Financial Institutions Group | Technology, Media & Telecommunications

Singapore Parliament Passes Bill to Regulate Certain Digital Token Service Providers, Harmonise and Enhance MAS Regulatory Power over FIs

Introduction

The Financial Services and Markets Bill ("**FSM Bill**"), which seeks to implement a financial sector-wide regulatory approach for financial services and markets, was passed in Parliament on 5 April 2022. The FSM Bill will consolidate the provisions and powers that relate to the Monetary Authority of Singapore's ("**MAS**") regulatory oversight of different financial institution classes in a single Act. The FSM Bill has yet to come into operation.

The FSM Bill contains provisions on the following key areas:

(a) Regulation of certain digital token ("**DT**") service providers created in Singapore for anti-money laundering and countering of financing of terrorism ("**AML/CFT**") purposes;
(b) Harmonised power to impose technology risk management ("**TRM**") requirements on financial institutions ("**FIs**") and increased maximum penalty for breaches of TRM requirements;
(c) Harmonised and expanded power to issue prohibition orders ("**POs**"); and
(d) Statutory protection from liability for mediators, adjudicators and employees of an operator of an approved dispute resolution scheme.

By way of background, the FSM Bill was tabled for first reading in Parliament on 14 February 2022, please click here for Rajah & Tann's Client Update on the FSM Bill when it was first introduced. The FSM Bill incorporates feedback received by MAS pursuant to its earlier "Consultation Paper on the New Omnibus Act for the Financial Sector" ("**Consultation Paper**") on the draft version of the Bill.

This Update provides an overview of these key areas to be regulated under the FSM Bill.

Regulating Certain DT Service Providers Created in Singapore for AML/CFT Purposes

MAS aims to align the AML/CFT regulation and supervision of virtual asset service providers ("**VASPs**") with the enhanced standards issued by the Financial Action Task Force (FATF) for VASPs ("**Standards**") that was revised in 2019. The Standards specify, among other things, that the

jurisdiction where a VASP is created must regulate and supervise it. In addition, other jurisdictions where the VASP has operations or customers in, may also choose to regulate that VASP. This ensures that every VASP will be regulated by at least one jurisdiction, regardless of where it conducts its businesses or where its customers are located.

Regulating VASPs created in Singapore but carries out VA activities outside Singapore

Current legislation in Singapore regulates an entity that carries on a business of conducting certain virtual asset ("**VA**") activities in Singapore, regardless of whether the entity is created in Singapore. The FSM Bill will extend the regulatory framework to a person in Singapore who carries on a business of providing VA activities outside of Singapore.

Subject to certain exclusions, a corporation (including a limited liability partnership) that is incorporated or formed in Singapore which carries on a business of providing DT services outside Singapore will be licensed as a DT service provider under the FSM Bill. The licensing regime will extend to an individual or a partnership, who from a place of business in Singapore, carries on a business of providing DT service outside Singapore (including a situation where the overseas DT service is provided by someone other than the individual or partnership in Singapore).

Some examples of persons who will not be regulated under the FSM Bill include:

- an entity that is already licensed, or exempted from licensing, under the relevant provisions in the Securities and Futures Act 2001 ("**SFA**"), Financial Services Act 2001 ("**FAA**") and Payment Services Act 2019 ("**PS Act**") for providing DT services outside Singapore;

- a technical service provider which provides any service that supports the provision of any DT service and does not enter into possession of any money or DT under that DT service, such as:

  - the service of processing and storing data,
  - any information technology ("**IT**") security, trust or privacy protection service;
  - any data and entity authentication service;
  - any IT service;
  - the service of providing a communication network; and
  - the service of providing and maintaining any terminal or device used for any DT service.

  For example, those who solely engage in the activity of blockchain mining or perform the function of validator nodes will not fall within the purview of the FSM Bill.

- a central bank or FI which provides any DT service in respect of any central bank DT; and

- any person who provides DT services in respect of any limited purpose digital payment token ("**DPT**") (e.g. digital points awarded to customers pursuant to a loyalty programme).

Definition of DT and scope of DT services

A DT is defined under the FSM Bill as:

- a DPT as defined in the PS Act; or
- a digital representation of a capital markets product as defined in the SFA which:
  - can be transferred, stored or traded electronically; and
  - satisfies such other characteristics as MAS may prescribe. This limb is to allow MAS to act in a timely manner to subject any new business model to the licensing and AML/CFT requirements under the FSM Bill pursuant to consultations with the industry.

Asset-backed DTs which fall within the definition of a DPT or digital representation of a capital markets product would be considered as DTs. This would capture certain asset-backed DTs structured as a security. Other types of tokens that represents a physical product will not be caught under the FSM Bill if it is neither a DPT nor a digital representation of a capital markets product.

