transaction Reporting Officer as soon as is reasonably practicable after it comes to his attention.

2.3 Therefore, MAS proposes to introduce a legislative framework and to develop a secure digital platform for FIs to share information with each other[4]. Such information would include information relating to, or particulars of, a customer[5] (e.g. the beneficial owners and authorised signatories of a customer) and transactions, the high risk behaviour exhibited, and risk observations or analysis that are relevant to the account or customer ("risk information"). FIs will also be able to review the risk information shared on the platform using data analytics to disrupt illicit transactions. This enriched set of risk information will enable FIs to conduct sharper analysis of customer behaviours and activities, as well as alert each other to situations which pose higher financial crime risks, thus raising overall defences for Singapore's financial system. The benefits of information sharing amongst FIs have also been recognised by several major jurisdictions. In designing the regulatory framework and risk information sharing platform, we have sought to learn from the successes and challenges faced by these jurisdictions, such as the United States and the United Kingdom, which have regimes to facilitate FI-FI information sharing for AML/CFT purposes.

2.4 The aim of sharing risk information through the platform is to prevent illicit actors from exploiting information gaps between FIs. At the same time, it is necessary to safeguard the interests and privacy of legitimate persons and minimise any undue inconvenience to them. Hence, it is intended that such sharing will be permitted only:

(a) to address potential ML, TF or PF concerns in key risk areas;

(b) if the customer's behaviours and transaction activities exhibit multiple red flags that cross risk thresholds to suggest that potential financial crime could be taking place;

(c) in the data format specified by MAS, such that only relevant risk information is shared, and in a proportionate manner[6]; and

[4] The Financial Services and Markets Bill is targeted to be introduced in Parliament later this year. MAS intends to amend this new Act ("FSMA") to include this framework.

[5] For the purposes of this consultation, given that the participating FIs in the initial phase are banks, we have used the term "customer" in this consultation paper. However, in the draft provisions as set out in Annex B, the term "relevant party" is used instead to allow for the possible inclusion of other types of parties as MAS progressively extends COSMIC to a wider segment of the financial sector in the future. MAS intends to prescribe in subsidiary legislation the types of "relevant party" for each class of FI participating on COSMIC.

[6] The extent of risk information shared by FIs should be strictly relevant and necessary for the purposes of assessing ML/TF/PF risks.

(d) via a secured digital platform owned and operated by MAS, to be named the Collaborative Sharing of ML/TF Information & Cases, or COSMIC in short.

For the vast majority of individuals and companies that are legitimate and do not exhibit risky behaviours, FIs will have no reason to share their customer's information, nor will they be allowed to.

2.5 COSMIC will be developed and deployed in phases, to ensure operational stability and efficiency. In the initial phase, we intend to focus on combating the key risk areas of misuse of legal persons, trade-based ML, and PF. The initial participants will be six banks which are major players in the commercial and small-medium enterprises (SME) banking segment: DBS, OCBC, UOB, Standard Chartered Bank, Citibank and HSBC[7]. Together with the Association of Banks in Singapore, we have involved the banks extensively on the design of the key features of COSMIC, to support effective and efficient risk detection.

2.6 To allow participant FIs adequate time to familiarise themselves with this new paradigm, information-sharing on COSMIC will be voluntary in the initial phase[8]. Subsequently, certain aspects of information sharing will be made mandatory[9], in order to realise effective detection outcomes. MAS will progressively extend COSMIC to a wider segment of the financial sector and increase the key areas of focus where appropriate in the subsequent phases. The features of COSMIC and its safeguards are elaborated upon in the following sections, and further details on the phased implementation of COSMIC are set out in paragraph 5.

3 Key Information-Sharing Features of COSMIC

Focus on key risks

3.1 Sharing of risk information through COSMIC will focus on detecting key ML/TF/PF risks, which have been identified as priority targets for mitigation in line with Singapore's

[7] MAS will also step up supervisory surveillance and engagement to address the risk of criminals shifting their illicit activities to other FIs.

[8] The initial phase is expected to last for approximately two years. MAS will review and adjust this period as necessary to achieve operational stability and to provide participant FIs adequate implementation run-way.

