Technology, Media & Telecommunications | White Collar Crime

Implementation of the Online Criminal Harms Act

Codes of Practice for Designated Online Services Come into Force

Introduction

The Online Criminal Harms Act ("**OCHA**") was enacted to enable the authorities to deal more effectively with online criminal activities. While most of the provisions came into operation on 1 February 2024, the remaining provisions have now come into operation on 24 June 2024. These provisions relate to Codes of Practice ("**COP**") and implementation directives for online services to counter scams and malicious cyber activities.

Pursuant to these provisions coming into operation, two COPs have been issued by the Singapore Police Force ("**SPF**"), which have taken effect from 26 June 2024. The Ministry of Home Affairs ("**MHA**") has further issued the list of designated online services that will be subject to these COPs, as well as the timeline for implementation.

- **Online Communication Code** – This is applicable to designated online communication services, which must implement appropriate systems, processes or measures to achieve the prescribed objectives.
- **E-Commerce Code** – This is applicable to designated e-commerce services. It contains the same requirements as the Online Communication Code, with additional requirements on verification of users and provision of payment protection mechanisms.

In this Update, we highlight the key provisions of the OCHA that have now come into operation, as well as provide a summary of the principles and timelines under the COPs.

Overview of OCHA

The OCHA is aimed at online content or activity which is criminal in nature, or which is used to facilitate or abet crimes. It was passed in Parliament on 5 July 2023. For more information on the OCHA, please see our earlier Legal Update on the OCHA being passed in Parliament, available here.

The provisions which came into force on 1 February 2024 relate to the following measures:

- Directions to online services to restrict the exposure of Singapore users to criminal activities on their platforms;
- Orders to limit further exposure to the criminal activities being conducted on the platforms of non-compliant online services; and
- Powers to require information to administer the Act and facilitate investigations and criminal proceedings.

The provisions which have now come into force on 24 June 2024 relate to the following measures:

- The power to issue COPs regulating designated online services;
- Rectification Notices for non-compliant service providers; and
- Implementation Directives over designated online services.

Codes of Practice

One of the key measures that has now come into operation is that the Competent Authority, sited within SPF, can issue COPs to require providers of designated online services to put in place appropriate systems, processes or measures to disrupt scams and malicious cyber activities affecting people in Singapore.

Pursuant to this, SPF has issued the following COPs: (i) the Online Communication Code; and (ii) the E-Commerce Code.

Online Communication Code

The Online Communication Code applies to the following designated online communication services, which present the highest risk of scams to Singapore users:

- Facebook;
- WhatsApp;
- Instagram;
- Telegram; and
- WeChat.

The key requirements under the Online Communication Code are summarised in the table below. Providers of the designated online services Code will be required to implement the appropriate systems, processes or measures by 31 December 2024.

Technology, Media & Telecommunications | White Collar Crime

Aim	Requirements
Quick disruption of malicious accounts and activities	• Proactively detect, and promptly take all necessary actions against, suspected scams and/or malicious cyber activities ("**scams**") • Provide an easily accessible reporting mechanism for users and take appropriate actions promptly • Implement a fast-track channel to facilitate the receipt of reports on scams from relevant law enforcement agencies • Inform relevant law enforcement agencies expeditiously of any detected trends or modalities of scams • Retain all available data of accounts detected as being used for scams for a minimum of 90 days • Maintain and preserve any such records requested by law enforcement agencies for criminal investigations • Facilitate requests for information and data from law enforcement agencies
Deployment of safeguards to prevent propagation of malicious activities	• Ensure reasonable verification measures are put in place to prevent the creation and usage of accounts for scams • Conduct additional verification procedures on an account when there is detection of suspicious conduct or activity • Require holders of accounts to have strong login verification features • Provide holders of accounts with the option to designate their accounts as 'verified', that comes with stronger verification measures
Accountability	Submit to the Competent Authority an annual report on the implementation of measures and efforts to counter and prevent scams. The report shall include: • Measures implemented to detect, prevent and respond to scams • New challenges in countering and preventing scams • Measures being explored or developed to improve existing systems and techniques against scams • Suitable metrics and information on the effectiveness of the implemented measures

Technology, Media & Telecommunications | White Collar Crime

E-Commerce Code

The E-Commerce Code applies to the following designated e-commerce services, which present the highest risk of scams to Singapore users:

- Carousell;
- Facebook Marketplace;
- Facebook Advertisements; and
- Facebook Pages.

The key requirements under the E-Commerce Code and the respective implementation timelines are summarised in the table below.

Requirement	Implementation Timeline
Comply with the same requirements as those under the Online Communication Code, as summarised above	Compliance required by 31 December 2024
Subject users who advertise or post about the sales of goods and/or services, or those who intend to do so, to verification against Government-issued records	MHA will prioritise the implementation of the user verification requirement as follows: • For a start, the designated online services will be allowed to apply this requirement only to users who they identify to be risky. • Should the e-commerce scam situation fail to improve, MHA will then require the services to expand the coverage of the verification requirement. The assessment periods are as follows: • Carousell – 1 July 2024 to 31 December 2024 • Facebook Marketplace – 1 June 2024 to 30 November 2024 • Facebook Advertisements – 1 July 2024 to 31 December 2024 • Facebook Pages – Verification requirement waived for now to allow prioritisation of Facebook Marketplace and Advertisements

Requirement	Implementation Timeline
Provide, as an option for users, payment protection mechanisms that require delivery of goods or services to be verified, before payment is released to the sellers	MHA will assess the need for this requirement based on the effectiveness of the user verification measures. MHA will waive this requirement for now and reassess this in 2025.

