REPUBLIC OF SINGAPORE

GOVERNMENT GAZETTE

BILLS SUPPLEMENT

Published by Authority

NO. 16] **TUESDAY, AUGUST 4** **[2026**

First published in the Government *Gazette*, www.egazette.gov.sg, on 4 August 2026 at 5 pm.

Notification No. B 16 — The Scams (Countermeasures) and Other Matters Bill is published for general information. It was introduced in Parliament on 4 August 2026.

Scams (Countermeasures) and Other Matters Bill

Bill No. 16/2026.

Read the first time on 4 August 2026.

A BILL

intituled

An Act to amend the Protection from Scams Act 2025 and the Miscellaneous Offences (Public Order and Nuisance) Act 1906 to counter and prevent scams, to amend the Online Criminal Harms Act 2023 and the Police Force Act 2004 to enhance enforcement measures and to make related and consequential amendments to the Banking Act 1970.

Be it enacted by the President with the advice and consent of the Parliament of Singapore, as follows:

Short title and commencement

1. This Act is the Scams (Countermeasures) and Other Matters Act 2026 and comes into operation on a date that the Minister appoints by notification in the *Gazette*.

PART 1

AMENDMENT OF
PROTECTION FROM SCAMS ACT 2025

Replacement of long title

2. In the Protection from Scams Act 2025 (called in this Part the Protection from Scams Act), replace the long title with —

"An Act to protect persons from scams by empowering the issuance of orders to banks in Singapore and other service providers to restrict transactions, limit services, disable accounts or disclose information, so as to prevent their services from being used for scam-related offences.".

Amendment of section 2

3. In the Protection from Scams Act, in section 2 —

(*a*) before the definition of "bank", insert —

" "account disabling order" means an order issued under section 6B(1) or (2);";

(*b*) replace the definition of "bank" with —

" "bank" and "bank in Singapore" have the meanings given by section 2(1) of the Banking Act 1970;";

(*c*) after the definition of "credit facility", insert —

" "digital payment token account" has the meaning given by section 2(1) of the Payment Services Act 2019;

"disable" has the meaning given by section 6C;

"disclosure order" means an order issued under section 6G(1) or (2);

"identified person" has the meaning given by section 6A(1);

"identity card" has the meaning given by section 2(1) of the National Registration Act 1965;

"online account" means an account (including a free account and a prepaid account) on an online service;

"online service" has the meaning given by section 2(1) of the Online Criminal Harms Act 2023;

"payment account" has the meaning given by section 2(1) of the Payment Services Act 2019;

"police officer" has the meaning given by section 2(1) of the Police Force Act 2004;";

(*d*) in the definition of "scam offence", after "specified in", insert "Part 1 of";

(*e*) after the definition of "scam victim", insert —

" "scam-enabling service" means 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;

"scam-related offence" means any offence specified in Part 2 of the Schedule;"; and

(*f*) replace the definition of "specified officer" with —

" "service limitation order" means an order issued under section 6A(1);

"service provider" means the provider of a scam-enabling service;

"Singapore public sector agency" has the meaning given by section 2(1) of the Public Sector (Governance) Act 2018;

"specified officer" means a police officer, a Commercial Affairs Officer appointed under section 64(1) of the Police Force Act 2004 or a civilian specialist officer appointed under section 65C of that Act;

"telecommunication service" has the meaning given by section 2 of the Telecommunications Act 1999;

"telephone line account" means any telecommunication service to which a telephone number is allocated;

"unique identification number" means a person's identity card number, passport number or the number of any other similar document of identity issued by a government authority as evidence of the person's nationality or place of residence, and includes a foreign identification number;

"user", in relation to any scam-enabling service, means a person to whom the service is provided by a service provider.".

Amendment of section 3

4. In the Protection from Scams Act, in section 3, after "one or more banks", insert "in Singapore".

Amendment of section 4

5. In the Protection from Scams Act, in section 4, after "one or more banks", insert "in Singapore".

New section 5A

6. In the Protection from Scams Act, after section 5, insert —

"**Disclosure to specified officer of information on persons who must be notified of issue of restriction order**

5A. If a specified officer issues a restriction order to a bank in Singapore under section 4(1), the bank must disclose the following information to a specified officer:

(*a*) the name, contact details and last known residential address or registered address of every person who must be notified of the issue of the restriction order, as prescribed by regulations;

(*b*) the unique identification number and date of birth of the scam victim in relation to whom the restriction order is issued;

(*c*) any other prescribed information.".

New Part 2A

7. In the Protection from Scams Act, after Part 2, insert —

"PART 2A

ORDERS RELATING TO SCAM-ENABLING SERVICES

Division 1 — Service limitation orders and account disabling orders

Service limitation orders

6A.—(1) If a specified officer suspects or has reason to believe that a person (called in this Act the identified person) will use a scam-enabling service to commit, or facilitate the commission of, a scam-related offence, the specified officer may issue an order (called in this Act a service limitation order) to the service provider of the scam-enabling service, directing the service provider to restrict the provision of the scam-enabling service to the identified person for a period of 3 years or any shorter period that may be specified in the order.

(2) A service limitation order must specify —

(*a*) the name of the identified person;

(*b*) any other information about the identified person that is necessary to enable the service provider to whom the order is issued to identify the identified person;

(*c*) the scam-enabling service the provision of which the service provider must restrict;

(*d*) the period for which the service provider must restrict the provision of the scam-enabling service to the identified person; and

(*e*) the time at which the order takes effect.

Account disabling orders

6B.—(1) If a specified officer suspects or has reason to believe that a bank account, payment account, digital payment token account, telephone line account or online account has been or will be used preparatory to, or in furtherance of, the commission of a scam-related offence, the specified officer may issue an order (called in this Act an account disabling order) to the service provider who provides the account —

(*a*) identifying the account; and

(*b*) directing the service provider to disable the account.

(2) If a specified officer has reason to believe that any bank account, payment account, digital payment token account, telephone line account or online account in relation to which specific conditions (called in this Act disabling conditions) are satisfied is, or is likely to be, an account that has been or will be used preparatory to, or in furtherance of, the commission of a scam-related offence, the specified officer may issue an account disabling order to a service provider —

(*a*) specifying the disabling conditions; and

(*b*) directing the service provider to disable any bank account, payment account, digital payment token account, telephone line account or online account provided by the service provider in relation to which the disabling conditions are satisfied.

(3) A specified officer must not issue any account disabling order that directs a service provider to disable an account for a period of more than 30 days.

(4) An account disabling order must specify —

(*a*) in the case of an order issued under subsection (1) — the name or number of the account and any other information on the account that is necessary to enable the service provider to identify the account;

(*b*) in the case of an order issued under subsection (2) — the disabling conditions;

(*c*) if the order directs a service provider to disable a bank account, payment account or digital payment token account — the specific uses of the account that the service provider must prevent;

(*d*) if the order directs a service provider to disable a telephone line account or online account —

(i) the persons or classes of persons with whom communication by the use of the telephone line account or online account (as the case may be) must be prevented; or

(ii) the other telephone line accounts or online accounts through which communication by the use of the firstmentioned telephone line account or online account (as the case may be) must be prevented;

(*e*) the period for which a service provider must disable the account identified in the order or an account in relation to which the disabling conditions are satisfied; and

(*f*) the time at which the order takes effect.

(5) The disabling conditions of an account disabling order may be specified generally, or specifically in relation to particular

classes of bank accounts, payment accounts, digital payment token accounts, telephone line accounts and online accounts.

(6) Without limiting subsection (5), the disabling conditions of an account disabling order may include (but are not limited to) the following conditions:

(*a*) if the order directs a service provider to disable a bank account, payment account or digital payment token account, that —

(i) the account was used to carry out a specified number of transactions, or transactions of a specified type, during a specified period;

(ii) the account was used to carry out transactions in relation to a specified amount of money or property during a specified period;

(iii) the account was used to carry out a transaction with a specified bank account, payment account or digital payment token account or with a bank account, payment account or digital payment token account the user of which is a specified person; or

(iv) the user of the account is a specified person;

(*b*) if the order directs a service provider to disable a telephone line account or online account, that —

(i) the account was used to communicate with any person in a specified manner;

(ii) the account was used to communicate with specified persons or with persons through other specified telephone line accounts or other specified online accounts, as the case may be; or

(iii) the user of the account is a specified person.

Meaning of "disable"

6C. For the purposes of this Act —

(*a*) a service provider "disables" a bank account, payment account or digital payment token account in accordance with an account disabling order by preventing the use of the account for one or more of the following, as specified in the order:

(i) the deposit of money or property;

(ii) the holding of money or property;

(iii) the transfer of money or property;

(iv) the receipt of money or property;

(v) the withdrawal of money or property; and

(*b*) a service provider "disables" a telephone line account or online account in accordance with an account disabling order by preventing the use of the account to —

(i) communicate with any person or class of persons specified in the order; or

(ii) communicate with any person through other telephone line accounts or other online accounts specified in the order.

Cancellation of service limitation order or account disabling order

6D.—(1) A specified officer may, at any time, cancel a service limitation order or account disabling order.

(2) The cancellation of a service limitation order or account disabling order does not affect the operation of the order, or anything done or omitted to be done in compliance with the order, before the date of its cancellation.

Variation of service limitation order or account disabling order

6E.—(1) A specified officer may vary a service limitation order issued to a service provider by permitting the service provider to provide a scam-enabling service specified in the order to the identified person, subject to any limit or condition that the specified officer may specify to the service provider.

