ONLINE CRIMINAL HARMS ACT 2023
CODE OF PRACTICE FOR E-COMMERCE SERVICES

1. This Code of Practice is issued pursuant to Section 21(1)(*b*) of the Online Criminal Harms Act 2023 ("the Act") and applies to all designated e-commerce services[1].

2. It will come into operation on 26 June 2024.

3. All providers of designated e-commerce service ("Designated Providers") must take all reasonably practicable steps to comply with this Code of Practice, including but not limited to implementing appropriate systems, processes or measures to counter and prevent the use of their designated online service(s) for the commission of scams and/or malicious cyber activity offences specified in the Second Schedule to the Act.

Requirements

4. The requirements under this Code of Practice aim to achieve the following:

(a) the quick disruption of malicious accounts and activities;
(b) the deployment of safeguards to prevent propagation of malicious activities; and
(c) accountability.

5. All Designated Providers must implement appropriate systems, processes or measures within six (6) months from the date of application of this Code of Practice as stated in the Code Application Notice that is issued to you, or unless otherwise informed by the competent authority, to do the following:

Section A – Quick Disruption of Malicious Accounts and Activities

A1) Proactively detect, and promptly take all necessary actions[2] against, suspected scams and/or malicious cyber activities, as well as accounts which are used to commit or facilitate them, including compromised, inauthentic or bot[3]-controlled accounts.

A2) Allow Singapore end-users to report suspected scams and/or malicious cyber activities, compromised end-user accounts and accounts that

[1] E-Commerce service means any online service which provides a platform that (i) enables consumer-to-consumer and/or business-to-consumer sales; (ii) facilitate the buying, selling and/or renting of products and/or services; (iii) enables end-users to promote or advertise products and/or services to other users. "Designated e-commerce service" means an e-commerce service that has been designated under s20(a) of the Act.
[2] Actions to be taken include, but are not limited to reviewing, investigating, verifying, warning, suspending, or restricting the scams and/or malicious cyber activities, and accounts used to commit or facilitate them, with the outcome of disrupting the scams and/or malicious cyber activities.
[3] "Bot" means a computer program made or altered for the purpose of running automated tasks.

impersonate the end-users, through an easily accessible reporting mechanism; and take appropriate actions[4] promptly.

A3) Implement a fast-track channel to facilitate the receipt of reports on scams and/or malicious cyber activities from relevant law enforcement agencies. Such reports may include information on trends or modalities of scams and/or malicious cyber activities. Designated Providers shall act on the reports promptly and update the agencies expeditiously on the specific measures taken or to be taken to detect, prevent and minimise the occurrence of, similar activities, and on the implementation timeline.

A4) Inform relevant law enforcement agencies expeditiously of any detected trends or modalities of scams and/or malicious cyber activities occurring on the designated services and provide relevant associated information, and the actions that have been taken by the Designated Providers to address them.

A5) Retain all available data of accounts detected as being used or having been used for scams and/or malicious cyber activities, such as records that identify the user(s) of the account, records of transactions or interactions, activity logs, IP addresses and metadata, for a minimum of 90 days, in order to facilitate potential criminal investigation into the scams and/or malicious cyber activities.

A6) Maintain and preserve any such records requested by law enforcement agencies for criminal investigations into scams and/or malicious cyber activities for as long as is deemed necessary by the law enforcement agencies.

A7) Facilitate requests for information and data from law enforcement agencies, including putting in place expedited channels for emergency requests.

Section B – Deployment of Safeguards to Prevent Propagation of Malicious Activities

B1) Ensure reasonable verification measures are put in place to prevent the creation and usage of accounts, including compromised, inauthentic or bot-controlled accounts, for scams and/or malicious cyber activities.

B2) Conduct additional verification procedures on an account when there is detection of suspicious conduct or activity by the account.

B3) Require holders of accounts to have strong login verification features.

[4] Actions to be taken include, but are not limited to reviewing, investigating, verifying, warning, suspending, or restricting the scams and/or malicious cyber activities, and accounts used to commit or facilitate them, with the outcome of disrupting the scams and/or malicious cyber activities

B4) Provide holders of accounts with the option to designate their accounts as ‘verified’, that comes with stronger verification measures. Inform end-users that ‘verified’ accounts are more likely to be authentic and more reliable, and the process and criteria for obtaining such status.

B5) Subject users who advertise or post about the sales of goods and/or services, or those who intend to do so, to verification against Government-issued records.

B6) Provide, as an option for users, payment protection mechanisms that require the delivery of goods or services to be verified before payment is released to sellers.

Section C – Accountability

C1) Submit to the competent authority an annual report on the implementation of measures and efforts to counter and prevent scams and/or malicious cyber activities covered in sections A and B, in accordance with the timeline as stated in the Code Application Notice that is issued to the Designated Providers, or unless otherwise informed by the competent authority. The report shall include, but is not limited to the following information:

i. Descriptions of existing and new policies, programs, systems, techniques, processes and other measures implemented to detect, prevent and respond to scams and/or malicious cyber activities on the online service(s).

ii. New challenges in countering and preventing scams and/or malicious cyber activities on the online service(s), such as changes in tactics employed by malicious actors.

iii. Measures being explored or developed to improve existing systems and techniques to detect, prevent and respond to scams and/or malicious cyber activities on the online service(s).

iv. Suitable metrics and information, proposed by the Designated Providers and subject to the agreement of the competent authority, on the effectiveness of the implemented measures. This may include, but is not limited to the following:
    a) Number of accounts/ contents associated with scams and/or malicious cyber activities, proactively detected and removed or banned; and
    b) Number of Singapore end-user reports received, number of Singapore end-user reports on which actions were taken, and time taken to take action from the moment of receipt of Singapore end-user reports.