31 May 2023

New Online Criminal Harms Bill to Fight Online Crime

Online criminal activities, including malicious cybercrimes and scams perpetrated through online platforms, have been steadily rising over the years. To tackle this growing problem, the Online Criminal Harms Bill was introduced in the Singapore Parliament on 8 May 2023. The objective of the Bill is to empower the authorities to take swift and pro-active action to disrupt the spread and impact of online criminal activities on the Singapore public.

Key Features of the Bill

Government Directions

Under the Bill, the following Government Directions may be issued when:

(1) **there is reasonable suspicion** that an online activity is being carried out to commit *specified criminal offences* (e.g. offences that affect national security, national harmony and individual safety); or

(2) **there is suspicion or reason to believe** that an online activity is being undertaken to commit a scam or malicious cyber activity offence:

Type of Direction	Who it is issued to	What it means
Stop Communication Direction	Individual or entity who posted the online criminal content	Remove the criminal content so that it is not accessible to persons in Singapore
Disabling Direction	Online Service Provider	Disable access to the criminal content by persons in Singapore
Account Restriction Direction	Online Service Provider	Restrict account which is propagating the criminal content from interacting with persons in Singapore
Access Blocking Direction	Internet Service Provider (ISP)	Disable access to the offending website by persons in Singapore
App Removal Direction	App Distributor	Remove app from the Singapore app distribution service

For more examples of specified criminal offences, click here *(Annex A of the Ministry of Home Affairs' Press Release dated 8 May 2023).* The full list can be found in the First Schedule of the Bill.

Code of Practice & Directives

The Bill also creates a framework to foster closer collaboration between the authorities and designated online service providers to counter specified criminal offences affecting the Singapore public.

Codes of Practice, which may be different depending on the nature of the online services, may require designated online services to have in place systems, processes and measures for the purposes of:

(1) enabling partnerships and sensemaking with the Government to proactively deal with scams and malicious cyber activities:
(2) prevention of scams and malicious cyber activities on the services; and
(3) supporting the Government's enforcement actions against such online crimes.

Where there is persistent risk of scams or malicious cyber activities on the designated online services, the relevant authority may issue a Directive to require the service to implement specific risk reduction measures.

Appeal Mechanism

Recipients of a Government Direction and originators of the online activity targeted by the Direction may appeal to vary or cancel the Direction. The appeal will be heard by a Reviewing Tribunal, which will comprise a District Judge or Magistrate appointed by the President, on the advice of the Cabinet.

Designated online services can appeal to the Minister for Home Affairs against decisions by the relevant authority relating to Codes of Practice and Directives.
For queries or more information, please contact:

Wilson Wong
Director
wilson.wong@amicalaw.com
(65) 6303 6213

Geraldine Tan
Director
geraldine.tan@amicalaw.com
(65) 6303 6231

Anna Toh
Director
anna.toh@amicalaw.com
(65) 6303 6234