(2) A specified officer may vary an account disabling order issued to a service provider by permitting the service provider to do the following, subject to any limit or condition that the specified officer may specify to the service provider:

(*a*) if the order directs the service provider to disable a bank account, payment account or digital payment token account — allow the use of the account for one or more of the following:

(i) the deposit of money or property;

(ii) the holding of money or property;

(iii) the transfer of money or property;

(iv) the receipt of money or property;

(v) the withdrawal of money or property;

(*b*) if the order directs the service provider to disable a telephone line account or online account —

(i) allow the use of the account to communicate with any person or class of persons; or

(ii) allow the use of the account to communicate with any person through any other telephone line account or online account.

(3) A specified officer may, at any time before the end of the period mentioned in section 6B(4)(*e*), extend the period for a further period not exceeding 30 days.

(4) A specified officer must not extend a period under subsection (3) more than once.

Offence of failure to comply with service limitation order or account disabling order

6F.—(1) Any service provider who is issued a service limitation order or account disabling order and who, without reasonable excuse, fails to comply with the order commits an offence.

(2) A person who is guilty of an offence under subsection (1) shall be liable on conviction —

(*a*) in the case of an individual, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 12 months or to both and, in the case of a continuing offence, to a further fine not exceeding $2,000 for every day or part of a day during which the offence continues after conviction; or

(*b*) in any other case, to a fine not exceeding $1 million and, in the case of a continuing offence, to a further fine not exceeding $100,000 for every day or part of a day during which the offence continues after conviction.

Division 2 — Disclosure orders

Disclosure orders

6G.—(1) A specified officer may issue an order (called in this Act a disclosure order) to a service provider who has been issued a service limitation order or account disabling order, directing the service provider to disclose the following information to the persons specified in the order:

(*a*) in the case of a service provider to whom a service limitation order has been issued —

(i) information on whether the service provider has restricted the provision of the scam-enabling service specified in the service limitation order to the identified person; or

(ii) information on whether the service provider has, on its own motion, restricted the provision of any other scam-enabling service to the identified person, and if so, information on the other scam-enabling service;

(*b*) in the case of a service provider to whom an account disabling order has been issued —

(i) information on whether the service provider has disabled the bank account, payment account, digital payment token account, telephone line account or online account as directed under the account disabling order;

(ii) information on whether any bank account, payment account, digital payment token account, telephone line account or online account provided by the service provider satisfies any disabling condition of the account disabling order; or

(iii) any other information relating to the bank account, payment account, digital payment token account, telephone line account or online account directed to be disabled under the account disabling order, or relating to any user of the account.

(2) A specified officer may issue a disclosure order to any service provider directing the service provider to disclose any information relating to any bank account, payment account, digital payment token account, telephone line account or online account provided by the service provider, or any user of such an account, to the persons specified in the order, if the specified officer —

(*a*) is satisfied that the disclosure is necessary or expedient for preventing the commission of a scam-related offence; and (*b*) believes on reasonable grounds that the service provider is capable of disclosing the information.

(3) A disclosure order must specify —

(*a*) the information that the service provider to whom the order is issued must disclose;

(*b*) the circumstances under which the service provider must disclose the information;

(*c*) the persons to whom the service provider must make the disclosure;

(*d*) the purpose of the disclosure;

(*e*) the manner in which the service provider must make the disclosure; and

(*f*) the time by which the service provider must make the disclosure or, if the order directs the service provider to make the disclosure at regular intervals, the frequency at which the service provider must make the disclosure.

(4) A disclosure order directing a bank to disclose customer information has no effect unless the Authority has issued a notice under section 55(1) of the Banking Act 1970 to the bank, or a class of banks that includes the bank, that requires the bank to comply with the disclosure order or with such disclosure orders generally.

(5) In this section and section 6J(2) —

"Authority" means the Monetary Authority of Singapore established by section 3 of the Monetary Authority of Singapore Act 1970;

"customer information", in relation to a bank, has the meaning given by section 40A of the Banking Act 1970.

Cancellation of disclosure order

6H.—(1) A specified officer may, at any time, cancel a disclosure order.

(2) The cancellation of a disclosure order does not affect the operation of the order, or anything done or omitted to be done in compliance with the order, before the date of its cancellation.

Variation of disclosure order

6I. A specified officer may vary any of the following:

(*a*) the information that a service provider is directed by a disclosure order to disclose;

(*b*) the circumstances under which the service provider must disclose the information;

(*c*) the persons to whom the service provider must make the disclosure;

(*d*) the manner in which the service provider must make the disclosure;

(*e*) the time by which, or the frequency at which, the service provider must make the disclosure.

Offences of failure to comply with disclosure order and providing false or misleading information

6J.—(1) Subject to subsection (2), any service provider who is issued a disclosure order directing the service provider to disclose information to any other person commits an offence if the service provider —

(*a*) without reasonable excuse, fails to comply with the order; or

(*b*) wilfully or recklessly provides to the other person —

(i) information that is false or misleading in a material particular; or

(ii) information that omits any matter or thing without which the information is misleading in a material particular.

(2) Subsection (1)(*a*) does not apply to a bank acting in accordance with a notice issued by the Authority mentioned in section 6G(4).

(3) A person who is guilty of an offence under subsection (1)(*a*) shall be liable on conviction —

(*a*) in the case of an individual, to a fine not exceeding \$5,000 or to imprisonment for a term not exceeding 6 months or to both; or

(*b*) in any other case, to a fine not exceeding \$10,000.

(4) It is not a defence to a charge for an offence under subsection (1)(*a*) that the service provider is subject to a duty of confidentiality or privacy imposed by any rule of law or a duty imposed by any contract or any rule of professional conduct, that prevents or restricts the service provider from complying with a requirement of the disclosure order.

(5) A person who is guilty of an offence under subsection (1)(*b*) shall be liable on conviction —

(*a*) in the case of an individual, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 2 years or to both; or

(*b*) in any other case, to a fine not exceeding \$40,000.

Division 3 — Miscellaneous

Application of orders under this Part outside Singapore

6K. A service limitation order, account disabling order or disclosure order may be issued to a person —

(*a*) whether the person is a resident or citizen of Singapore or is physically present in Singapore or outside Singapore;

(*b*) whether the person (not being an individual) is formed, constituted or registered in Singapore or outside Singapore;

(*c*) whether the person is carrying on a business or is operating in Singapore or outside Singapore;

(*d*) whether the order directs the person to do or not do any act in Singapore or outside Singapore; and (*e*) whether the order directs the person to disclose any information stored in Singapore or outside Singapore.

Service of orders under this Part

6L.—(1) A service limitation order, account disabling order or disclosure order may be served on an individual —

(*a*) by giving it to the individual personally;

(*b*) by sending it by prepaid registered post to the address specified by the individual for the service of documents generally or, if no address is so specified, the individual's residential address or business address;

(*c*) by leaving it at the individual's residential address with an adult apparently resident there, or at the individual's business address with an adult apparently employed there;

(*d*) by affixing a copy of the order in a conspicuous place at the individual's residential address or business address; or

(*e*) by sending it by email to the individual's last email address.

(2) A service limitation order, account disabling order or disclosure order may be served on a partnership (other than a limited liability partnership) —

(*a*) by giving it to any partner or other similar officer, or an authorised representative, of the partnership;

(*b*) by leaving it at, or by sending it by prepaid registered post to, the partnership's business address; or

(*c*) by sending it by email to the partnership's last email address.

(3) A service limitation order, account disabling order or disclosure order may be served on a body corporate (including a limited liability partnership) or unincorporated association —

(*a*) by giving it to the secretary or other similar officer of the body corporate or unincorporated association, or the manager of the limited liability partnership;

(*b*) by leaving it at, or by sending it by prepaid registered post to, the registered office or principal office in Singapore of the body corporate or unincorporated association; or

(*c*) by sending it by email to the last email address of the body corporate or unincorporated association.

(4) Service of a service limitation order, account disabling order or disclosure order takes effect —

(*a*) if the order is sent by email, at the time that the email becomes capable of being retrieved by the person to whom it is sent; and

(*b*) if the order is sent by prepaid registered post, 2 days after the day the order was posted (even if it is returned undelivered).

(5) In addition, a service limitation order, account disabling order or disclosure order may be served on an individual, partnership, body corporate or unincorporated association by giving an electronic notice to the individual, partnership, body corporate or unincorporated association (called in this section an addressee) by the addressee's chosen means of notification, stating that the order is available and how the addressee may use the addressee's chosen means of access to access the order's contents.

(6) A service limitation order, account disabling order or disclosure order may also be served on a person —

(*a*) by email sent to the last email address given by the person to a designated officer, the competent authority, an authorised officer, a police officer or an enforcement officer for the service of documents under section 45 of the Online Criminal Harms Act 2023; or (*b*) by an electronic means that the person has nominated as a chosen means of notification for the giving or serving of a document by a chosen means of access under section 45 of the Online Criminal Harms Act 2023.

(7) In this section —

"authorised representative", in relation to a partnership (other than a limited liability partnership), means any person authorised to accept service of documents on behalf of the partnership;

"business address" means —

(*a*) in the case of an individual, the individual's usual or last known place of business in or outside Singapore; or

(*b*) in the case of a partnership (other than a limited liability partnership), the partnership's principal or last known place of business in or outside Singapore;

"chosen means of access", for an addressee on whom is or is to be served a service limitation order, account disabling order or disclosure order, means an electronic means that the addressee agrees with any specified officer as the means by which the addressee may access the contents of any service limitation order, account disabling order or disclosure order;

"chosen means of notification", for an addressee on whom is or is to be served a service limitation order, account disabling order or disclosure order, means an electronic means that the addressee nominates to any specified officer as the means by which the addressee may be notified that any service limitation order, account disabling order or disclosure order has been served on the addressee;

"last email address" means the last email address given by the addressee concerned to any specified officer as the email address for the service of orders under this Act;

"residential address" means an individual's usual or last known place of residence in or outside Singapore.

