Financial Institutions | White Collar Crime

MAS Consults on Features & Legislative Framework of Digital Platform for FIs to Share Information for AML/CFT Purposes

Executive Summary

The Monetary Authority of Singapore ("**MAS**") is seeking feedback on its proposal to deploy a secured digital platform, to be named COSMIC (Collaborative Sharing of ML/TF Information & Cases), that will allow financial institutions ("**FIs**") to share information to help them detect and disrupt illicit transactions in a timelier manner. Such information relates to the particulars of a customer (including the beneficial owners and authorised signatories of the customer) and transactions, money laundering ("**ML**"), terrorism financing ("**TF**") and proliferation financing ("**PF**") risk observations or analysis relating to the customer, or the high-risk behaviour exhibited ("**risk information**").

These proposals are set out in MAS' "Consultation Paper on FI-FI Information Sharing Platform for AML/CFT" that was published on 1 October 2021. The consultation ends on **1 November 2021**, with MAS intending to launch COSMIC in the first half of 2023.

This Update outlines salient features of COSMIC and the proposed legislative framework.

Background Information

Under the Singapore anti-money laundering ("**AML**") and countering the financing of terrorism ("**CFT**") regime, FIs are required to, among other things, file a suspicious transaction report ("**STR**") if they have reasonable grounds to suspect that a customer is involved in ML/TF/PF activities. However, FIs are not permitted to warn each other about potentially suspicious activity involving their customers, creating an information gap that is exploited by financial criminals. This creates an information gap to make illicit transactions through a web of entities with accounts in different FIs.

As such, MAS is proposing to develop and operate COSMIC to plug this information gap, allowing FIs to query and alert each other on potential illicit behaviours in a timely fashion. It is intended that sharing will be permitted only:

- to address potential ML, TF or PF concerns in key risk areas;
- 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;
- in the data format specified by MAS, such that only relevant risk information is shared, and in a proportionate manner; and

- via COSMIC.

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

Phased development and deployment

To ensure operational stability and efficiency, COSMIC will be developed and deployed in phases as follows.

Initial Phase	• Focus on sharing of risk information in three key risk areas of (1) misuse of legal persons; (2) trade-based ML; and (3) PF. • Information-sharing on COSMIC will be voluntary. • Will be made available to six participant banks, namely, DBS, OCBC, UOB, Standard Chartered Bank, Citibank and HSBC. • Expected to last for about two years.
Subsequent Phase	• Increase key risk areas for sharing of risk information. • To be participated in by wider segment of financial sector. • Certain aspects of information-sharing will be made mandatory, namely, abiding by the requirements with regard to sending a "Provide" message and placing an "Alert" on a customer (see below for more information).

Key Features of COSMIC

Nature of information to be shared

The sharing of risk information among FIs on COSMIC is intended to detect key ML/TF/PF risks which have been identified as priority targets for mitigation in line with Singapore's national strategy to combat serious financial crime.

Before an FI is required to or may share risk information on a customer on COSMIC, a customer must first exhibit multiple high-risk behaviours or indicators that suggest serious financial crime ("**red flags**"). FIs will be required to obtain an explanation from the customer as part of its risk assessment of potential financial crime concerns. This is to address the fact that there may be legitimate explanations for such red flags.

The thresholds and red flags are based on typologies of past domestic and global cases in the key risk areas of ML/TF/ PF. MAS intends to issue the red flags and threshold criteria to participant FIs privately. FIs and their officers will be required by law to keep the red flags and threshold criteria confidential so that they are not disclosed to bad actors. The indicators that suggest serious financial crime that

underpin the red flags and threshold criteria will be adjusted over time to reflect any change in criminals' methods or mode of criminality.

Modes of information-sharing

Depending on the level of ML/TF/ PF risks exhibited by a customer, an FI will be able to share risk information with another FI through COSMIC in three ways set out below, depending on whether the customer's behaviour crosses relevant thresholds.

Request	Provide	Alert
Customer's activities exhibited red flag behaviour, raising suspicion of involvement in illicit activity	**Customer's unusual activities indicated greater risk of involvement in illicit activity**	**Customer's activities exhibited higher threshold of red flags, FI has filed STR and terminated relationship**
• FI sends a **Request** message to other FIs for risk information on the customer which is linked to the customer's activity to help it assess its suspicion. • Receiving FI should furnish the requested risk information within a reasonable timeframe, if it is satisfied that the information may assist in the assessment. • Receiving FI may use the risk information it received from the Request to perform an AML/CFT assessment of its own customer.	• FI sends a **Provide** message to other FIs. • Receiving FI must 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.	• FI places an **Alert** on this customer on the "watchlist"[1] on COSMIC. • Participant FIs should 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.
General Requirements: • FI should only initiate a **Request** or **Provide** message to share risk information with another FI, if the customer had transacted with customers of the latter FI and/or where its customer is also a customer of the latter FI. • FI should explain in its **Request**, **Provide** or **Alert** message the context of its concern, including red flags observed and relevant risk information on the customer.		

[1] FIs should not reject or exit a customer purely because the customer is placed on the COSMIC watchlist. The FI should allow the customer to explain the unusual behaviour and perform its own risk assessment based on the information obtained from the customer. Based on this assessment, the FI may decide to exit or retain/onboard the customer. The FI must properly document its assessment and decision.

Other Aspects of COSMIC

- **Access and use of COSMIC information by MAS and STRO in the Singapore Police Force's Commercial Affairs Department ("CAD").** 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.

