Client Update | Corporate Commercial; Technology, Media & Telecommunications *September 2026*

Singapore Passes the Scams (Countermeasures) and Other Matters Bill

Background

On 9 September 2026, Parliament passed the Scams (Countermeasures) and Other Matters Bill (Bill No. 16/2026) (the "**Proposed Act**"), which when enacted will amend five existing statutes: the Protection from Scams Act 2025 ("**PSA**"), the Miscellaneous Offences (Public Order and Nuisance) Act 1906, the Online Criminal Harms Act 2023 ("**OCHA**"), the Police Force Act 2004, and the Banking Act 1970 to strengthen measures to detect, disrupt, and deter scams[1].

Key measures which will be introduced by the Proposed Act include the introduction of new offences to deter misuse of online accounts, the enhancement of the OCHA, and enabling and safeguarding of scam-related information exchange between the Singapore Police Force and key service providers such as financial institutions, telcos, payment and other online platforms[2].

This update examines the specific obligations that the Proposed Act will impose on the key service providers, with a particular focus on telcos.

New Orders Under the Protection from Scams Act 2025

Building upon the Facility Restriction Framework launched in October 2025 which restricts scam mules' access to financial, telecommunications, and Singpass/Corppass services[3], the Proposed Act will introduce new orders relating to scam-enabling services[4].

"Scam-enabling service" is defined very broadly to encompass any service through which money or property moves – including bank accounts, payment accounts, and digital payment token accounts – as well as

---

[1] First reading of the Scams (Countermeasures) and Other Matters Bill | Ministry of Home Affairs

[2] Ibid.

[3] Joint press release by SPF, MAS, IMDA and GovTech on restricting access to facilities for scam mules

[4] Section 3(e) of the Proposed Act defines a "scam-enabling service" to mean any of the following services:

(a) any service through which money or property may be deposited, held, transferred, received or withdrawn, including —
  (i) an account with a bank (including a bank in Singapore);
  (ii) a payment account; or
  (iii) a digital payment token account;
(b) any service through which a person may communicate with any person other than the person providing the service, including —
  (i) a telephone line account; or
  (ii) an online account;
(c) any service of granting a credit facility or allowing a drawdown of a credit facility;
(d) any secondary service that facilitates or enables the use of any service mentioned in paragraph (a), (b) or (c), including —
  (i) any web hosting service; or
  (ii) any domain name registration service;
(e) any other service that may be prescribed, being a service that may be used preparatory to, or in furtherance of, the commission of a scam-related offence;

communication services such as telephone line and online accounts, credit facilities, and ancillary services including web hosting and domain registration. Accordingly, telcos, banks, online platforms, web hosts, and domain registrars will be deemed relevant service providers.

Three new types of orders will be issuable by prescribed officers (including police officers, Commercial Affairs officers, or civilian specialist officers):

- Service Limitation Orders to direct service providers to restrict a scam-enabling service to a named person for up to three years, where the officer suspects or has reason to believe that person will use the service to commit or facilitate a scam. The Proposed Act does not provide guidance on what would constitute "suspects" or "reason to believe". However, the Singapore courts have previously held that "reason to believe" is more than mere suspicion and requires a "chain of probable reasoning" that leads to the conclusion[5]; while "suspicion" is a lower threshold, although it should be clear, grounded and targeted on specific facts[6]. The courts' interpretations in these cases are in the context of different legislation and it remains to be seen whether the Singapore courts will apply a similar interpretation when interpreting the Proposed Act. If so, it means that orders may be issued even on the basis of preliminary indicators of scam-related activity.
- Account Disabling Orders to direct service providers to disable any bank account, payment account, digital payment token account, telephone line account or online account where the officer suspects or has reason to believe[7] that the same has been or will be used preparatory to, or in furtherance of, the commission of a scam-related offence. An account shall be disabled for an initial period of up to 30 days, and can be extended once for a further 30 days. In the context of telephone lines or online accounts, "disable" refers to the preventing of the use of the account to communicate with specified persons or through designated accounts.
- Disclosure Orders to require service providers to hand over compliance-related, account-related or user-related information, if the officer is satisfied that disclosure is necessary or expedient for preventing the commission of a scam-related offence and reasonably believes the service provider is capable of disclosing the information. While the Proposed Act does not define what would constitute "reasonable belief", the Singapore courts have held in the context of interpreting other statutes that it combines a subjective, honestly held belief, and objectively reasonable grounds supporting that belief.[8] Assuming a similar interpretation is adopted in the context of the Proposed Act, then the threshold for the issuance of a Disclosure Order is likely higher than that required for issuing a Service Limitation Order or Account Disabling Order.

All three types of order have extra-territorial effect, regardless where the recipient or the relevant data is located.

Penalties for Non-Compliance

The Proposed Act will impose significant penalties on service providers that fail to comply with the new orders:

[5] *Koh Hak Boon v PP* [1993] SGHC 198
[6] *Gobi a/l A v PP* [2020] SGCA 102
[7] Similar to the Service Limitation Orders, the threshold will likely be relatively low, and an officer need only form a clear, grounded suspicion before issuing the order.
[8] *Mah Kiat Seng v Attorney-General* [2023] SGHC 14, though this was in the context of interpreting Section 7 of the Mental Health (Care and Treatment) Act 2008.