[9] Please refer to paragraphs 3.6 to 3.13 of this consultation paper and sections X7, X8, X9, Y7, Y8 and Y9 of the draft provisions set out in Annex B for the requirements that will be made mandatory after the initial phase.

national strategy to combat serious financial crime. In COSMIC's initial phase, sharing will be permitted to detect and disrupt:

(a) **Misuse of legal persons**: The ease of setting up a company in Singapore and opening a local bank account contributes to our attractiveness as a commercial centre. This competitive advantage must be safeguarded from abuse by criminals. Internationally, the misuse of legal persons to launder illicit proceeds and disguise their origin is a dominant financial crime concern. It is also a material risk for Singapore: the Singapore Police Force's Commercial Affairs Department ("CAD") and MAS have observed cases of shell companies being used to launder suspicious or illicit flows, e.g. scams, as well as the use of front companies to evade sanctions imposed by the United Nations Security Council.

(b) **Trade-based ML:** International trade is an important engine of the Singapore economy. However, global trade is also an attractive guise for criminals seeking to transfer illicit proceeds across borders, as these can be hidden amidst flows of large volume and value. Mitigating such trade-based ML is important to protect the trust in our FIs and companies, so they can continue to engage in and facilitate legitimate regional and global trade flows.

(c) **Proliferation financing:** Singapore's deep financial and trade linkages globally are also vulnerable to being exploited for PF, which is the illicit financing of weapons of mass destruction, as well as the evasion of international sanctions. For example, companies and individuals in Singapore have been charged and convicted of supplying prohibited items to the Democratic People's Republic of Korea (commonly known as North Korea) in violation of United Nations sanctions. Such cases involved the use of front companies and middlemen to disguise the criminal activities.

3.2 To evade detection by FIs and the authorities, criminals engaged in PF, trade-based ML and the misuse of legal persons to create networks of accounts or business relationships across multiple FIs, and transfer illicit funds amongst them to disguise the origins of the funds. They may also present fictitious trade or business documents to justify these transactions and/or obtain financing. Through COSMIC, FIs will be able to share risk information on these bad behaviours and unusual transactions of customers with each other to more effectively identify illicit networks, ascertain if a customer's explanation bears out, and warn each other of potentially suspicious customer activities.

Red flags and thresholds for information sharing

3.3 MAS recognises that sharing of risk information amongst FIs, if done indiscriminately, raises legitimate concerns about customer confidentiality, information security and privacy. MAS will thus introduce a legislative framework to govern the sharing of risk information on COSMIC. This will ensure that information is shared only for AML/CFT purposes[10] and in a proportionate manner, to enable an FI to examine whether there are reasonable grounds for suspecting its customer of illicit activity, or warn other FIs that a customer is engaging in potentially suspicious behaviour.

3.4 Under the proposed framework, a customer must first exhibit multiple high risk behaviours or indicators that suggest serious financial crime ("red flags"), before an FI is required to or may share risk information on that customer with other participant FIs. This sets an objective threshold to ensure that COSMIC is used only for cases of significant concern, and safeguards against frivolous requests that unnecessarily expose customer information. 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.

3.5 The thresholds and red flags are based on typologies of past cases, both domestic and global, in the key risk areas mentioned in paragraph 3.1. These indicators will be adjusted over time as criminals' methods evolve. While the details and permutations of the red flags have to be kept confidential to avoid circumvention[11], broadly speaking, these will include:

(a) indications that a company's profile may be fictitious;

(b) the customer undertaking a series of financial transactions with unclear economic purpose, such as "round tripping" funds back to their sender, rapidly passing

[10] AML/CFT purposes include purposes relating to counter proliferation financing.

[11] 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. Specifically, FIs may be liable on conviction to a fine not exceeding $1 million and, in the case of a continuing offence, to a further fine of $100,000 for every day or part of a day during which the offence continues after conviction. In the case of an individual, he/she may be liable on conviction to a fine not exceeding $125,000 or to imprisonment for a term not exceeding 3 years or to both. The proposed penalties are aligned with current penalties under section 27B(2) of the MAS Act for breaches of requirements for prevention of ML and TF.

monies from one party to another, or receiving or making sizeable payments from/to parties in unrelated industries;

(c) the company being evasive or giving inconsistent replies to the FI's queries about its unusual behaviour, or providing supporting documents that do not appear genuine; and/or

(d) indications that seemingly unrelated companies conducting business with each other may in fact be operated or controlled by the same beneficial owners, with unusual patterns in the transactions amongst them.

Modes of information sharing

3.6 Under the proposed framework, an FI will be able to share risk information with another FI through COSMIC in three ways, i.e. Request, Provide and Alert.