Confidentiality of information contained in or provided under orders under this Part

6M.—(1) A service provider to whom a service limitation order, account disabling order or disclosure order is issued must not —

(*a*) disclose any information contained in the order to any other person; or

(*b*) use any information contained in the order for any purpose other than to prevent or detect the commission of a scam-related offence,

except where lawfully required or allowed to do so by or under the service limitation order, account disabling order or disclosure order, by or under the provisions of any written law or by any court.

(2) A person who receives any information that was provided to the person under a disclosure order, knowing that such information was provided under a disclosure order, must not —

(*a*) disclose the information to any other person; or

(*b*) use the information for any purpose other than to prevent or detect the commission of a scam-related offence,

except where lawfully required or allowed to do so by or under a service limitation order, account disabling order or disclosure order, by or under the provisions of any written law or by any court.

(3) A service provider to whom a service limitation order, account disabling order or disclosure order is issued must take

the prescribed measures to ensure the confidentiality of any information contained in the order.

(4) A person who receives any information that was provided to the person under a disclosure order, knowing that such information was provided under a disclosure order, must take the prescribed measures to ensure the confidentiality of the information.

(5) Any person who, without reasonable excuse, contravenes subsection (1), (2), (3) or (4) commits an offence.

(6) A person who is guilty of an offence under subsection (5) shall be liable on conviction —

(*a*) in the case of an individual, to a fine not exceeding $125,000 or to imprisonment for a term not exceeding 3 years or to both; or

(*b*) in any other case, to a fine not exceeding $250,000.

Jurisdiction of courts

6N.—(1) Where an offence under this Part is committed by a person wholly or partly outside Singapore, the person may be dealt with in respect of that offence as if the offence had been committed wholly in Singapore.

(2) Despite the Criminal Procedure Code 2010, a District Court or a Magistrate's Court has jurisdiction to try any offence under this Part and has power to impose the full punishment for any such offence.".

Amendment of section 7

8. In the Protection from Scams Act, in section 7 —

(*a*) after subsection (1), insert —

"(1A) Any of the following persons may appeal to the Commissioner against any decision of a specified officer under this Act in relation to a service limitation order:

(*a*) the identified person in relation to the order;

(*b*) any other person who is a user of the scam-enabling service specified in the order.

(1B) Any user of any bank account, payment account, digital payment token account, telephone line account or online account directed to be disabled under an account disabling order may appeal to the Commissioner against any decision of a specified officer under this Act in relation to the account disabling order."; and

(*b*) in subsection (2)(*c*), delete "after the time of receipt of the notification relating to the decision appealed against".

Amendment of section 8

9. In the Protection from Scams Act, in section 8 —

(*a*) replace subsection (1) with —

"(1) The Commissioner may designate any of the following persons to hear and determine, in the Commissioner's place, appeals generally or a class of appeals or any specific appeal:

(*a*) for appeals against decisions of specified officers under this Act in relation to restriction orders — an appropriate officer;

(*b*) for appeals against decisions of specified officers under this Act in relation to service limitation orders or account disabling orders — a police officer not below the rank of superintendent or any other specified officer of a rank equivalent to superintendent.";

(*b*) in subsection (2), replace "subsection (1)" with "subsection (1)(*a*)"; and (*c*) after subsection (2), insert —

"(2A) Upon a designation under subsection (1)(*b*), any reference in section 7 to the Commissioner includes a reference to the specified officer so designated for that appeal.".

Amendment of section 9

10. In the Protection from Scams Act, in section 9 —

(*a*) in the section heading, delete "**restriction**";

(*b*) in subsection (1)(*a*) and (*b*), after "bank", insert "in Singapore"; and

(*c*) replace subsection (2) with —

"(2) No criminal or civil liability is to be incurred by —

(*a*) a service provider; or

(*b*) an officer, employee or agent of a service provider,

for anything done or omitted to be done in good faith and with reasonable care —

(*c*) in complying with any service limitation order, account disabling order or disclosure order; or

(*d*) in the execution or purported execution of any duty under this Act.

(3) In this section and sections 9A(1) and 9B(1), "officer" —

(*a*) in relation to a corporation, means any director, chief executive, manager, secretary or other similar officer of the corporation, and includes —

(i) any person purporting to act in any such capacity; and

(ii) for a corporation whose affairs are managed by its members — any of those members as if the member were a director of the corporation;

(*b*) in relation to an unincorporated association (other than a partnership), means the president, the secretary or any member of the committee of the unincorporated association, and includes —

(i) any person holding a position analogous to that of president, secretary or member of the committee of the unincorporated association; and

(ii) any person purporting to act in any such capacity; and

(*c*) in relation to a partnership (including a limited partnership), means a partner of the partnership, and includes any person purporting to act as a partner of the partnership.”.

New sections 9A and 9B

11. In the Protection from Scams Act, after section 9, insert —

“**Immunity for voluntary disclosure of information**

9A.—(1) Despite any obligation of a prescribed service provider as to secrecy or any other restrictions upon the disclosure of information imposed by any written law (including the Banking Act 1970 and the Personal Data Protection Act 2012), rule of law, contract or rule of professional conduct, the prescribed service provider, or an officer, employee or agent of the prescribed service provider authorised to act for the prescribed service provider —

(*a*) may disclose information in the circumstances mentioned in subsection (2);

(*b*) is not liable for any loss arising out of any disclosure of information in the circumstances mentioned in subsection (2); and

(*c*) does not commit any offence under section 48D, 48E or 48F of the Personal Data Protection Act 2012 in disclosing information in the circumstances mentioned in subsection (2).

(2) The circumstances mentioned in subsection (1)(*a*), (*b*) and (*c*) are that —

(*a*) the prescribed service provider has been issued an account disabling order or disclosure order;

(*b*) the information disclosed —

(i) is obtained by the prescribed service provider in the course of complying with, or on the basis of information contained in, the order mentioned in paragraph (*a*);

(ii) is related to any bank account, payment account, digital payment token account, telephone line account or online account, or any user of such an account; and

(iii) is within a prescribed class of information;

(*c*) the information is disclosed to a specified officer or a prescribed Singapore public sector agency in the prescribed form and manner;

(*d*) the information is disclosed for the purpose of preventing any scam-related offence in good faith and with reasonable care; and

(*e*) any conditions that may be prescribed are satisfied.

Immunity for voluntary actions

9B.—(1) A service provider, or an officer, employee or agent of a service provider authorised to act for the service provider —

(*a*) may prevent the use (in whole or in part) of any bank account, payment account, digital payment token account, telephone line account or online account in the circumstances mentioned in subsection (2), even if the service provider has not been issued any account disabling order relating to the account; and

(*b*) is not liable for any loss arising out of any act mentioned in paragraph (*a*).

(2) The circumstances mentioned in subsection (1)(*a*) and (*b*) are that —

(*a*) the service provider suspects or has reason to believe that the account has been or will be used preparatory to, or in furtherance of, the commission of a scam-related offence;

(*b*) the suspicion or belief mentioned in paragraph (*a*) is based (in whole or in part) on information contained in an account disabling order or disclosure order issued to the service provider;

(*c*) the account is prevented from use for a period of not more than 30 days;

(*d*) the service provider acted in good faith and with reasonable care; and

(*e*) any conditions that may be prescribed are satisfied.".

Amendment of Schedule

12. In the Protection from Scams Act, in the Schedule —

(*a*) replace the Schedule heading with —

"PART 1

SCAM OFFENCES"; and

(*b*) after Part 1 (as amended by paragraph (*a*)), insert —

“PART 2

SCAM-RELATED OFFENCES

1. Offences under the Computer Misuse Act 1993.
2. Offences under sections 51, 54, 55 and 55A of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992.
3. Offences under Part 6A of the Miscellaneous Offences (Public Order and Nuisance) Act 1906.
4. Offences under section 19 of the Moneylenders Act 2008.
5. Offences under Chapters 12 and 18 and sections 170, 383 to 389, 405 to 409, 415 to 420A, 424A and 424B of the Penal Code 1871.
6. The following offences under the Securities and Futures Act 2001:
   (*a*) offences under section 204 for contravention of section 197, 199, 200, 201, 201A, 201B or 202;
   (*b*) offences under section 210 for contravention of section 207 or 209.
7. An abetment of, or a conspiracy or an attempt to commit, an offence mentioned in item 1, 2, 3, 4, 5 or 6.”.

PART 2

AMENDMENT OF MISCELLANEOUS OFFENCES (PUBLIC ORDER AND NUISANCE) ACT 1906

Amendment of Part 6A heading

13. In the Miscellaneous Offences (Public Order and Nuisance) Act 1906 (called in this Part the Miscellaneous Offences Act), in Part 6A, in the Part heading, after “SIM CARDS”, insert “AND DESIGNATED ONLINE ACCOUNTS”.

New Division 1 heading of Part 6A

14. In the Miscellaneous Offences Act, in Part 6A, before section 39A, insert —

"*Division 1 — Preliminary*".

Amendment of section 39A and new Division 2 heading of Part 6A

15. In the Miscellaneous Offences Act, in section 39A —

(*a*) in subsection (1), after the definition of "compromised SIM card", insert —

""designated online account" means an online account on a designated online service;

"designated online service" means an online service designated as a designated online service under section 20(1) of the Online Criminal Harms Act 2023;

"online account" means an account (including a free account, a prepaid account and anything that may reasonably be regarded as the equivalent of an account) on an online service;

"online service" has the meaning given by section 2(1) of the Online Criminal Harms Act 2023;"; and

(*b*) after subsection (3) (including the *Illustration*), insert —

"(4) For the purposes of this Part —

(*a*) a reference to a person (*C*) selling, renting, lending or supplying a designated online account to another person (*D*) includes a reference to *C* selling, renting, lending or supplying to *D* any information (such as a username, a password or a user authentication code) that *D* may use to obtain control of the designated online account; and (*b*) a reference to *C* buying, renting, borrowing or receiving a designated online account from *D* includes a reference to *C* buying, renting, borrowing or receiving from *D* any information (such as a username, a password or a user authentication code) that *C* may use to obtain control of the designated online account.