Order / Offence	Penalty (Individual)	Penalty (Non-Individual)
Non-compliance with a Service Limitation or Account Disabling Order	Fine up to $20,000, imprisonment up to 12 months, or both; continuing fine up to $2,000/day	Fine up to $1 million; continuing fine up to $100,000/day
Non-compliance with a Disclosure Order	Fine up to $5,000, imprisonment up to 6 months, or both	Fine up to $10,000
Providing false or misleading information under a Disclosure Order	Fine up to $20,000, imprisonment up to 2 years, or both	Fine up to $40,000
Breach of confidentiality obligations with regards to Orders	Fine up to $125,000, imprisonment up to 3 years, or both	Fine up to $250,000

Immunity for Voluntary Disclosure and Voluntary Action

The Proposed Act will incorporate a framework of statutory immunity for certain acts. A service provider that voluntarily discloses information to a specified officer or public sector agency, in good faith and with reasonable care, is protected notwithstanding any secrecy obligation under the Banking Act 1970, the Personal Data Protection Act 2012, contract, or professional conduct rules. A service provider may also voluntarily prevent use of an account for up to 30 days without first receiving an order, provided the suspicion is grounded at least partly in information from an existing Account Disabling Order or Disclosure Order and the provider acts in good faith[9] and with reasonable care. As a service provider may be exempt from liability arising from such voluntary disclosure or voluntary action if the relevant conditions are met, service providers can take a more pro-active role in the prevention of scams.

Enhanced OCHA Enforcement

With regards to online platforms, the Proposed Act will allow directions issued under Part 2 (Directions Against Offences) of the OCHA, namely stop communication and disabling directions, to be issued if a computer program assesses that an offence has occurred or that an activity is preparatory to a scam, subject to a "responsible officer" authorisation framework. Administrative penalties for non-compliance with a code of practice will be increased from S$1 million to S$10 million per instance, a new compliance order mechanism will be introduced for non-compliance with implementation directives (also capped at S$10 million), and the criminal penalty for non-compliance with a compliance order will be raised to S$10 million with a further fine of up to S$300,000 a day for a continuing offence.

Other Changes Worth Noting

The Proposed Act will allow banks to share customer information with the Singapore Police Force under additional circumstances, closing an erstwhile gap that prevented disclosure of details of joint account holders

[9] In the case of *AHTC v Aljunied-Hougang-Punggol Town Council* [2022] SGCA 72, the Singapore Court of Appeal held that factors relevant when considering whether an act was done in good faith (though in the context of Section 52 of the Town Councils Act 1988) include whether the act in question was done honestly and for proper purposes, with a basic degree of competence and diligence, such that a reasonable person in that position would regard the course of action as inappropriate.

linked to restricted scam victims[10]. The Proposed Act will also empower the Minister to appoint civilian specialist officers with police-style powers of arrest, search and seizure, intended to bolster the recently launched Cyber Command (a unit of the Singapore Police Force launched on 3 July 2026 as part of its strategy to combat cybercrime and scams)[11].

What This Means for Telecommunications Companies

For telcos, the following are noteworthy:

- As telephone line accounts can fall under "scam-enabling services", telcos may therefore receive Service Limitation Orders and Account Disabling Orders directly, and will need to have a process to identify, verify and act on these within whatever timeframe the order specifies. As orders may be served by delivery, registered post, email, or electronic notice, telcos should establish appropriate protocols with personnel who are trained to receive, verify, and act on such orders. Telcos should also ensure that they are able to identify all affected accounts, apply only the restrictions stated in the order, and maintain a complete audit trail of the order (i.e. the affected services, responsible staff who were involved, and completion time with duration and expiry tracking).
- As the 30-day disabling window will be extendable only once, telcos will need internal escalation paths and processes in place to facilitate timely compliance. Accordingly, telcos should ensure clear procedures and timelines are in place for the operations team to receive and verify such orders, and to escalate the same to the appropriate management levels. Telcos may also consider implementing regular training and simulation drills (with appropriate after-action reviews).
- Non-compliance is a criminal offence. Failing to comply with a Service Limitation or Account Disabling Order, without reasonable excuse, will expose an entity to hefty fines as noted above. Additionally, the provision of false or misleading information in response to such an order also carries fines and imprisonment. The Singapore Courts have held that having "reasonable excuse" is assessed from the perspective of a reasonable person in the accused's position, and the accused bears the burden of proving the excuse on a balance of probabilities[12]. Accordingly, telcos should ensure that it documents its efforts to comply with such orders, such that it can better aid any efforts to demonstrate that it has complied with a Service Limitation or Account Disabling Order.
- The regime will apply regardless of where a telco is based or where its data is stored, so foreign telcos serving Singapore subscribers, and Singapore telcos storing data offshore, are not insulated from these obligations.

Next Steps

The Proposed Act will come into effect on a date to be appointed by the Minister. It is recommended that affected stakeholders, particularly telcos and online platforms, begin reviewing internal compliance frameworks, escalation processes and information-sharing protocols ahead of the commencement date.

---

[10] By amending the PSA and the Banking Act 1970.
[11] By amending the Police Force Act 2004.
[12] *Lim Ghee v PP* [1997] SGHC 108 in the context of the Building Control Act 1989 and *PP v Lim Yong Kiat* [2018] SGHC 137 in the context where "reasonable excuse" operates as a defence.

This Client Update was authored by Ted Teo (Partner) and Chen Jun Wei (Associate).

For more information, please contact:

Ted Teo
Partner – Corporate Commercial;
Technology, Media &
Telecommunications
T: +65 6439 4893
E: ted.teo@shooklin.com

Disclaimer:

This information is provided for general information and does not constitute legal or other professional advice. Specific advice should always be sought in relation to any legal issue. Shook Lin & Bok LLP does not accept any responsibility for any loss which may arise from reliance on the above information.

Shook Lin & Bok LLP
1 Robinson Road #18-00
AIA Tower Singapore 048542
www.shooklin.com

Follow us on LinkedIn