Request

3.7 Where a customer has exhibited some red flag behaviour and an FI requires more risk information to assess whether there are reasons to suspect that its customer is involved in illicit activity, it may request for risk information on the customer from other FIs which are linked to the activity.

3.8 A **Request** message must be focused on clarifying a potential suspicion involving certain red flag behaviour that the customer has exhibited. The message should explain the context of the Request, including the red flags observed and relevant risk information on the customer[12], and the FI can only seek information that would help the requesting FI to either establish or clear suspicions on its customer. The receiving FI 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[13].

[12] Relevant risk information on the customer would include its particulars and (where applicable) those of its directors or beneficial owners, such as their name, date of incorporation or birth, residential and/or business address, nationality or place of incorporation, and unique identification number. It would also include any transactions or other information that led to the Request being sent. Such information is critical to help FIs accurately identify the criminals engaging in red flag behaviours, and avoid "false positives" that would inconvenience legitimate customers.

[13] In the initial phase, the requirement for a receiving FI to furnish the requested risk information will be non-mandatory. This requirement will be made mandatory after the initial phase (please refer to section X7 and Y7 of the draft provisions in Annex B)

The receiving FI may also use the risk information it has received from the Request to perform an AML/CFT assessment of its own customer.

Provide

3.9 Where the customer's unusual activities cross a higher threshold, indicating a greater risk of the customer being involved in illicit activity, an FI would have to proactively provide risk information on the customer to other FIs with a link to the customer's activities.

3.10 This means that an FI should send a **Provide** message to another FI on COSMIC if its customer's behaviour crosses the relevant threshold[14]. As with Request messages, the Provide message should explain the context of the concern, including red flags observed and relevant risk information on the customer. An FI must upon receipt of a Provide message, perform an AML/CFT assessment of its own customer within a reasonable time period, taking into account the information received. If necessary, the receiving FI may also make a further Request and/or issue more Provide messages to the same FI or other participant FIs.

Alert

3.11 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"[15] in COSMIC[16]. As with Request and Provide, the FI should explain in its submission its reasons for concern, including red flags observed and relevant risk information on the customer. Participant FIs on COSMIC should

[14] In the initial phase, the requirement for a participant FI to send a Provide message will be non-mandatory. This requirement will be made mandatory after the initial phase (please refer to section X8 and Y8 of the draft provisions in Annex B).

[15] FIs should not reject or exit a customer solely based on the fact that the customer is placed on the COSMIC watchlist. The FI should provide the customer an opportunity to explain the unusual behaviour and perform its own risk assessment based on the information obtained from the customer, which may provide additional or new perspectives on the risk level of the customer. Based on this assessment, the FI may decide to exit or retain/ onboard the customer, and should ensure that the assessment and decision are properly documented.

[16] In the initial phase, the requirement for a participant FI to place an Alert on the customer will be non-mandatory. This requirement will be made mandatory after the initial phase (please refer to section X9 and Y9 of the draft provisions in Annex B). Participant FIs will be required to ensure that information shared on the platform is accurate and complete. They will be required to rectify and update the risk information of the customer, including the information in the watchlist, where they receive further details that clarify or rectify it.

check if a prospective or existing customer is on the watchlist and use the risk information as part of their AML/CFT assessments on prospective or existing customers.

3.12 To ensure that FIs share risk information appropriately and for the specific purpose of combating ML/TF/PF, an FI must first assess that the customer has crossed the stipulated thresholds which would be based on combinations of red flags the customer exhibits, before initiating risk information sharing via COSMIC. 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. The materiality thresholds are set higher for Provide and Alert, as these are higher-risk scenarios where the FI should proactively warn the other FIs.

3.13 FIs should also respond to Request messages, send Provide messages and place Alerts on customers within a reasonable time period so that the information from COSMIC is received and can be acted upon in a timely manner. Material networks of suspicious actors and activities, forming across FIs, will also be automatically escalated by the platform to MAS for further analysis and follow-up. [17]

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.

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.

4 Legal Basis for Sharing and Use of Information

4.1 The legal framework for COSMIC will be set out in the FSMA. It will provide for the sharing of risk information between FIs for AML/CFT purposes as set out above, as well as safeguards on the use and confidentiality of information obtained from the

[17] The sharing of risk information on COSMIC by participant FIs and MAS' analysis of the information on COSMIC do not change the requirement for FIs to file an STR under section 39 of the CDSA.

platform ("platform information")[18]. The proposed legislative provisions for COSMIC are set out in Annex B.