Other Measures

Another key measure that has now come into operation is that of Rectification Notices. If the Competent Authority assesses that a provider of a designated online service has not complied with the applicable COP, it may issue a Rectification Notice requiring the provider to correct the non-compliance by a specified time. Failure to comply with the Rectification Notice would be a criminal offence.

The Competent Authority may also issue Implementation Directives to the provider of any designated online service to implement a specific system, process or measure to address the risk of scams or malicious cyber activities.

Concluding Words

The OCHA sets out a proactive framework to combat online criminal activities. In particular, the issuance of the Online Communication Code and the E-Commerce Code pursuant to the OCHA marks a significant step in engaging online service providers and setting out their responsibilities in this regard.

Online service providers should take note of the requirements set out in the COPs and assess their existing policies and procedures to determine the measures that need to be taken and the policies that need to be implemented to ensure that they are in compliance with the COPs.

The full COPs are available here. The full media release from MHA is available here.

For further queries, please feel free to contact our team below.

Technology, Media & Telecommunications | White Collar Crime

Contacts

Technology, Media & Telecommunications

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications

T +65 6232 0751

rajesh@rajahtann.com

Steve Tan
Deputy Head, Technology, Media & Telecommunications

T +65 6232 0786

steve.tan@rajahtann.com

Benjamin Cheong
Deputy Head, Technology, Media & Telecommunications

T +65 6232 0738

benjamin.cheong@rajahtann.com

Click **here** for our Partners in our Technology, Media and Telecommunications Practice.

White Collar Crime

Thong Chee Kun
Partner, White Collar Crime

T +65 6232 0156

chee.kun.thong@rajahtann.com

Click **here** for our Partners in our White Collar Crime Practice.

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

Our Regional Contacts

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

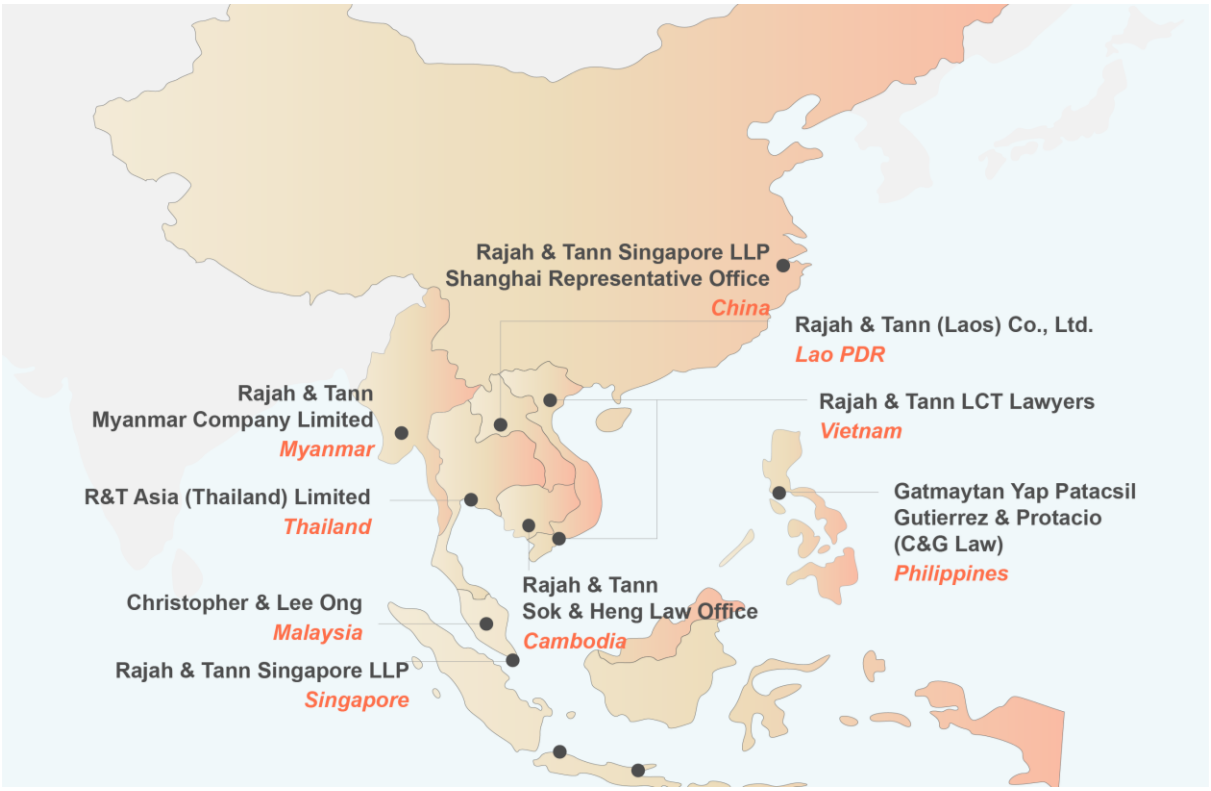
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

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.