For the purposes of the FSM Bill, the scope of DT services is aligned with the Standards and it includes:

- dealing in DTs;
- facilitating the exchange of DTs;
- inducing or attempting to induce any person to enter into or to offer to enter into any agreement for or with a view to buying or selling any DTs in exchange for any money or any other DTs;
- accepting DTs for the purposes of transmitting, or arranging for the transmission of, the DTs;
- safeguarding of a DT or DT instrument, where the service provider has "control" over the DT or the DT associated with the DT instrument. MAS explains that "control" over a DT or DT instrument includes having the ability to control the access to the DT or to execute transactions involving the DT. For example, a service provider will fall under the purview of the FSM Bill if it has control over the private cryptographic keys of a multi-signature wallet; and
- providing financial advice relating to the offer or sale of DTs which includes advising others by issuing or promulgating research analyses or research reports concerning any DTs, but not including professional legal or accounting-related advisory services.

The Consultation Paper (at page 12) sets out a brief explanation of each service, and the activities which each service is intended to capture.

Licensing and ongoing requirements for DT service provider

The FSM Bill sets out the licensing and ongoing requirements on DT service providers, to ensure that such entities have a meaningful presence in Singapore. This allows MAS to have adequate supervisory oversight over them, even though they provide DT services outside of Singapore. Among other things, an applicant for a DT service provider licence must appoint at least one executive director who is resident in Singapore, have a permanent place of business in Singapore and satisfy financial requirements as may be prescribed by MAS.

MAS expects a permanent place of business to have a dedicated, segregated space where records of transactions, customer risk assessments and documentation of mitigation measures are kept securely and readily accessible by MAS and other relevant Singapore authorities.

DT service providers will be expected to have adequate compliance arrangements commensurate with the scale, nature and complexity of their operations. The minimum compliance arrangements applicable to a DT service provider will model closely after those set out in the "Guidelines on Licensing for Payment Service Providers". MAS will be seeking public feedback on the measures it requires in respect of the compliance function in due course.

AML/CFT and technology risk management requirements applicable to DT service provider

Due to the anonymity and speed of transactions relating to DT services, MAS regards these transactions as carrying inherently higher money laundering and terrorism financing risks ("**ML/TF risks**"). Therefore, DT service providers are primarily regulated under the FSM Bill for ML/TF risks, in addition to technology and cyber risks.

A DT service provider will be expected to assess the risks of the jurisdictions which it has operations in and take a risk-based approach in applying the requirements, including performing enhanced customer due diligence measures in higher risk scenarios. MAS intends to apply AML/CFT requirements which are similar to those set out in the "MAS Notice PSN02 on Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Service Licence (Digital Payment Token Service)" to DT service providers.

Harmonised Power to Impose Requirements on Technology Risk Management

At present, MAS relies on powers in the respective Acts under which FIs are regulated to specify its requirements on TRM for regulated activities pursuant to the Notices on Technology Risk Management and Notices on Cyber Hygiene (collectively, "**Tech-Risk Notices**") issued by MAS in respect of the respective regulated activity.

Technology risks are increasing significantly with the prevalence of digital services and as such systems become more complex. This increasing complexity, coupled with the significant increase in the number of breach incidents and private and state-sponsored threat actors, requires that existing policies, processes and cybersecurity frameworks be enhanced accordingly to deal with these technology risks (including cybersecurity risks). To this end, the FSM Bill will provide for the following requirements.

- **TRM requirements:** The FSM Bill will empower MAS to make regulations or issue directions on TRM, including cybersecurity risks, and the safe and sound use of technology to deliver financial services and protect data (which may include both personal data as well as organisational/corporate data) that apply to any FI or class of FIs. This enables MAS to impose TRM requirements on any FI or any class of FIs in relation to any FI's system, even though the system does not support a regulated activity. This is because a system that does not support a regulated activity can pose contagion cyber risk to systems that do due to inter-linkages.

  To ensure compliance with the above, FIs should conduct comprehensive testing of new technologies to ensure that they are safe and reliable before adoption. FIs should also ensure that their technical design, architecture and procedures are safe and sound. In this regard, FIs should be aware that using a secure technology solution in an unsafe architecture, design or manner will vitiate the safe and sound use of technology.

  Further, FIs should be aware that training of staff in the safe and sound use of technology is also of paramount importance. Putting untrained/under-trained hands behind the steering wheel of technology is likely to result in the occurrence of breach or non-compliance with TRM requirements.