Purpose and confidentiality of information-sharing

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.

4.3 In the initial phase, sharing information on COSMIC via Request, Provide and Alert will be non-mandatory. Thereafter, we expect that sharing of risk information via Provide and Alert to be made mandatory. It will also be mandatory for participant FIs to respond to Request messages after the initial phase. FIs that breach the requirements in relation to Request, Provide and Alert after the initial phase may be subject to penalties.[19] In addition, an 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.[20] Any individual that failed to secure the FI's compliance with these requirements may also be subject to penalties.[21]

4.4 MAS will also require FIs to guard against inappropriate sharing of platform information and put in place controls to prevent information security breaches. These requirements will be set out in subsidiary legislation and include requirements to have systems and processes in place to prevent unauthorised access to and use of platform

[18] Platform information includes risk information and information that are disseminated by MAS to FIs via COSMIC, including MAS' analysis of material networks that are escalated by the platform. Please also refer to paragraph 3.13 and paragraph 6.2 for more information on MAS' use and access to COSMIC, including analysing and following up on material networks that are escalated by the platform.

[19] FIs may be liable on conviction to a fine not exceeding $1 million and, in the case of a continuing offence, to a further fine of $100,000 for every day or part of a day during which the offence continues after conviction. The proposed penalties are aligned with current penalties under section 27B(2) of the MAS Act for breaches of requirements for prevention of ML and TF.

[20] FIs may be liable on conviction to a fine not exceeding $250,000. The proposed penalties are aligned with section 47(6) of the Banking Act for breaches of requirements relating to the privacy of customer information.

[21] Any individual charged with the duty of securing the FI's compliance, and was in the position to discharge that duty, may be liable on conviction – (a) if the individual committed the offence wilfully, to a fine not exceeding $125,000 or to imprisonment for a term not exceeding 3 years or to both; or (b) if the individual did not commit the offence wilfully, to a fine not exceeding $125,000.

information, and requirements to maintain records and audit trails of access to and provision of risk information[22]. Apart from the security features[23] built in COSMIC, FIs should also restrict staff access to COSMIC, and any platform information obtained from COSMIC, on a need-to-know basis. This would include only allowing designated staff to access COSMIC, and keeping a register of such staff, with timely and regular reviews of this list. For avoidance of doubt, COSMIC's information security requirements will apply from the initial phase. FIs that breach these requirements may be subject to penalties[24]. In addition, any person who knowingly or recklessly furnishes false and misleading information onto COSMIC may be subject to penalties.[25]

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.

Statutory protection against civil liabilities

4.5 MAS intends to confer statutory protection from civil liability to FIs which participate on COSMIC, in respect of their disclosure of information onto COSMIC, if the FI had exercised reasonable care and acted in good faith. This will serve to protect the participant FIs from undue legal challenges arising from their participation on COSMIC. It will provide participant FIs confidence that legitimate information sharing to highlight higher risk customers and their related activities will not expose them to civil suits, which

[22] These requirements would include maintenance of records and audit trails when customer risk information is provided to any other participant FI, or further disclosed to local or overseas affiliates, and other third parties (e.g. operational outsourced functions and Singapore court or police officers) (please refer to paragraphs 4.6 to 4.11)

[23] These 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.

[24] FIs may be liable on conviction to a fine not exceeding $1 million and, in the case of a continuing offence, to a further fine of $100,000 for every day or part of a day during which the offence continues after conviction. The proposed penalties are aligned with current penalties under section 27B(2) of the MAS Act for breaches of requirements for prevention of ML and TF.

[25] Such persons may liable on conviction – (a) in the case of an individual, to a fine not exceeding $125,000 or to imprisonment for a term not exceeding 3 years or to both; and (b) in any other case, to a fine not exceeding $1 million and, in the case of a continuing offence, to a further fine of $100,000 for every day or part of a day which the offence continues after conviction. The proposed penalties are aligned with current penalties under section 27B(2) of the MAS Act for breaches of requirements for prevention of ML and TF.

may be brought about by the very actors that COSMIC seeks to guard against. Such statutory protection is in line with those given to persons filing STRs under the CDSA, which, similar to information sharing on COSMIC, requires disclosure of information where specified threshold conditions are met.[26]