Division 2 — SIM cards".

New Division 3 of Part 6A and new Division 4 heading of Part 6A

16. In the Miscellaneous Offences Act, after section 39G, insert —

"*Division 3 — Designated online accounts*

Supplying, etc., of designated online account for criminal activity

39GA.—(1) A person commits an offence if the person —

(*a*) sells, rents, lends or otherwise supplies, or offers to sell, rent, lend or otherwise supply, a designated online account to another person; and

(*b*) does so knowing, or having reasonable grounds to believe, that the designated online account will be used —

(i) to commit, or to facilitate the commission by any person of, any offence under any written law; or

(ii) to cause, or to facilitate the causing by any person of, wrongful gain or wrongful loss to any person.

(2) In proceedings for an offence under subsection (1) involving the fault element mentioned in subsection (1)(*b*)(i), a person (*X*) who does an act mentioned in subsection (1)(*a*) is presumed, until the contrary is proved, to have reasonable grounds to believe that the designated online account will be

used to commit, or to facilitate the commission by a person of, an offence under any written law, if —

(*a*) *X* does the act for any gain; or

(*b*) at the time *X* does the act, *X* fails to take reasonable steps to ascertain —

(i) the identity and physical location of the person to whom the designated online account is supplied; or

(ii) the purpose for which the person receives the designated online account from *X*.

(3) A person who does an act mentioned in subsection (1)(*a*) does not commit an offence if, at the time the person does the act, the person has reasonable grounds to believe that the purpose of the act is to facilitate the use of, or access to, the designated online account for a lawful purpose.

(4) For the purpose of proving whether a designated online account was used to commit, or to facilitate the commission of, an offence, it is not necessary for the prosecution to prove that a specific offence occurred.

(5) Subject to subsection (6), a person who commits an offence under subsection (1) shall be liable on conviction —

(*a*) in the case of an individual —

(i) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and

(ii) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both; or

(*b*) in any other case —

(i) to a fine not exceeding $20,000; and

(ii) in the case of a second or subsequent conviction, to a fine not exceeding $40,000.

(6) Where an individual is convicted of an offence under subsection (1) involving the fault element mentioned in subsection (1)(*b*)(i), the individual shall, in addition to the punishment under subsection (5)(*a*), be liable to caning of not more than 12 strokes if the individual knew that the designated online account will be used to commit, or to facilitate the commission by any person of, any scam offence.

(7) For the purposes of subsection (6), it is not necessary for the prosecution to prove that the commission, or facilitation of the commission, of a scam offence was carried out.

Receiving, retaining control, etc., of designated online account for criminal activity

39GB.—(1) A person commits an offence if the person —

(*a*) does any of the following acts:

(i) buys, rents, borrows or otherwise receives, or offers to buy, rent, borrow or otherwise receive, a designated online account;

(ii) retains control of a designated online account opened using another person's personal information; and

(*b*) does so intending to use the designated online account, or to supply the designated online account to any other person —

(i) to commit, or to facilitate the commission by any person of, any offence under any written law; or

(ii) to cause, or to facilitate the causing by any person of, wrongful gain or wrongful loss to any person.

(2) In proceedings for an offence under subsection (1) involving the fault element mentioned in subsection (1)(*b*)(i), a person (*X*) who does an act mentioned in subsection (1)(*a*)(i) is presumed, until the contrary is proved, to have the intent to use or supply (as the case may be) the designated online account to

commit, or to facilitate the commission by a person of, an offence under any written law, if *X* does the act for any gain.

(3) A person who does an act mentioned in subsection (1)(*a*) does not commit an offence if, at the time the person does the act, the person has reasonable grounds to believe that the purpose of the act is to facilitate the use of, or access to, the designated online account for a lawful purpose.

(4) For the purpose of proving whether a designated online account was used to commit, or to facilitate the commission of, an offence, it is not necessary for the prosecution to prove that a specific offence occurred.

(5) Subject to subsection (6), a person who commits an offence under subsection (1) shall be liable on conviction —

(*a*) in the case of an individual —

(i) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and

(ii) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both; or

(*b*) in any other case —

(i) to a fine not exceeding $20,000; and

(ii) in the case of a second or subsequent conviction, to a fine not exceeding $40,000.

(6) Where an individual is convicted of an offence under subsection (1) involving the fault element mentioned in subsection (1)(*b*)(i), the individual shall, in addition to the punishment under subsection (5)(*a*), be liable to caning of not more than 12 strokes if the individual intended to use the designated online account or to supply the designated online account to any other person, to commit, or to facilitate the commission by any person of, any scam offence.

(7) For the purposes of subsection (6), it is not necessary for the prosecution to prove that the commission, or facilitation of the commission, of a scam offence was carried out.

Unlawful provision, etc., of person's personal information for purpose of opening designated online account

39GC.—(1) A person commits an offence if —

(*a*) the person —

(i) provides, or offers to provide, the person's personal information to be used by another person; or

(ii) consents to, or offers to consent to, the person's personal information being used by another person; and

(*b*) the person does so knowing, or having reasonable grounds to believe —

(i) that the person's personal information will be used to open a designated online account; and

(ii) that the designated online account will be used —

(A) to commit, or to facilitate the commission by any person of, any offence under any written law; or

(B) to cause, or to facilitate the causing by any person of, wrongful gain or wrongful loss to any person.

(2) In proceedings for an offence under subsection (1) involving the fault element mentioned in subsection (1)(*b*)(ii)(A), a person (*X*) who does an act mentioned in subsection (1)(*a*) is presumed, until the contrary is proved, to have reasonable grounds to believe that the designated online account will be used to commit, or to facilitate the commission by a person of, an offence under any written law, if —

(*a*) *X* does the act for any gain; or

(*b*) at the time *X* does the act, *X* fails to take reasonable steps to ascertain —

(i) the identity and physical location of the person who uses *X*'s personal information to open the designated online account; or

(ii) the purpose for which the person uses *X*'s personal information to open the designated online account.

(3) A person who does an act mentioned in subsection (1)(*a*) does not commit an offence if, at the time the person does the act, the person has reasonable grounds to believe that the purpose of the act is to facilitate the use of, or access to, the designated online account for a lawful purpose.

(4) For the purpose of proving a person's state of mind under subsection (1)(*b*), it is not necessary for the prosecution to prove that the designated online account was used to commit, or to facilitate the commission of, a specific offence.

(5) Subject to subsection (6), a person who is guilty of an offence under subsection (1) shall be liable on conviction —

(*a*) in the case of an individual, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; or

(*b*) in any other case, to a fine not exceeding $20,000.

(6) Where an individual is convicted of an offence under subsection (1) involving the fault element mentioned in subsection (1)(*b*)(ii)(A), the individual shall, in addition to the punishment under subsection (5)(*a*), be liable to caning of not more than 12 strokes if the individual knew that the personal information will be used to open a designated online account that will be used to commit, or to facilitate the commission by any person of, any scam offence.

(7) For the purposes of subsection (6), it is not necessary for the prosecution to prove that the commission, or facilitation of the commission, of a scam offence was carried out.

Division 4 — Miscellaneous".

Amendment of section 39H

17. In the Miscellaneous Offences Act, in section 39H, replace "or 39G(1)" with ", 39G(1), 39GA(1), 39GB(1) or 39GC(1)".

PART 3

AMENDMENT OF
ONLINE CRIMINAL HARMS ACT 2023

Amendment of section 2

18. In the Online Criminal Harms Act 2023 (called in this Part the Online Criminal Harms Act), in section 2(1) —

(*a*) after the definition of "competent authority", insert —

" "compliance order" means an order given under section 24A(1)(*a*);";

(*b*) replace the definition of "implementation directive" or "directive" with —

" "implementation directive" means a directive given under section 24(1);";

(*c*) replace the definition of "non-compliant online service" with —

" "non-compliant online service" means an online service of an online service provider who did not comply with —

(*a*) a code of practice that applies to the online service; or

(*b*) a Part 2 direction, a rectification notice, an implementation directive, a compliance order or a Part 6 order, in relation to that online service or any online activity, online material, online account, app, online service or online location that can be accessed on or through that online service;"; and

(*d*) replace the definition of "rectification notice" with —

""rectification notice" means a notice given under section 23(1)(*a*);".

Amendment of section 6

19. In the Online Criminal Harms Act, in section 6, after subsection (3), insert —

"(4) Despite subsection (1), a Part 2 direction may be given by the operation of a computer program for which a responsible officer is responsible, if there is an assessment by the operation of the computer program —

(*a*) that a specified offence has been, or is likely to have been, committed and that any online activity is, or is likely to be, in furtherance of the commission of the offence; or

(*b*) that any online activity is, or is likely to be, preparatory to, or in furtherance of, the commission of a scam or malicious cyber activity offence.

(5) A Part 2 direction given under subsection (4) is deemed to be a Part 2 direction that is given by a designated officer.

(6) In this section —

"chief executive", in relation to a public authority, means the individual (however designated) who is appointed as the chief executive officer of the public authority, and includes any individual acting in that capacity;

"responsible officer", in relation to a computer program, means —

(*a*) a Permanent Secretary who authorised the use of the computer program by designated officers who are public officers from a particular Ministry or department of the Government (including officers under a secondment arrangement);

(*b*) the chief executive of a public authority who authorised the use of the computer program by designated officers employed by the public authority;

(*c*) the Commissioner of Police appointed under section 6(1) of the Police Force Act 2004 who authorised the use of the computer program by designated officers who are police officers within the meaning given by section 2(1) of the Police Force Act 2004, Commercial Affairs Officers appointed under section 64(1) of that Act or civilian specialist officers appointed under section 65C of that Act; or

(*d*) any other public officer appointed by a Minister as a responsible officer.".