- **Maximum penalty for contravention raised to S$1 million:** To underscore the criticality of TRM requirements, the maximum penalty for breaches of any requirements relating to TRM and the safe and sound use of technology to deliver financial services and protect data will be raised to S$1 million. Further, a technology event which impacts an FI's customers or other industry participants could involve breaches of several TRM requirements, meaning that an FI could face a penalty much higher than S$1 million for a serious cyberattack or disruption to essential financial service (e.g., ATM network disruption, online trading disruption). In determining the enforcement

actions to be taken in the event of a breach, MAS will assess the extent to which the FIs had implemented the necessary controls to meet the requirements. This addresses a perennial question among FIs on the potential quantum of penalties for non-compliance with MAS TRM Notices, Cyber Hygiene Notices and applicable TRM Guidelines.

The existing Tech-Risk Notices will be re-issued under the FSM Bill.

Harmonised and Expanded Powers to Issue POs

POs are issued by MAS to prohibit a person from conducting certain activities or from holding key roles in FIs for a period of time in cases of serious misconduct. MAS' existing powers to issue POs are provided for in the SFA, the FAA and the Insurance Act 1966 ("**IA**"). Currently, MAS is not empowered to issue POs to persons regulated under other Acts administered by MAS and its existing powers do not comprehensively address risks as they only prohibit the subject from carrying out a limited scope of regulated activities. In order to address these gaps, the FSM Bill will, among other things, provide for the following requirements.

- **Widen MAS' power to issue POs against any person.** MAS explains that although the FSM Bill provides broadly that a PO may be issued against any person, it will generally be issued only if a person has a former, existing or prospective nexus to the financial industry, including service providers of FIs and their employees. MAS will issue guidelines to provide greater clarity on how the power will be used.

- **Rationalise the grounds for issuing POs.** The FSM Bill provides that MAS may make a PO against a person on the ground that he/she is not a fit and proper person in accordance with the MAS Guidelines on Fit and Proper Criteria to:

  - become a substantial shareholder of or act as a director, partner, manager of an FI, or take part in the management of an FI ("**Role**");
  - carry out any activity or business, or provide any service, which is regulated by an Act that is administered by MAS ("**Activity**"); and
  - perform the following key functions of an FI in relation to an Activity ("**Functions**"):
    (i) handling of funds and assets;
    (ii) risk-taking;
    (iii) risk management and control (including AML/CFT and audit functions);
    (iv) critical system administration;
    (v) any other function critical to the integrity or functioning of FIs, which MAS may prescribe for the purpose of protecting trust or deterring misconduct in the financial industry.

- **Widen the scope of prohibition under POs.** In addition to the current powers to prohibit unsuitable persons from taking up a specified positions (e.g. directorship, substantial shareholder, management) and conducting any Activities, MAS will be empowered to prohibit a person who is subject to a PO from undertaking the Functions as these functions are critical to the integrity and functioning of FIs and it is important that MAS is able to prohibit persons who are not fit and proper from performing these functions.

- **Effect of POs.** An FI must not employ or enter into any arrangement with a person against whom a PO is made ("**Prohibited Person**"), or use a Prohibited Person's service, for any Role, Activity or Function which the person is prohibited from undertaking. FIs are expected to check that the relevant employees of their service providers who undertake the Functions for or on behalf of FIs have not been issued with POs prohibiting them from doing so. The FSM Bill provides for a defence for an FI which is found to have indirectly engaged a Prohibited Person through an outsourcing arrangement if the FI can show that it took all reasonable steps to ensure compliance with the requirement, and after doing so, believed on reasonable grounds that it would not be indirectly engaging a Prohibited Person. Such reasonable steps include performing due diligence checks on the relevant employees of the service provider by, among other things, checking the Enforcement Actions page on the MAS website, or relying on the service provider or a third party to conduct due diligence checks on the employees of the service provider and accordingly, confirm to the FIs that the employees have not been issued with a PO.

Statutory Protection from Liability for Mediators, Adjudicators and Employees of Operator of Approved Dispute Resolution Scheme

FIs prescribed under the Monetary Authority of Singapore (Dispute Resolution Schemes) Regulations 2007 are required to subscribe as members of an approved dispute resolution scheme. The Financial Industry Disputes Resolution Centre Ltd operates the only approved dispute resolution scheme.

The FSM Bill will provide an approved dispute resolution operator's mediators, adjudicators and employees with statutory protection from liability in the performance of their duties. This will enhance the confidence and autonomy of these persons in carrying out their duties. Specifically, a mediator, adjudicator or employee of an operator of an approved dispute resolution scheme will be exempted from liability for an act or omission done with reasonable care and in good faith.