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

Sharing of platform information with local and overseas affiliates of FIs, and third parties

4.6 FIs and their officers will not be permitted to disclose platform information to any other person, except in scenarios as expressly provided for under the FSMA as elaborated in the paragraphs below, in line with the principle that information shared should be strictly relevant, proportionate and necessary for the purposes of assessing ML/TF/PF risk[27]. FIs and their officers that fail to comply with this requirement may be subject to penalties.[28]

4.7 FIs will be permitted to disclose platform information for specific legal purposes and to facilitate investigations or prosecutions of offences. This includes disclosure of platform information for compliance with Court orders[29] or requests from police or public officers, and for the making of a complaint or report relating to an alleged offence[30]. FIs

[26] See section 39 of the CDSA at footnote 3 above.

[27] Please refer to section X11 and the X11 Schedule of Annex B for further details.

[28] Any person who contravenes these requirements (i.e. section X11 of Annex B) may be guilty of an offence and be liable on conviction – (a) in the case of an individual, to a fine not exceeding $125,000 or to imprisonment for a term not exceeding 3 years or to both; or (b) in any other case, to a fine not exceeding $250,0000. The proposed penalties are aligned with section 47(6) of the Banking Act for breaches of requirements relating to the privacy of customer information.

[29] This would include disclosures for compliance with an order of the Supreme Court or a Judge sitting in the Supreme Court pursuant to powers conferred under Part IV of the Evidence Act (Cap. 97).

[30] The disclosure should only be made for compliance with an order or request made under the specified written law as defined under the X11 Schedule of Annex B, or for the making of a complaint or report under the specified written law as defined under the X11 Schedule of Annex B. For reference, "specified written law" means the Companies Act (Cap. 50), the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A), the Criminal Procedure Code (Cap. 68), the Goods and Services Tax Act (Cap. 117A), the Hostage-Taking Act 2010, the Income Tax Act (Cap. 134), the Internal Security Act (Cap. 143), the Insolvency, Restructuring and Dissolution Act 2018, the Kidnapping Act (Cap. 151), the

will also be permitted to disclose platform information for compliance with the provisions of the FSMA. This is similar to the approach taken under section 47 and the Third Schedule of the Banking Act (Cap. 19), which expressly sets out certain scenarios where disclosure of customer information is not prohibited. FIs may wish to refer to section X11 and X11 Schedule of Annex B for details on the purposes for which the disclosure of platform information is not prohibited and the persons to whom platform information may be disclosed.

4.8 FIs may also need to disclose platform information for specific operational purposes, including for group-wide ML/TF/PF risk management (as elaborated in paragraph 4.9 and 4.10), and to facilitate the performance of ML/TF/PF risk management duties (e.g. for the carrying out of AML/CFT controls and processes including customer due diligence, transaction monitoring and AML data analytics, as well as audits on the FI's AML/CFT controls) and outsourcing of ML/TF/PF risk management operational functions. FIs will be required to comply with additional safeguards when making further disclosures of platform information for such purposes, as elaborated in the paragraphs below and in Table A.

4.9 Currently, an FI in Singapore may disclose customer information for risk management purposes within the financial group, including with overseas branches or subsidiaries. This strengthens group-wide ML/TF/PF risk mitigation and prevents bad actors from moving between FIs within the same group, and is aligned with international standards set by the Financial Action Task Force.

4.10 In line with this principle, FIs will also be permitted to disclose the platform information they receive from COSMIC to both their local and overseas affiliates only for group-wide ML/TF/PF risk management purposes, on a need-to-know basis and provided that the additional conditions in Table A are met. The additional conditions are necessary because COSMIC will provide a participant FI with access to information provided by other participant FIs on their customers that had exhibited red flags or high risk behaviours. MAS recognises that the sharing of information obtained from COSMIC within the financial group, including with entities outside Singapore, may increase the risk of leakage or unauthorised disclosures, and also expose the FIs that shared the information to

Moneylenders Act 2008 (Act 31 of 2008), the Prevention of Corruption Act (Cap. 241) and the Terrorism (Suppression of Financing) Act (Cap. 325).

unintended legal risks. Requiring adequate safeguards to mitigate these risks would not detract from the benefits of group-wide sharing.

