DECISION ISSUED BY THE INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY

ON

PROPOSALS TO STRENGTHEN SAFEGUARDS FOR SMS MESSAGES TO SINGAPORE USERS: IMPLEMENTATION OF ANTI-SCAM FILTER SOLUTION WITHIN MOBILE NETWORKS

14 OCTOBER 2022

BACKGROUND

1. On 15 August 2022, IMDA issued a public consultation on a proposal to implement an anti-scam filter solution within mobile networks to automatically review and filter scam Short Message Service ("**SMS**") messages ("**Anti-Scam Filter**"). This is against the backdrop that scammers commonly impersonate legitimate businesses to deceive victims into clicking links to gain access to victims' data. This has resulted in financial losses by Singapore consumers.

2. The technology to detect and filter potential scam SMS messages is commercially available. Such technology can filter scam SMS messages at the network level using automated machine scanning, based on the following:

    a. SMS messages containing malicious links that may lead consumers to websites asking for sensitive information or installation of malware and viruses; and

    b. Suspicious SMS messages containing patterns indicating that it is a scam message, such as the use of keywords or phrases found commonly in scams.

3. Driven by the significant uptick in scam SMS messages experienced globally, some mobile network operators in countries such as Australia and the United Kingdom have already implemented such Anti-Scam Filter solutions in a bid to better combat against scams. This implementation has since been reported to have blocked more than 50% of scam SMS messages. To allow all consumers to benefit from this additional level of protection, the mobile network operators in Australia and the United Kingdom have deployed such solutions at the network level and applied it to all mobile subscribers by default.

4. Thus, IMDA proposed for local telecom operators ("**Telcos**") to implement these similar commercial solutions in Singapore to reduce the number of scam SMS messages and better protect Singapore consumers. At the close of consultation on 14 September 2022, IMDA received written comments from Telcos and members of the public, and some members of the public have also responded to a survey conducted on the proposals outlined in the public consultation (collectively, the "**Respondents**").

PROPOSED IMPLEMENTATION OF ANTI-SCAM FILTER

IMDA's Proposal in the Consultation Document

5. IMDA proposed for the Anti-Scam Filter to be implemented as follows:

    <u>Filtering of scam SMS messages through the detection of malicious links</u>

    a. The process will be automated, via a machine built into mobile networks, without any human involvement. Specifically,

        i. The links in the SMS messages will be cross-checked against a database of known malicious links. If any link is "matched" against a link contained in

the database, the SMS message will be filtered and the consumer will not receive the SMS message; and

ii. The database will continuously be updated to stay relevant against new threats.

Further filtering of scam SMS messages that contain suspicious patterns

b. This further filtering would be similarly conducted through automated machine scanning without human intervention, as follows:

i. The machine will filter SMS messages based on suspicious patterns contained within, e.g., keywords, phrases and message formats that are typically used in scam SMS messages; and

ii. Machine learning ("**ML**") will be adopted to scan and identify common keywords and new patterns in scam SMS messages in order to keep pace with evolving scam tactics.

c. As part of the ML process, the filtered SMS messages may be further reviewed to ascertain if these are indeed scam messages. The SMS messages will first be anonymised by the machine before being channelled to the Telcos' technical personnel for review. It is envisaged that the ML process will allow the Anti-Scam Filter to develop higher filtering accuracy and efficacy over time.

Summary of Responses

6. Respondents expressed support for the implementation of the Anti-Scam Filter. Telcos also provided feedback that they would be ready to implement these commercially available solutions and put in place the Anti-Scam Filter within their networks. However, some Respondents noted that sufficient time would be needed to ensure proper implementation.

7. Respondents also sought some clarifications on the proposed scope and technical issues.

IMDA's Clarifications

Scope of SMS messages subject to Anti-Scam Filter

8. One Respondent sought clarification on whether all local person-to-person ("**P2P**") and application-to-person ("**A2P**") SMS messages would be subject to scanning, given that:

a. Most scam SMS messages originate internationally;

b. The implementation of IMDA's proposed Full SMS Sender ID Registry ("**SSIR**") Regime will already address A2P scam SMS messages; and

c. There is potential negative impact on the quality of service ("**QoS**") for SMS delivery given a higher volume of SMS messages to be scanned.

9. IMDA notes that scammers will invariably target pathways which remain vulnerable. Unless the Anti-Scam Filter is applied to all types of SMS messages, scammers will adapt their strategies to conduct their scams through pathways that are not subject to scanning (e.g., routing their scam SMS messages through domestic numbers).

10. IMDA notes that the proposed Full SSIR Regime aims to protect the ID layer (i.e., the "label") of the SMS message. On the other hand, the proposed Anti-Scam Filter looks at the body of the SMS message by scanning for malicious content within the SMS message. Both measures complement each other to enhance protection against scams.

11. On the potential impact to the QoS of SMS delivery, IMDA notes that SMS is a legacy technology and messages are not transmitted in real-time today and there are already delays. IMDA further notes that the Anti-Scam Filter solutions implemented overseas do not appear to have adversely affected SMS delivery standards.

Capabilities of Anti-Scam Filter

12. One Respondent highlighted that it would be necessary to ensure that the size of the database of malicious links is manageable and reasonable.

13. IMDA notes that the size of the database of malicious links will be dependent on the Telcos' technical and commercial decisions, given that it would be based on their individual system performance. Thus, Telcos will have to manage this accordingly to ensure smooth operation.

Other suggestions to combat scams

14. A few Respondents highlighted that there are other communication platforms such as over-the-top ("**OTT**") messaging applications (e.g., WhatsApp, Telegram), with one Respondent adding that scammers may switch to these platforms in view of the implementation of the Anti-Scam Filter for SMS.

15. IMDA notes that OTT applications are indeed also used by businesses and may be a target for scammers. IMDA will work alongside relevant stakeholders to review this area.

16. Some Respondents also suggested the following:

    a. ScamShield, an anti-scam application developed by the National Crime Prevention Council and Open Government Products, should be made available for Android devices; and

    b. Reported scam telephone numbers should be automatically blocked.

17. IMDA notes that ScamShield has been officially released for Android devices since 28 September 2022. On the blocking of reported scam telephone numbers, this is already in place today as IMDA has required Telcos to block any scam telephone numbers upon receiving instructions from relevant enforcement agencies.

IMDA'S DECISION

18. Given the overall support for IMDA's proposals, IMDA will work with all relevant Telcos to implement the Anti-Scam Filter solution in Singapore for their subscribers.

19. In summary, IMDA's decision is as follows:

    a. Anti-Scam Filter solution will be installed in Telcos' mobile networks and filtering of scam SMS messages will be done automatically via machine;

    b. Key Telcos (Singtel, StarHub and M1) will start to filter and block SMS messages containing malicious links from 31 October 2022. This service will be extended to subscribers of Mobile Virtual Network Operators on the respective Telco's network; and

    c. Further filtering of scam SMS messages that contain suspicious patterns will be phased in from 2023 onwards.