Financial Institutions Group | Technology, Media & Telecommunications

Further Information

Please click here for the full text of the FSM Bill (made available on the Parliament website (www.parliament.gov.sg), here for the Explanatory Brief for the FSM Bill (made available on the MAS website (www.mas.gov.sg)) and here for the Second Reading Speech by Mr Alvin Tan, Minister of State, Ministry of Culture, Community and Youth & Ministry of Trade and Industry, and Board Member of MAS, on behalf of Mr Tharman Shanmugaratnam, Senior Minister and Minister-in-charge of MAS (made available on the MAS website (www.mas.gov.sg)).

If you have any queries on the above development, please feel free to contact our team members below who will be happy to assist.

Contacts

Financial Institutions Group

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

Financial Institutions Group | Technology, Media & Telecommunications

Technology, Media & Telecommunications

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0751

rajesh@rajahtann.com

Steve Tan
Deputy Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0786

steve.tan@rajahtann.com

Benjamin Cheong
Deputy Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0738

benjamin.cheong@rajahtann.com

Lionel Tan
Partner, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0752

lionel.tan@rajahtann.com

Tanya Tang
Partner (Chief Economic and Policy Advisor), Competition & Antitrust and Trade; Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0298

tanya.tang@rajahtann.com

Financial Institutions Group | Technology, Media & Telecommunications

Rajah & Tann Cybersecurity

Wong Onn Chee
Chief Executive Officer, Rajah & Tann Cybersecurity

T +65 6932 2606

onnchee@rtcybersec.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

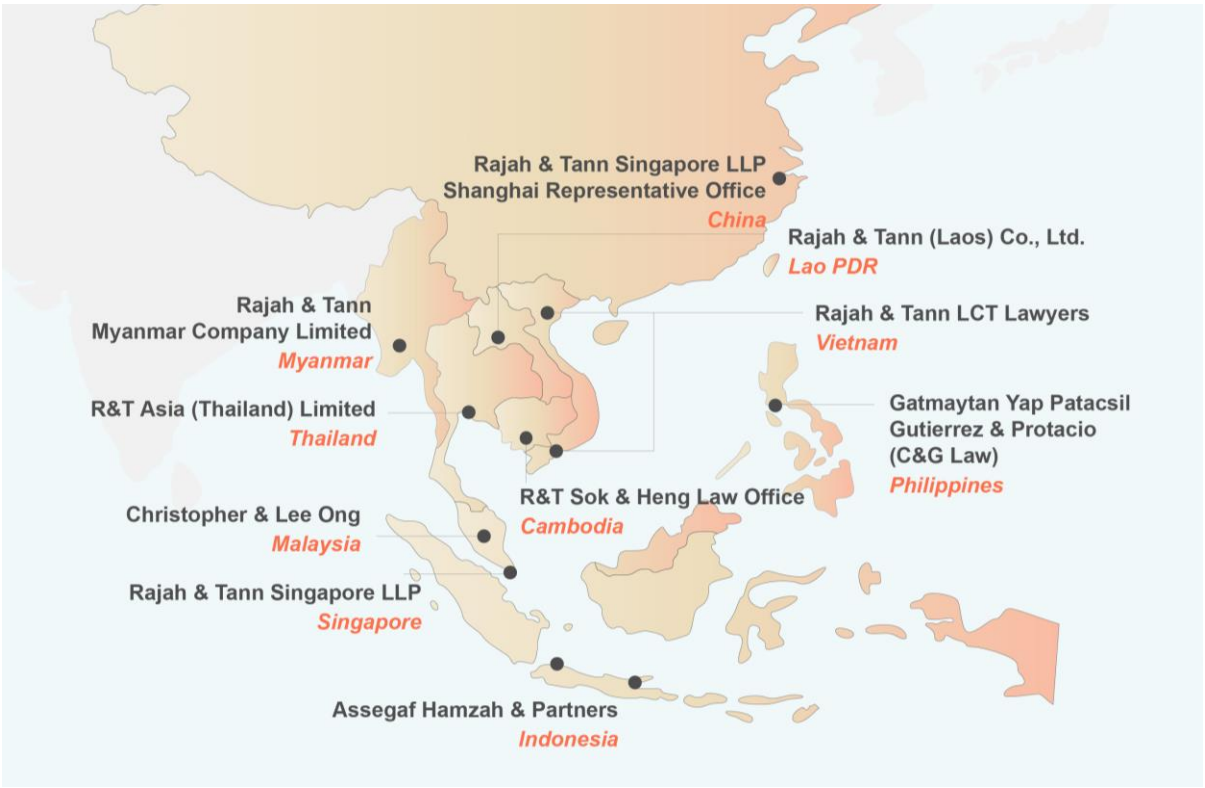
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

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.