4.11 Similarly, to mitigate the risks of leakage and unauthorised disclosures, and unintended legal risks to FIs that had shared the information, FIs will be required to comply with additional safeguards, as provided in Table A, when making disclosures of platform information to persons for the performance of ML/TF/PF risk management duties and outsourcing of ML/TF/PF risk management operational functions. FIs should note that platform information should not be <u>further</u> disclosed to any other persons and for any other purposes other than those as set out in paragraphs 4.8 to 4.11 (please refer to the X11 Schedule of Annex B for further details).

Table A: Disclosure of platform information

Purpose for which platform information may be disclosed	Persons to whom platform information may be disclosed	Conditions
For performance of ML/TF/PF risk management duties as an officer or professional adviser of the participant FI	i. Any officer of the participant FI; ii. Any officer designated in writing by the head office or parent company of the participant FI; or iii. Any auditor appointed or engaged by the participant FI or its head office/parent company	No disclosure shall be made by a participant FI to any persons referred to in the second column, who is outside Singapore, or is not part of the FI's financial group, unless the participant FI has anonymised the identities of the participant FI(s) and/or MAS that had provided the platform information or are otherwise named in the platform information. In addition, disclosure must not be made to any auditor referred to in (iii), other than an auditor appointed or engaged by the participant FI, unless the auditor has given to the participant FI a written undertaking that he will not disclose any platform information obtained by him in the

		course of the performance of the audit to any person except the head office or parent company of the participant FI.
For performance of ML/TF/PF risk management	Designated officers of entities within the participant FI's financial group, including local and overseas affiliates[31]	No disclosure shall be made by a participant FI to any person referred to in the second column who is outside of Singapore, unless i. the participant FI has filed an STR on the customer to which the disclosure relates; and ii. the participant FI has anonymised the identities of the participant FI(s) and/or MAS that had provided the information, or are otherwise named in the information.
For performance of ML/TF/PF risk management operational functions, where such operational functions have been out-sourced	Any person which is engaged by the participant FI to perform the out-sourced functions	If any such out-sourced function is to be performed outside Singapore, or by any person who is not part of the participant FI's financial group, the disclosure shall be subject to such

[31] 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.

		conditions (relating to information security safeguards for outsourcing arrangements that participant FIs must put in place) as may be specified in a notice or direction issued by the MAS.

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.

Specific information-sharing parameters and obligations

4.12 MAS will set out in subsidiary legislation the detailed parameters for COSMIC and safeguards that participant FIs will be required to put in place. These include requiring FIs to:

(a) ensure that information disclosed on the platform is accurate and complete. FIs will also be required to promptly notify MAS and other relevant participant FIs of any error in the information provided, and to rectify such error as soon as possible;

(b) ensure that any disclosure made in accordance to the information sharing modes of Request, Provide and Alert is done in a timely manner, and within the prescribed time periods; and

(c) establish and implement systems and processes to safeguard the information disclosed and received as mentioned in paragraph 4.4.

FIs may be subject to penalties if they fail to comply with the requirements set out in subsidiary legislation[32]. MAS will issue a public consultation on the proposed subsidiary legislation at a later stage.

5 Phased Implementation of COSMIC

5.1 MAS will take a phased approach in rolling out the COSMIC platform. As outlined in paragraph 2.5, during COSMIC's initial implementation phase, risk information sharing will be permitted for the six banks which have been actively involved in its development. During this phase, information sharing via Request, Provide and Alert will be expected, but non-mandatory, whilst banks adjust to the new information-sharing paradigm. The legal safeguards and requirements on the confidentiality, use and disclosure of information (both domestically and overseas) will apply from this initial phase, as will the proposed statutory protection against civil liability.

5.2 Strengthening collaboration amongst a group of banks may raise the risk of illicit actors shifting their activities to FIs that do not participate on COSMIC. To address this risk, MAS will strengthen our surveillance to uncover such "risk migration" scenarios, and 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. MAS and CAD will continue collaborating with FIs on priority ML/TF investigations through the AML/CFT Industry Partnership ("ACIP"), and involve non-COSMIC FIs in such investigations where warranted.

5.3 Following this initial phase, MAS intends to make the risk information sharing requirements mandatory[33]. MAS will also consider when to expand the scope of participant FIs and the key risks to be targeted by COSMIC.

[32] FIs may be liable on conviction to a fine not exceeding $1 million and, in the case of a continuing offence, to a further fine of $100,000 for every day or part of a day during which the offence continues after conviction. The proposed penalties are aligned with current penalties under section 27B(2) of the MAS Act for breaches of requirements for prevention of ML and TF.