Amendment of section 19

20. In the Online Criminal Harms Act, in section 19 —

(*a*) in subsection (1)(*a*), replace "against" with "that directly or indirectly counter"; and

(*b*) in subsections (2) and (3), replace "or an implementation directive" with ", an implementation directive or a compliance order".

Amendment of section 23

21. In the Online Criminal Harms Act, in section 23 —

(*a*) replace the section heading with —

"**Regulatory action for non-compliance with code of practice**";

(*b*) replace subsection (1) with —

"(1) If (whether upon a review of a report given pursuant to a code of practice or otherwise) the competent authority is of the opinion that a designated provider has not complied with any part of a code of practice that applies to the designated provider's service, the competent authority may —

(*a*) give the designated provider a notice (called in this Act a rectification notice) to rectify the non-compliance with that part of the code of practice within the permitted time; or

(*b*) subject to section 24B, order the designated provider to pay, in respect of each instance of non-compliance with the code of practice, a financial penalty of any amount not exceeding $10 million that the competent authority thinks fit, within the time specified in the order."; and

(*c*) in subsections (2) and (4), replace "subsection (1)" with "subsection (1)(*a*)".

Amendment of section 24

22. In the Online Criminal Harms Act, in section 24 —

(*a*) in subsection (1), after "directive", insert "(called in this Act an implementation directive)";

(*b*) in subsection (4), replace "subsection (1)" with "subsections (1) and (7) and section 24A";

(*c*) in subsection (6), after "given that", insert "implementation"; and

(*d*) after subsection (6), insert —

"(7) A designated provider that is given an implementation directive must ensure that the system, process or measure specified in the implementation directive remains implemented from the end of the permitted time until the implementation directive is cancelled or substituted under subsection (5).”.

New sections 24A, 24B and 24C

23. In the Online Criminal Harms Act, after section 24, insert —

“**Regulatory action for non-compliance with implementation directive**

24A.—(1) If the competent authority is of the opinion that a designated provider has not implemented any system, process or measure in compliance with an implementation directive given to the designated provider within the permitted time, the competent authority may —

(*a*) give the designated provider an order (called in this Act a compliance order) to comply with the implementation directive; or

(*b*) subject to section 24B, order the designated provider to pay, within the time specified in the order, a financial penalty of any amount not exceeding \$10 million that the competent authority thinks fit.

(2) A compliance order under subsection (1)(*a*) must set out —

(*a*) details of the non-compliance with the implementation directive; and

(*b*) the time within which the implementation directive must be complied with.

(3) This section applies to any non-compliance by a designated provider with an implementation directive that occurs entirely on or after the date of commencement of section 23 of the Scams (Countermeasures) and Other Matters Act 2026, whether the implementation directive was given to the designated provider before, on or after that date.

Procedure for ordering designated provider to pay financial penalty under section 23(1)(*b*) or 24A(1)(*b*)

24B.—(1) The competent authority must, before ordering a designated provider to pay a financial penalty under section 23(1)(*b*) or 24A(1)(*b*), give a written notice to the designated provider —

(*a*) stating that the competent authority intends to order the designated provider to pay a financial penalty under section 23(1)(*b*) or 24A(1)(*b*), as the case may be;

(*b*) specifying the details of the designated provider's non-compliance that is the subject of the order; and

(*c*) specifying the time within which written representations may be made to the competent authority as to why the designated provider should not be ordered to pay the financial penalty.

(2) The time mentioned in subsection (1)(*c*) must not be earlier than 7 days from the date of service of the written notice under subsection (1) on the designated provider.

(3) The competent authority may, after considering any written representation made by the designated provider under subsection (1)(*c*), decide to order or not to order the designated provider to pay a financial penalty under section 23(1)(*b*) or 24A(1)(*b*), as the case may be.

(4) When the competent authority has made a decision under subsection (3) against a designated provider, the competent authority must serve on the designated provider a written notice of the decision.

(5) A decision that is specified in a written notice given under subsection (4) takes effect from the date on which that notice is given, or on any other date that may be specified in the notice or decided by the Minister in an appeal.

Recovery of financial penalties

24C.—(1) If a person fails to pay any financial penalty imposed on the person under this Act by the date on which the financial penalty is due, the person is liable to pay the competent authority interest on the amount unpaid at the prescribed rate or, if no rate is prescribed, at the same rate as for a judgment debt.

(2) Any financial penalty and any interest on any financial penalty payable by a person under this Act is recoverable by the competent authority as a debt due to the competent authority from that person.

(3) The competent authority may, in any case in which the competent authority thinks fit, waive, remit or refund in whole or in part any financial penalty or any interest on any financial penalty payable under this Act.

(4) Any financial penalty and any interest on any financial penalty collected by the competent authority under this Act must be paid into the Consolidated Fund.".

Amendment of section 25

24. In the Online Criminal Harms Act, in section 25, in the table, after item 4, insert —

"5. Decision to order a designated provider to pay a financial penalty under section 23(1)(*b*) or 24A(1)(*b*)	The designated provider.".

Amendment of section 26

25. In the Online Criminal Harms Act, in section 26 —

(*a*) in subsection (2)(*b*), delete "or" at the end;

(*b*) in subsection (2), after paragraph (*b*), insert —

"(*ba*) if the appeal is against a decision to order a designated provider to pay a financial penalty under section 23(1)(*b*) or 24A(1)(*b*) — the date of service of the written notice of the decision on the designated provider under section 24B(4); or”;

(*c*) in subsection (6), after “against”, insert “(other than any decision to order a designated provider to pay a financial penalty under section 23(1)(*b*) or 24A(1)(*b*))”; and

(*d*) after subsection (7), insert —

“(7A) Without limiting subsection (7), in an appeal against a decision to order a designated provider to pay a financial penalty under section 23(1)(*b*) or 24A(1)(*b*), the Minister may vary all or any of the following:

(*a*) the amount of the financial penalty;

(*b*) the amount of any interest on the financial penalty;

(*c*) the period within which the designated provider must pay the financial penalty.”.

Amendment of section 47

26. In the Online Criminal Harms Act, in section 47 —

(*a*) renumber the section as subsection (1) of that section;

(*b*) in subsection (1), delete “to whom a Part 2 direction, a notice of designation as a designated online service, a code application notice, a rectification notice, an implementation directive or a Part 6 order may be given”; and

(*c*) after subsection (1), insert —

“(2) The competent authority may by written notice under this section require a designated provider to provide the competent authority with —

(*a*) any information that is relevant to assessing the designated provider’s compliance with any code of practice that applies to the designated provider's service or with any implementation directive given to the designated provider; and

(*b*) any information that is relevant to assessing whether a code application notice or implementation directive should be given to the designated provider.".

Amendment of section 51

27. In the Online Criminal Harms Act, in section 51 —

(*a*) in the section heading, replace "**implementation directive**" with "**compliance order**";

(*b*) in subsection (2)(*a*), replace "an implementation directive" with "a compliance order";

(*c*) in subsection (2)(*b*), replace "the directive" with "the compliance order"; and

(*d*) in subsection (3), replace "$1 million and, in the case of a continuing offence, to a further fine not exceeding $100,000" with "$10 million and, in the case of a continuing offence, to a further fine not exceeding $300,000".

Amendment of section 57

28. In the Online Criminal Harms Act, in section 57 —

(*a*) in subsection (1), after paragraph (*d*), insert —

"(*da*) any compliance order given to the person;"; and

(*b*) in subsection (2), after "an enforcement officer,", insert "a responsible officer mentioned in section 6(4),".

Amendment of Third Schedule

29. In the Online Criminal Harms Act, in the Third Schedule, after item 8, insert —

"9. To educate Singapore end-users of a designated provider's service on how to detect, and protect themselves against, scam or malicious cyber activities.".

Miscellaneous amendments

30. In the Online Criminal Harms Act —

(*a*) in section 28(1), after "implementation directive", insert ", a code of practice that applies to the person's service, a compliance order";

(*b*) in sections 29(2) and 30(2), replace paragraph (*b*) with —

"(*b*) an online location at which an online service of an online service provider can be assessed, if the online service provider did not comply with —

(i) a code of practice that applies to that online service; or

(ii) a Part 2 direction, a rectification notice, an implementation directive, a compliance order or a Part 6 order, in relation to that online service or any online activity, online material, online account, app, online service or online location that can be accessed on or through that online service.";

(*c*) in section 54(2)(*a*), replace "implementation directive or the code of practice concerned" with "compliance order, the code of practice concerned or the implementation directive concerned"; and

(*d*) in section 54(3)(*a*), replace "implementation directive" with "compliance order".

PART 4

AMENDMENT OF POLICE FORCE ACT 2004

New sections 65C and 65D

31. In the Police Force Act 2004, after section 65B, insert —

"**Appointment of civilian specialist officers**

65C. The Minister may appoint any individual to be a civilian specialist officer.

Powers of civilian specialist officers

65D.—(1) A civilian specialist officer may investigate any suspected offence which appears to him or her to have been committed under any written law.

