CODE OF PRACTICE FOR PREVENTING AND COUNTERING ABUSE OF ONLINE ACCOUNTS

In exercise of the powers conferred by Section 48 of the Protection from Online Falsehoods and Manipulation Act 2019 ("the Act"), the POFMA Office of the Info-communications Media Development Authority ("POFMA Office"), which has been appointed as the Competent Authority pursuant to Section 6(1) of the Act, hereby issues the Code of Practice for Preventing and Countering the Abuse of Online Accounts.

CITATION AND COMMENCEMENT

2 This Code of Practice for Preventing and Countering the Abuse of Online Accounts may be cited as the Online Accounts Code and shall come into operation on 2 October 2019.

INTERPRETATION

3 For the purpose of this Online Accounts Code, the following definitions shall apply:

a. "*bot*" has the same meaning as defined in Section 2 of the Act[1];
b. "*inauthentic online account*" has the same meaning as defined in Section 2 of the Act[2]; and
c. *"online account"* has the same meaning as defined in Section 2 of the Act[3].

APPLICATION AND PURPOSE OF THIS ONLINE ACCOUNTS CODE

4 This Online Accounts Code sets out the obligations that prescribed internet intermediaries have to comply with in preventing and countering the abuse of online accounts. This Online Accounts Code shall be read together with the Annex to the Online Accounts Code.

DUE DILIGENCE MEASURES

5 To minimise the likelihood of inauthentic online accounts being used to engage in malicious activities, prescribed internet intermediaries must put in place reasonable due diligence measures to:

---

[1] "bot" means a computer program made or altered for the purpose of running automated tasks.
[2] "inauthentic online account" means an online account that is controlled by a person other than the person represented (whether by its user profile, unique identifier or other information) as its holder, and the representation is made for the purpose of misleading end-users in Singapore of any internet intermediary service as to the holder's identity.
[3] "online account" means an account created with an internet intermediary for the use of an internet intermediary service.

a. Safeguard against misrepresentation of the identity of an end-user;
b. Ensure that bots' activities are not confused with human interactions; and
c. Limit abuse of their platforms through the use of inauthentic online accounts.

6 The due diligence measures stated in paragraph 5 above must include the following:

a. Having a published policy that prohibits the misrepresentation of identity, such as impersonation, and states what constitutes impermissible use of bots, such as manipulations to trending topics or artificially boosting the popularity of a piece of content or an account.

b. Having reasonable verification measures in place to prevent the creation and usage of inauthentic accounts or bots for malicious activities.

c. Conducting additional verification if suspicious conduct or activity is associated with an account.

d. Informing the holders of online accounts to have strong login verification requirements.

e. Providing selected holders of online accounts, the option of a 'verified' account(s) and/or page(s) that comes with stronger verification measures.

f. Informing other end-users that the 'verified' accounts and/or pages are authentic, for example, by inserting a tag next to the handles of verified accounts and/or pages.

g. During election periods (including an election to the office of President, a general election of Members of Parliament, a by-election of a Member of Parliament, or a referendum), prescribed internet intermediaries must verify accounts and/or pages belonging to political parties and candidates.

h. Requiring the holder of any online account that employs a bot to communicate or interact with end-users to effectively disclose the use of the bot(s).

i. Having in place reporting mechanisms for end-users to report the following, and acting on said reports as soon as practicable:
    - Compromised end-user account(s); and
    - Accounts that impersonate verified account(s).

ANNUAL REPORTS

7 Prescribed internet intermediaries shall provide the POFMA Office with an annual report on the implementation of the above measures.

ANNEX TO CODE OF PRACTICE FOR
PREVENTING AND COUNTERING THE ABUSE OF ONLINE ACCOUNTS

In exercise of the powers conferred by Section 48 of the Protection from Online Falsehoods and Manipulation Act ("the Act"), the POFMA Office in the Info-communications Media Development Authority ("POFMA Office"), which has been appointed as the Competent Authority pursuant to Section 6(1) of the Act, hereby issues this Annex to the Code of Practice for Preventing and Countering the Abuse of Online Accounts ("Online Accounts Code").

CITATION AND COMMENCEMENT

2 This Annex may be cited as the Annex to the Online Accounts Code and shall come into operation on 2 October 2019.

INTERPRETATION

3 For the purposes of this Annex, the definitions in the Online Accounts Code shall apply.

APPLICATION AND PURPOSE

4 This Annex sets out the obligations that prescribed internet intermediaries are required to comply with in preventing and countering the abuse of online accounts. This Annex shall be read together with the Online Accounts Code.

DUE DILIGENCE MEASURES

5 Prescribed internet intermediaries are to put in place reasonable due diligence measures to detect and report inauthentic accounts or bots engaging in malicious activities. Examples of malicious activities include inauthentic engagements or activities that manipulate the prominence of an account or content.

6 The due diligence measures stated in paragraph 5 are to include the following:

a. Having in place systems and processes to detect inauthentic accounts or bot-controlled accounts that are engaging in malicious activities on the platforms; and

b. Having in place a fast-track Government reporting channel to receive and respond to Government reports on suspected inauthentic accounts or bots engaging in malicious activities.

7 In the lead-up to or during major events (e.g. election period) or public emergency (e.g. public order incident), the POFMA Office may impose stricter

timeframes for prescribed internet intermediaries to respond to Government reports and take the necessary action as soon as practicable. As far as practicable, the POFMA Office will provide prior notice of the period(s) during which the stricter timeframes apply.

ANNUAL REPORTS

8 Prescribed internet intermediaries shall provide POFMA Office with an annual report containing the following information:

a. Broad descriptions of existing policies, systems and techniques to detect suspected inauthentic accounts or bots engaging in malicious activities on their platforms;

b. New challenges observed in preventing and countering the abuse of online accounts, such as changes in tactics employed by malicious actors; and

c. Measures being explored or developed to improve existing systems and techniques to detect suspected inauthentic accounts or bots engaging in malicious activities on their platforms.