[33] After the initial phase, the requirements for (i) a receiving FI to respond to a Request message, (ii) a participant FI to send a Provide message, and (iii) a participant FI to place an Alert on a customer, will be made mandatory.

6 Access and Use of COSMIC Information by MAS and the Suspicious Transaction Reporting Office in CAD

6.1 Within the government, only authorised officers from MAS and the Suspicious Transaction Reporting Office ("STRO") in CAD will be able to directly access and use information from COSMIC.

6.2 As the owner of the COSMIC platform and AML/CFT supervisor, MAS requires access to information on COSMIC to monitor if FIs are using it appropriately, and to identify where adjustments are needed to improve effectiveness (e.g. calibration of red flags). MAS will also include information from COSMIC, including material networks of suspicious actors escalated by the platform, in its risk surveillance to target higher risk activities in the financial system for supervisory intervention.[34]

6.3 STRO is Singapore's financial intelligence unit. STRO receives STRs and other financial information, such as cash movement reports and cash transaction reports, and analyse them to detect ML, TF and other serious crimes. Where possible offences are detected, STRO disseminates the financial intelligence to relevant enforcement and regulatory authorities. Authorised STRO officers in CAD will be able to use other information sources, including COSMIC information, to augment their analysis.

7 Conducting Reviews of Customer Relationships

7.1 COSMIC provides FIs with additional information from other FIs on individuals and companies that are engaging in high risk behaviours or highly unusual activities. As with other instances where an FI obtains risk-relevant information on its customer, MAS expects an FI to perform an AML/CFT assessment of customers that are flagged through COSMIC.

7.2 In conducting these assessments, an FI should not rely solely on the information received from COSMIC or the fact that a customer's name was found in COSMIC's watchlist, in connection with a potentially suspicious activity. Instead, in its risk assessment, the FI should use information from COSMIC in combination with other sources of information, such as its own checks with the customer, reviewing the customer's transactions, public information sources or intelligence from authorities. It

[34] MAS may share information in its possession with a domestic or foreign AML/CFT authority, as provided in Sections 154 and 155 of the MAS Act and subject to the conditions therein.

should also consider the extent of the customer's involvement in such activity. In deciding whether to exit the customer relationship, the FI should give the customer adequate opportunity to explain the observed activity.

7.3 In practice, the last discipline would already be relevant and applicable to all customer exits for financial crime reasons, and not just those triggered by sharing from COSMIC. Therefore, MAS intends to amend the AML/CFT Notices to require that, prior to exiting a customer relationship, an FI must provide the customer an adequate opportunity to address its concerns. The FI must also document its assessment and the results of these checks with the customer. MAS intends for these requirements to apply to all FIs, not just those with access to COSMIC. The adjustments seek to balance between financial crime disruption and preventing unintended "de-risking" of legitimate customers. MAS will consult on these Notice amendments prior to implementation.

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.

8 Design of the access to COSMIC system

8.1 Participant FIs will be able to access the COSMIC system through both a web-based user interface and automated information exchange channels. This achieves the twin objectives of providing a human-centric interface to support collaboration between FI users, while allowing FIs to seamlessly integrate COSMIC data with their internal IT systems and data analytics programmes for higher productivity.

Web-based User Interface

8.2 The web-based user interface will allow participating FIs to connect to COSMIC with minimal initial infrastructure outlay, which could facilitate the onboarding of additional FIs in subsequent phases where these FIs have yet to adopt automated data exchange channels. FIs will be able to exchange risk information through online forms and file uploads/downloads, as well as access in-built functionalities such as workflows and case management to collaborate with other FIs.

Automated information exchange channels

8.3 These channels will facilitate the seamless exchange of information between COSMIC system and participant FIs, although they may entail some changes to FIs' existing

IT infrastructure, systems and operational processes. The automated information exchange can be achieved through various technological means, such as application programme interfaces ("APIs") or secured file transfer protocols ("SFTPs").

8.4 For both approaches, MAS will identify and implement the appropriate technologies to enable the exchange of information in a secure, reliable and efficient way. Amongst other considerations, MAS will take into account the cybersecurity controls, the expected frequency, volume and size of the information flowing from the COSMIC platform, as well as the technological infrastructure of the participating FIs.

Annex A

LIST OF QUESTIONS

Monetary Authority of Singapore