(2) For the purposes of subsection (1), a civilian specialist officer —

(*a*) has all the powers of investigation conferred on police officers —

(i) in relation to the investigation of offences under the Criminal Procedure Code 2010; or

(ii) under any other written law that the Minister may, by notification in the *Gazette*, prescribe,

and is deemed to be a police officer not below the rank of inspector for the purposes of those provisions;

(*b*) may without warrant, arrest any person —

(i) who has been concerned in an arrestable offence or is reasonably suspected of having been involved in one, or against whom a reasonable complaint has been made or credible information has been received of the person having been so concerned or involved;

(ii) who possesses anything that may reasonably be suspected to be stolen or fraudulently obtained property, and who may reasonably be suspected of having committed an offence in acquiring it; or

(iii) who obstructs a civilian specialist officer while that civilian specialist officer is doing his or her duty, or has escaped or tries to escape from the lawful custody of a civilian specialist officer or any other person;

(*c*) when exercising the powers of investigation under the Criminal Procedure Code 2010 in relation to an arrestable offence by virtue of paragraph (*a*), may —

(i) enter any place belonging to or under the control of any person who —

(A) is under arrest in connection with the offence;

(B) is reasonably believed to be connected with the offence; or

(C) is reasonably believed to have given shelter to a person under arrest; and

(ii) search the place for any evidence of the offence;

(*d*) may, when lawfully making a search for anything in any place in respect of any offence —

(i) lawfully detain every person found there until the search is completed; and

(ii) search each person found in the place for any thing sought that can be concealed on a person;

(*e*) may, whenever a person is arrested in the following circumstances, search the person and place in safe custody all articles other than necessary wearing apparel found upon the person:

(i) the person is arrested by a civilian specialist officer under a warrant which does not provide for the taking of bail;

(ii) the person is arrested by a civilian specialist officer under a warrant which provides for the taking of bail but the person cannot furnish bail;

(iii) the person is arrested without warrant by a civilian specialist officer and the person cannot legally be admitted to bail or is unable to furnish bail;

(*f*) may, where the civilian specialist officer has reason to believe that a person whom the civilian specialist officer may lawfully arrest is inside any place —

(i) demand entry to the place;

(ii) enter and search the place if —

(A) entry to the place cannot be gained under sub-paragraph (i); or

(B) an arrest warrant may be issued but cannot be obtained without the risk of the person to be arrested escaping; and

(iii) break open any outer or inner door or window of the place or use any other reasonable means to gain such entry, if the civilian specialist officer is unable to obtain entry to the place despite stating his or her authority and purpose and demanding entry to the place;

(*g*) may break open a place to free himself or herself or any other person who (having lawfully gone inside to make an arrest) is detained in the place;

(*h*) may release any person on bail or personal bond in accordance with Division 5 of Part 6 of the Criminal Procedure Code 2010;

(*i*) may serve on any person (whom the civilian specialist officer has reasonable grounds for believing has committed an offence) a notice to attend court, or require any person to execute a bond to appear before a court, in accordance with Division 6 of Part 6 of the Criminal Procedure Code 2010; and

(*j*) may require a person (whom the civilian specialist officer has reasonable grounds for believing has committed an offence) to surrender the person's travel document in accordance with Division 7 of Part 6 of the Criminal Procedure Code 2010.

(3) A civilian specialist officer —

(*a*) when making an arrest under subsection (2)(*b*), must comply with sections 67, 68, 73, 74, 75 and 76 of the Criminal Procedure Code 2010; and

(*b*) when searching a woman, must comply with section 83(1) of the Criminal Procedure Code 2010,

as if the civilian specialist officer were a police officer.

(4) If a civilian specialist officer has reason to believe that a person whom the civilian specialist officer may lawfully arrest is inside any place and demands entry to that place, any person residing in or in charge of the place must allow the civilian specialist officer free entry and provide all reasonable facilities for a search in the place.

(5) A person arrested by a civilian specialist officer must not be released except on the person's own bond or on bail, or by a written order of a court or of any civilian specialist officer.

(6) The provisions of Divisions 5, 6 and 7 of Part 6 of the Criminal Procedure Code 2010 apply in relation to the exercise of the powers of a civilian specialist officer under subsection (2)(*h*), (*i*) or (*j*) and, for that purpose, any reference in those provisions to an officer, a police officer or a police officer not below the rank of sergeant is a reference to a civilian specialist officer.

(7) For the purposes of subsection (1), section 25 applies to a civilian specialist officer as if he or she were a police officer.

(8) The Commissioner may confer on one or more civilian specialist officers as the Commissioner may determine the

powers of an Assistant Superintendent of Police under any written law that the Minister may, by notification in the *Gazette*, prescribe.

(9) Apart from this section and sections 25 and 65C, this Act does not apply to a civilian specialist officer.”.

PART 5

RELATED AND CONSEQUENTIAL AMENDMENTS

Related and consequential amendments to Banking Act 1970

32. In the Banking Act 1970 —

(*a*) in section 55(2)(*q*), delete “and” at the end;

(*b*) in section 55(2)(*r*), replace the full-stop at the end with “; and”;

(*c*) in section 55(2), after paragraph (*r*), insert —

“(*s*) the requirement of a bank or a class of banks to comply with a disclosure order issued to the bank or class of banks by a specified officer under section 6G(1) or (2) of the Protection from Scams Act 2025 or such disclosure orders generally.”; and

(*d*) in the Third Schedule, in Part 1, after item 10, insert —

“

11. Disclosure is required under section 5A of the Protection from Scams Act 2025.	All persons to whom the disclosure is required to be made under that section.	
12. Disclosure is necessary to comply with an order issued to the bank by a specified officer under section 6G(1) or (2) of the Protection from Scams Act 2025.	All persons to whom the disclosure is directed to be made under the order.	

13. Disclosure is made in the circumstances mentioned in section 9A(2) of the Protection from Scams Act 2025.	All persons mentioned in section 9A(2)(*c*) of the Protection from Scams Act 2025.	

”.

PART 6

SAVING AND TRANSITIONAL PROVISIONS

Saving and transitional provisions

33.—(1) Despite section 21 —

(*a*) section 23 of the Online Criminal Harms Act 2023 as in force immediately before the date of commencement of section 21 continues to apply, as if section 21 had not been enacted, to any designated provider who fails to comply before that date with any part of a code of practice; and

(*b*) to avoid doubt, section 24B of the Online Criminal Harms Act 2023 also does not apply to any designated provider in respect of such non-compliance.

(2) Despite section 27 —

(*a*) section 51(1) and (3) of the Online Criminal Harms Act 2023 as in force immediately before the date of commencement of section 27(*d*) continues to apply, as if that provision had not been enacted, to any designated provider who fails to comply with a rectification notice that was given before that date; and

(*b*) section 51(2) and (3) of the Online Criminal Harms Act 2023 as in force immediately before the date of commencement of section 27(*b*), (*c*) and (*d*) continues to apply, as if those provisions had not been enacted, to any designated provider who fails to comply with an implementation directive that was given before that date, if the non-compliance started before that date and continues on or after that date.

(3) For a period of 2 years after the date of commencement of any provision of this Act, the Minister may, by regulations, prescribe any additional provisions of a saving or transitional nature consequent on the enactment of that provision that the Minister may consider necessary or expedient.

EXPLANATORY STATEMENT

This Bill seeks to amend various acts to counter and prevent scams and to enhance enforcement measures.

Clause 1 relates to the short title and commencement.

PART 1

AMENDMENT OF PROTECTION FROM SCAMS ACT 2025

Part 1 (clauses 2 to 12) amends the Protection from Scams Act 2025 (the PFSA) to introduce a regime where service providers (mainly banks, telecommunication service providers and online service providers) may be ordered to restrict the provision of certain services, disable accounts or disclose information, so as to prevent the commission of scam-related offences.

Clause 2 replaces the long title to state that the PFSA empowers the issuance of orders to banks in Singapore and other service providers, so as to prevent their services from being used for scam-related offences.

Clause 3 amends section 2 to insert new definitions of various terms, including “scam-enabling service” and “service provider”, which are terms used in the new Part 2A.

A scam-enabling service includes any service through which money or property may be deposited, held, transferred, received or withdrawn, including a bank account. A scam-enabling service also includes any service through which a person may communicate with any person other than the person providing the service, including a telephone line account or an online account.

A service provider means the provider of any scam-enabling service, such as a bank.

Clause 3 also replaces the definition of “bank” with the definitions of “bank” and “bank in Singapore” to be consistent with those in the Banking Act 1970. Part 2 continues to apply to a “bank in Singapore” while Part 2A applies to a service provider which includes a “bank”.

Clauses 4 and 5 amend sections 3 and 4, respectively, to preserve the position that restriction orders issued under section 4(1) may only be issued to banks in Singapore.

Clause 6 inserts a new section 5A. The new section 5A provides that, if a specified officer issues a restriction order to a bank in Singapore, the bank must disclose to the specified officer certain information on every person who must be notified of the issue of the restriction order and on the scam victim in relation to whom the restriction order is issued.

Clause 7 inserts a new Part 2A containing new sections 6A to 6N. The new Part 2A deals with orders relating to scam-enabling services, which are service limitation orders, account disabling orders and disclosure orders.

The new section 6A provides for the issuance of service limitation orders. A service limitation order directs a service provider to restrict the provision of a scam-enabling service by the service provider to a person identified in the order (called the identified person) for a period of 3 years or any shorter period that may be specified in the order. A specified officer may issue a service limitation order if the specified officer suspects or has reason to believe that the identified person will use the scam-enabling service specified in the order to commit, or facilitate the commission of, a scam-related offence. The identified person may be an existing user of services provided by the service provider, or any other person who will be prevented from obtaining services from the service provider by the service limitation order.

The new section 6B provides for the issuance of account disabling orders. An account disabling order directs a service provider to disable a bank account, payment account, digital payment token account, telephone line account or online account provided by the service provider for a period of not more than 30 days. The order must either identify the account or specify conditions (called disabling conditions) that must be satisfied in relation to the account. An example of a disabling condition is the condition that a bank account was used to carry out transactions in relation to a specified amount of money or property during a specified period.