- **Process for reviewing customer relationships prior to exit.** FIs are expected to perform an AML/CFT assessment of customers with reference to risk information obtained from COSMIC, in combination with other sources of information from its own dealings with the customer, public information or intelligence from authorities. Should an FI decide to terminate the customer relationship after the assessment, the FI should provide the customer an adequate opportunity to explain the activity or behaviour assessed to be suspicious. MAS is of the view that this requirement should apply to all customer exits for financial crime reasons, and not be limited to those triggered by information sharing on COSMIC. Therefore, MAS seeks feedback on introducing a requirement in the MAS AML/CFT Notices for all FIs to put in place a process for reviewing customer relationships prior to exit, which would include seeking an explanation from the customer on their suspicious activities. The FI must document its assessment and the results of these checks with the customer. It is proposed that the requirements would apply to all FIs, not just to those with access to COSMIC.

- **Design of participant FI access of COSMIC.** Participant FIs will be able to access the COSMIC system through both a web-based user interface and automated information exchange channels. For both approaches, MAS will identify and implement the appropriate technologies to enable the exchange of information in a secure, reliable, and efficient way. Considerations that MAS will take into account include the cybersecurity controls, the expected frequency, volume and size of the information flowing from COSMIC, and the technological infrastructure of the participating FIs.

Key Aspects of Proposed Legislative Framework

The proposed regulatory framework will be set out in the Financial Services and Markets Bill, which is targeted to be introduced in Parliament later this year. Under the proposed framework governing information sharing on COSMIC, information sharing by FIs is permitted only for AML/CFT purposes. All COSMIC participants are required to implement robust measures to safeguard against unauthorised use and disclosure of COSMIC information. MAS will supervise FIs for compliance with these requirements and will take action against errant FIs. We highlight below three key aspects of the proposed framework, namely:

- Safeguarding confidentiality of information sharing;
- Statutory protection against civil liabilities; and

- Sharing of information on COSMIC with local and overseas affiliates of FIs, and third parties.

Safeguarding confidentiality of information sharing

FIs will be required to safeguard against inappropriate sharing of COSMIC information and prevent information security breaches. These requirements will be set out in subsidiary legislation that MAS will be consulting on at a later stage. Among other things, FI will be required to:

- Establish systems and processes to prevent unauthorised access to and use of risk information on COSMIC;
- Maintain records and audit trails of access to and provision of risk information;
- Restrict staff access to COSMIC, and any risk information obtained from COSMIC, on a need-to-know basis.

These information security requirements will apply to FIs participating in the initial phase. Penalties will apply to FIs that breach these requirements or any person who knowingly or recklessly submits false and misleading information to COSMIC.

Statutory protection against civil liabilities

An FI that had exercised reasonable care and acted in good faith will be conferred statutory protection from civil liability in respect of the information disclosed on COSMIC. This statutory protection aims to protect participant FIs who engage in legitimate information sharing from undue legal challenges by the very actors that COSMIC seeks to guard against.

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

Just like the approach taken for the banking secrecy rules, FIs and their officers will not be permitted to disclose risk information on COSMIC to any other person, except in scenarios that are expressly provided in the legislation. The overarching principle is that information shared should be strictly relevant, proportionate and necessary for the purposes of assessing ML/TF/PF risks. FIs and their officers that fail to comply with this requirement would be subject to penalties.

Details of the proposed scenarios and related conditions that have to be met before an FI may share COSMIC platform information are set out at Table A of the Consultation Paper. These proposed scenarios include, among other things, disclosure made:

- for specific legal purposes and to facilitate investigations or prosecutions of offences;
- for specific operational purposes, including for group-wide ML/TF/PF risk management, 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. Such disclosures may be made to the FI's local and overseas affiliates on a need-to-know basis, provided that the additional conditions and safeguards are met. For example, a FI may only disclose the risk information on COSMIC to a designated officer of the FI's overseas affiliates if the FI has filed an STR on the customer to which the disclosure relates, and the FI has anonymised the identities of the participant FIs and/or MAS that had provided the information, or are otherwise named in the information.

Information on COSMIC should not be further disclosed to any other persons and for any other purposes other than those as set out in the proposed legislation.

Further Information

If you have any queries on the above development or would like to submit any feedback to the consultation paper, please feel free to contact our team members below who will be happy to assist.

Click on the following links for more information:

- MAS media release titled "MAS and Financial Industry to Use New Digital Platform to Fight Money Laundering" (1 October 2021)
- Consultation Paper on the FI-FI Information Sharing Platform for AML/CFT

Contacts

Financial Institutions

Regina Liew
Head, Financial Institutions Group

T +65 6232 0456

regina.liew@rajahtann.com

Larry Lim
Deputy Head, Financial Institutions Group

T +65 6232 0482

larry.lim@rajahtann.com

Benjamin Liew
Partner, Financial Institutions Group

T +65 6232 0686

benjamin.liew@rajahtann.com

White Collar Crime

Hamidul Haq
Partner, White Collar Crime

T +65 6232 0398

hamidul.haq@rajahtann.com

Thong Chee Kun
Partner, White Collar Crime

T +65 6232 0156

chee.kun.thong@rajahtann.com

Yusfiyanto Yatiman
Partner, White Collar Crime

T +65 6232 0787

yusfiyanto.yatiman@rajahtann.com

Josephine Chee
Partner, White Collar Crime

T +65 6232 0591

josephine.chee@rajahtann.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com

Our Regional Contacts

RAJAH & TANN | *Singapore*
Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*
R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*
Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*
Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL
GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Our Regional Presence

Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.