A specified officer may issue an account disabling order that identifies an account if the specified officer suspects or has reason to believe that the account has been or will be used preparatory to, or in furtherance of, the commission of a scam-related offence. A specified officer may issue an account disabling order that specifies disabling conditions if the specified officer has reason to believe that any account in relation to which the disabling conditions are satisfied is, or is likely to be, an account that has been or will be used preparatory to, or in furtherance of, the commission of a scam-related offence.

The new section 6C sets out the definition of “disable”. A service provider “disables” an account by preventing one or more specific uses of the account, as specified in the order. For example, an account disabling order may direct a service provider to disable a bank account by preventing the use of the bank account for the transfer of money or property and the receipt of money or property, or may direct a service provider to disable an online account by preventing the use of the account to communicate with a person or a class of persons specified in the order.

The new section 6D provides for the cancellation of a service limitation order or an account disabling order.

The new section 6E provides for the variation of a service limitation order or an account disabling order. One of the ways in which a specified officer may vary an account disabling order issued to a service provider is by extending the period for which the service provider must disable an account for a further period not exceeding 30 days.

The new section 6F provides that it is an offence for a service provider who is issued a service limitation order or an account disabling order to fail to comply with the order without reasonable excuse.

The new section 6G provides for the issuance of disclosure orders. A disclosure order directs a service provider to disclose the information specified in the order to persons specified in the order.

Under the new section 6G(1), if a service provider has been issued a service limitation order, a specified officer may issue a disclosure order directing the service provider to disclose information such as information on whether the service provider has restricted the provision of the scam-enabling service specified in the service limitation order to the identified person. If the service provider has been issued an account disabling order, a specified officer may issue a disclosure order directing the service provider to disclose information such as information relating to the account that the order directs the service provider to disable.

Under the new section 6G(2), a specified officer may also issue a disclosure order directing a service provider to disclose any information relating to any bank account, payment account, digital payment token account, telephone line account or online account provided by the service provider, or relating to any user of the account, if the specified officer is satisfied that the disclosure is necessary or expedient for preventing the commission of a scam-related offence and believes on reasonable grounds that the service provider is capable of disclosing the information.

However, under the new section 6G(4), a disclosure order directing a bank to disclose customer information has no effect unless the Monetary Authority of Singapore (called MAS) has issued a notice under section 55(1) of the Banking Act 1970 to the bank or a class of banks that includes the bank, that requires the bank to comply with the disclosure order, or with disclosure orders generally.

The new sections 6H and 6I provide for the cancellation and variation, respectively, of a disclosure order.

The new section 6J provides that it is an offence for a service provider who is issued a disclosure order to fail to comply with the order without reasonable excuse. It also provides that it is an offence for a service provider to wilfully or recklessly provide false or misleading information to the person specified in the disclosure order.

The new section 6K provides for the application of service limitation orders, account disabling orders and disclosure orders outside Singapore.

The new section 6L provides for the means of service of service limitation orders, account disabling orders and disclosure orders. Under the new section 6L(6), such orders may be served on a person by email sent to the last email address given by the person to a designated officer, the competent authority, an authorised officer, a police officer or an enforcement officer for the service of documents under section 45 of the Online Criminal Harms Act 2023. Such orders may also be served on a person by an electronic means that the person has nominated as a chosen means of notification for the giving or serving of a document by a chosen means of access under section 45 of the Online Criminal Harms Act 2023.

The new section 6M provides that information contained in a service limitation order, an account disabling order or a disclosure order and information provided under a disclosure order must not be disclosed and must not be used for any purpose other than to prevent or detect the commission of a scam-related offence, except where lawfully required or allowed to do so by or under a service limitation order, an account disabling order or a disclosure order, by or under the provisions of any written law or by any court. Under the new section 6M(5), it is an offence to do so and it is also an offence to fail to take the prescribed measures to ensure the confidentiality of the information.

The new section 6N provides that where a person commits an offence under the new Part 2A wholly or partly outside Singapore, the person may be dealt with in respect of that offence as if the offence had been committed wholly within Singapore. The new section 6N also provides that despite the Criminal Procedure Code 2010, a District Court or a Magistrate’s Court has the jurisdiction to try any offence under the new Part 2A and has power to impose the full punishment for any such offence.

Clause 8 amends section 7 to provide for appeals to the Commissioner of Police (called the Commissioner) against decisions of specified officers in relation to service limitation orders and account disabling orders.

Clause 9 amends section 8 to empower the Commissioner to designate a police officer not below the rank of superintendent or any other specified officer of a rank equivalent to superintendent to hear and determine, in the Commissioner’s place, appeals against decisions of specified officers in relation to service limitation orders or account disabling orders.

Clause 10 amends section 9 to protect a service provider and an officer, employee or agent of a service provider from criminal and civil liability for any act or omission in complying with any service limitation order, account disabling order or disclosure order or in the execution or purported execution of any duty under the PFSA. The immunity applies only if the act was done, or the omission was made, in good faith and with reasonable care.

Clause 11 inserts new sections 9A and 9B.

The new section 9A(1) provides that, despite any obligation of a prescribed service provider as to secrecy or any other restrictions upon the disclosure of information imposed by any written law, rule of law, contract or rule of professional conduct, a prescribed service provider, or an officer, employee or agent of the prescribed service provider authorised to act for the prescribed service provider, may disclose information in the circumstances mentioned in the new section 9A(2). The prescribed service provider and the officer, employee or agent is not liable for any loss arising out of their disclosure of information in those circumstances and does not commit any offence under section 48D, 48E or 48F of the Personal Data Protection Act 2012 in disclosing information in those circumstances. The circumstances are that, among other things, the information disclosed is obtained by the prescribed service provider in the course of complying with, or on the basis of information contained in, an account disabling order or a disclosure order issued to the prescribed service provider.

The new section 9B(1) provides that a service provider, or an officer, employee or agent of a service provider authorised to act for the service provider, may prevent the use (in whole or in part) of any bank account, payment account, digital payment token account, telephone line account or online account in the circumstances mentioned in the new section 9B(2), even though the service provider has not been issued any account disabling order relating to the account. The service provider and the officer, employee or agent is not liable for any loss arising out of that act. The circumstances are that, among other things, the service provider suspects or has reason to believe that the account has been or will be used preparatory to, or in furtherance of, the commission of a scam-related offence and the suspicion or belief is based (in whole or in part) on information mentioned in an account disabling order or disclosure order issued to the service provider.

Clause 12 amends the Schedule to set out scam offences in the new Part 1 of the Schedule and to set out scam-related offences in the new Part 2 of the Schedule.

PART 2

AMENDMENT OF MISCELLANEOUS OFFENCES (PUBLIC ORDER AND NUISANCE) ACT 1906

Part 2 (clauses 13 to 17) amends the Miscellaneous Offences (Public Order and Nuisance) Act 1906.

Clause 13 amends the Part heading of Part 6A to reflect the insertion of new sections 39GA, 39GB and 39GC in Part 6A. The new sections provide for new offences relating to the misuse of designated online accounts.

Clause 14 inserts a new Division 1 heading before section 39A so that section 39A, which sets out the definitions applicable to Part 6A, is contained in the new Division 1 of Part 6A.

Clause 15 amends section 39A to insert new definitions, including the definition of "designated online account". A designated online account is an online account on an online service designated as a designated online service under section 20(1) of the Online Criminal Harms Act 2023. Clause 15 also amends section 39A to make it clear that a reference to a person (*C*) selling, renting, lending or supplying a designated online account to another person (*D*) includes a reference to *C* selling, renting, lending or supplying to *D* any information (such as a username, a password or a user authentication code) that *D* may use to obtain control of the designated online account, and a reference to *C* buying, renting, borrowing or receiving a designated online account from *D* includes a reference to *C* buying, renting, borrowing or receiving from *D* any information (such as a username, a password or a user authentication code) that *C* may use to obtain control of the designated online account.

Clause 16 inserts a new Division 3 in Part 6A. The new Division 3 contains the new sections 39GA, 39GB and 39GC.

The new section 39GA makes it an offence for a person (*X*) to sell, rent, lend or otherwise supply (or offer to sell, rent, lend or otherwise supply) a designated online account to another person, if *X* does this knowing, or having reasonable grounds to believe, that the designated online account will be used to commit (or facilitate the commission of) an offence, or to cause (or facilitate the causing of) wrongful gain or wrongful loss to any person. *X* is presumed to have reasonable grounds to believe that the designated online account will be used to commit (or facilitate the commission of) an offence, if *X* does the act for any gain, or fails to take reasonable steps to ascertain the identity and physical location of the person to whom the designated online account is supplied, or the purpose for which the person receives the designated online account.

Under the new section 39GA(6), where an individual is convicted of an offence under the new section 39GA(1) involving the fault element of knowing, or having reasonable grounds to believe, that the designated online account concerned will be used to commit (or facilitate the commission of) an offence, the individual shall be liable to an additional punishment of caning of not more than 12 strokes if the individual knew that the designated online account will be used to commit (or facilitate the commission of) any scam offence.

The new section 39GB makes it an offence for a person (*X*) to buy, rent, borrow or otherwise receive (or offer to buy, rent, borrow or otherwise receive) a designated online account, or to retain control of a designated online account opened using another person's personal information, if *X* does this intending to use the designated online account (or to supply the designated online account to any other person) to commit (or facilitate the commission of) an offence, or to cause (or facilitate the causing of) wrongful gain or wrongful loss to any person. *X* is presumed to have the intent to use (or supply) the designated online account to commit (or facilitate the commission of) an offence, if *X* does the act for any gain.

Under the new section 39GB(6), where an individual is convicted of an offence under the new section 39GB(1) involving the fault element of intending to use (or supply) the designated online account concerned to commit (or facilitate the commission of) an offence, the individual is liable to an additional punishment of caning of not more than 12 strokes if the individual intended to use (or supply) the designated online account to commit (or facilitate the commission of) any scam offence.

The new section 39GC makes it an offence for a person (*X*) to provide (or offer to provide) *X*'s personal information to be used by another person, or to consent (or offer to consent) to *X*'s personal information being used by another person, if *X* does this knowing, or having reasonable grounds to believe, that *X*'s personal information will be used to open a designated online account and that the designated online account will be used to commit (or facilitate the commission of) an offence, or to cause (or facilitate the causing of) wrongful gain or wrongful loss to any person. *X* is presumed to have reasonable grounds to believe that the designated online account will be used to commit (or facilitate the commission of) an offence, if *X* does the act for any gain, or fails to take reasonable steps to ascertain the identity and physical location of the person who uses *X*'s personal information to open the designated online account, or the purpose for which the person uses *X*'s personal information to open the designated online account.

Under the new section 39GC(6), where an individual is convicted of an offence under the new section 39GC(1) involving the fault element of knowing, or having reasonable grounds to believe, that the individual's personal information will be used to open a designated online account and that the designated online account will be used to commit (or facilitate the commission of) an offence, the individual shall be liable to an additional punishment of caning of not more than 12 strokes if the individual knew that the individual's personal information will be used to open a designated online account that will be used to commit (or facilitate the commission of) any scam offence.

Clause 17 amends section 39H to provide that offences under the new sections 39GA(1), 39GB(1) and 39GC(1) have extra-territorial effect in certain circumstances. Where a person commits an offence under any of those sections wholly or partly outside Singapore, the person may be dealt with as if the offence had been committed wholly within Singapore if any of these circumstances applies.

PART 3

AMENDMENT OF ONLINE CRIMINAL HARMS ACT 2023

Part 3 (clauses 18 to 30) amends the Online Criminal Harms Act 2023 (the OCHA) mainly to introduce administrative financial penalties for non-compliance with a code of practice or an implementation directive.

Clause 18 makes consequential amendments to the definitions of various terms in section 2(1) and inserts a new definition for "compliance order", which is an order given under the new section 24A(1)(*a*).

Clause 19 amends section 6 to provide that a Part 2 direction may be given by the operation of a computer program for which a responsible officer is responsible. A Part 2 direction so given is deemed to be a Part 2 direction given by a designated officer. It may be cancelled or substituted in accordance with section 14 and may be affirmed, cancelled or substituted by a designated officer under section 17 after receipt of an application under section 16 for reconsideration of the Part 2 direction. A responsible officer, in relation to a computer program, is someone who authorises the use of the computer program and may be a Permanent Secretary, the chief executive of a public authority, the Commissioner of Police or a public officer appointed by a Minister.

Clause 20 amends section 19 to provide that one of the purposes of Part 4 is to counter the commission of offences specified in the Second Schedule by promoting or requiring good practices by a designated provider that directly or indirectly counter the commission of offences within a related offence group of its designated online service.

Clause 21 amends section 23 to provide that, if the competent authority is of the opinion that a designated provider has not complied with any part of a code of practice that applies to the designated provider's service, the competent authority may either give the designated provider a rectification notice or order the designated provider to pay a financial penalty of any amount not exceeding $10 million that the competent authority thinks fit. Non-compliance with a rectification notice is an offence under section 51.

Clause 22 amends section 24 to provide that a designated provider who is given an implementation directive must ensure that the system, process or measure specified in the implementation directive remains implemented until the implementation directive is cancelled or substituted.

Clause 23 inserts new sections 24A, 24B and 24C.

The new section 24A provides that, if the competent authority is of the opinion that a designated provider has not implemented any system, process or measure in compliance with an implementation directive given to the designated provider within the permitted time, the competent authority may either give the designated provider an order (called a compliance order) to comply with the implementation directive or order the designated provider to pay a financial penalty of any amount not exceeding $10 million that the competent authority thinks fit. In respect of an implementation directive given before the date of commencement of clause 23, the new section 24A applies to it if non-compliance with that implementation directive occurs entirely on or after that date. If the non-compliance with the implementation directive started before that date, it is an offence under section 51(2), which will continue to apply, and is saved by clause 33.

The new section 24B sets out the procedure for ordering a designated provider to pay a financial penalty under the new section 23(1)(*b*) or 24A(1)(*b*). Before so ordering, the competent authority must give a written notice to the designated provider specifying, among other things, the time within which written representations may be made to the competent authority as to why the designated provider should not be ordered to pay the financial penalty. The competent authority may decide to order or not to order the designated provider to pay a financial penalty after considering any representations made by the designated provider and must serve on the designated provider a notice of its decision.

The new section 24C provides for the recovery of financial penalties. A person who fails to pay any financial penalty imposed on the person under the OCHA by the date on which the financial penalty is due is liable to pay the competent authority interest on the amount unpaid at the prescribed rate or, if no rate is prescribed, at the same rate as for a judgment debt. The competent authority may recover any financial penalty payable by a person under the OCHA and any interest thereon as a debt due to the competent authority from that person. The financial penalty, and any interest, is to be paid into the Consolidated Fund.

Clauses 24 and 25 amend sections 25 and 26, respectively, to provide for appeals by designated providers to the Minister against any decision to order the designated providers to pay financial penalties under the new section 23(1)(*b*) or 24A(1)(*b*). The Minister may, on hearing such an appeal, vary the amount of the financial penalty, the amount of any interest on the financial penalty or the period within which the designated provider must pay the financial penalty.

Clause 26 amends section 47 to provide that a designated officer, the competent authority or an authorised officer may, by written notice, require information necessary for the administration of the OCHA from any person.

Clause 26 also amends section 47 to provide that the competent authority may require a designated provider to provide the competent authority with specific information such as any information relevant to assessing the designated provider's compliance with any code of practice that applies to the designated provider's service.

Clause 27 amends section 51 to provide that a person commits an offence if the person is given a compliance order and, without reasonable excuse, fails to comply with any requirement of the compliance order. It will no longer be an offence for a person who is given an implementation directive to fail to comply with any requirement of the implementation directive. Clause 27 also amends section 51 to increase the penalty for an offence under section 51(1) or (2) to a fine not exceeding $10 million and, in the case of a continuing offence, to a further fine not exceeding $300,000 for every day or part of a day during which the offence continues after conviction.

Clause 28 amends section 57(1) to confer immunity from civil or criminal liability under any written law or rule of law, and from liability for breach of confidence or any disciplinary action by a professional body, for anything done or omitted to be done, with reasonable care and in good faith and for the purpose of complying with or giving effect to any compliance order. Clause 28 also amends section 57(2) to confer immunity from liability on a responsible officer mentioned in section 6(4) for anything done or intended to be done with reasonable care and in good faith in the execution or purported execution of the OCHA.

Clause 29 amends the Third Schedule to provide that one of the purposes of Part 4 is to counter the commission of offences specified in the Second Schedule by requiring a designated provider to implement appropriate systems, processes or measures for the purpose of educating Singapore end-users of a designated provider's service on how to detect, and protect themselves against, scam or malicious cyber activities in relation to a related offence group of its designated online service.

Clause 30 makes consequential amendments to sections 28(1), 29(2) and 30(2) to provide that the competent authority may give a Part 6 order if any person has not complied with a requirement of a code of practice that applies to the person's service or with a compliance order. Clause 30 also makes consequential amendments to section 54 to provide that, among other things, certain duties that prevent or restrict a person from complying with certain requirements of a compliance order are not a defence to an offence under section 51.

PART 4

AMENDMENT OF POLICE FORCE ACT 2004

Part 4 (clause 31) inserts new sections 65C and 65D in the Police Force Act 2004 to provide for the appointment of civilian specialist officers.

The new section 65C provides that the Minister may appoint any individual to be a civilian specialist officer.

The new section 65D provides for the powers of a civilian specialist officer. A civilian specialist officer may investigate any suspected offence which appears to him or her to have been committed under any written law. While civilian specialist officers will initially focus on investigating cybercrime, they may eventually investigate other offences in the future.

A civilian specialist officer has the same powers as the powers that are conferred, or may be conferred, on a Commercial Affairs Officer under section 64. In addition, under the new section 65D(2)(*j*), a civilian specialist officer also has the power to require a person (whom the civilian specialist officer has reasonable grounds for believing has committed an offence) to surrender the person's travel document in accordance with Division 7 of Part 6 of the Criminal Procedure Code 2010.

PART 5

RELATED AND CONSEQUENTIAL AMENDMENTS

Part 5 (clause 32) makes amendments to the Banking Act 1970 that are related to, and consequential on, the amendments to the PFSA in Part 1.

First, section 55 is amended to provide that MAS may give a notice under section 55(1) in respect of the requirement of a bank or a class of banks to comply with a disclosure order issued to the bank or class of banks under the new section 6G(1) or (2) of the PFSA or such disclosure orders generally.

Second, the Third Schedule is amended to provide that a bank in Singapore or any of its officers may disclose customer information for any of the following purposes:

(*a*) the disclosure is required under the new section 5A of the PFSA;

(*b*) the disclosure is necessary to comply with a disclosure order issued to the bank under the new section 6G(1) or (2) of the PFSA;

(*c*) the disclosure is made in the circumstances mentioned in the new section 9A(2) of the PFSA.

PART 6

SAVING AND TRANSITIONAL PROVISIONS

Part 6 (clause 33) provides for saving and transitional provisions.

EXPENDITURE OF PUBLIC MONEY

This Bill will not involve the Government in any extra financial expenditure.