CONSULTATION PAPER 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

Submission by StarHub Mobile Pte Ltd to the Infocomm Media Development Authority

14 September 2022

Contact Details:	StarHub Mobile Pte Ltd 67 Ubi Avenue 1 #05-01 StarHub Green Singapore 408942 Phone: +65 6825 5000 Fax: +65 6721 5002 Tim Goodchild Email: timothy@starhub.com

Introduction:

1. StarHub Mobile Pte Ltd ("**StarHub**") thanks the Info-comm Media Development Authority of Singapore (the "**Authority**") for providing the opportunity to comment on its proposal to implement an anti-scam filter solution within mobile networks (the "**Proposed Solution**").

2. The Authority's proposals are described at a high-level, without setting out the technical details on the Proposed Solution and its functionalities. In addition, the proposal does not highlight the risks involved with the Proposed Solution. We submit that it is necessary for the Authority to consider the following issues:

- While the proposal indicates that the Proposed Solution will not be fool-proof, it is important to note that:
    - The Proposed Solution is likely to allow through a significant number of scam-related SMS messages. Furthermore, Scammers will keep changing their tactics to circumvent any blocking, and any system will require time to change the blocking rules to play "catch-up" with the scammers' evolving tactics. Any blocking can therefore only be on a best-efforts basis, based on the capabilities of the deployed solution.
    - The Proposed Solution could potentially block legitimate SMS messages. The stricter the blocking rules adopted, the more likely that legitimate SMS messages will be blocked.
    - The Proposed Solution will not apply to other types of messaging apps (such as WhatsApp or Facebook Messenger), which are already used for scams. If scammers find it difficult to send scam SMS, they may simply migrate to other (unregulated) channels.
- The proposal suggests that all SMS messages (including local person-to-person ("**P2P**") messages) will be scanned by the Proposed Solution. This will cover private messages sent locally, and will mean that such messages could potentially be flagged to the mobile network operators ("**MNOs**") for human review. This may raise serious personal data protection issues.
- The Authority has already created a Singapore SMS Sender ID Registry ("**SSIR**") to provide better assurance that "*only bona-fide Organisations are using Sender IDs*". It is therefore unnecessary to scan such "*bona fide*" SMS messages.
- There could be quality of service ("**QoS**") issues if large number of SMS messages are scanned, causing potential delays in the delivery of the messages. The size of the malicious URL database also needs to be carefully managed, to prevent any

overloading of the Proposed Solution. This could potentially cause One-Time-Passwords to "time-out".

3. StarHub's detailed comments on the Authority's Proposed Solution are set-out below.

StarHub's Detailed Comments:

Proposed solution will not be fool-proof:

5. The consultation paper states that anti-scam filter solutions implemented overseas have "*blocked more than 50% of scam SMS messages*". Unfortunately, this still means that almost half of all scam SMS messages will continue to be delivered to customers.

6. It is important to note that, despite best efforts, it is likely that the Proposed Solution will not be able to block all scam SMS messages. As examples of some of the difficulties with blocking of scam SMS messages:

- Scammers will amend the contents of their messages to avoid standard scanning.
- Some SMS messages may exceed the normal character length limit, which results in the malicious URLs being split across multiple messages. The Proposed Solution may therefore need to piece together URLs across multiple SMS messages. This may not always be successful.
- Scammers may disguise their malicious URLs by using link shorteners. It may only be possible to filter SMS messages with the exact match of the malicious URL provided.

7. It is therefore important that the public is not lulled into a false sense of security that scam messages will be blocked if the Proposed Solution is implemented. Blocking by the Proposed Solution is best seen as a best-efforts basis, based on the capabilities of a deployed solution.

8. Furthermore, the Proposed Solution only applies to SMS messages. It does not apply to other channels which are already used for scams. The Police have stated that, for banking-related phishing scams, over-the-top ("**OTT**") applications such as "*IMO, Viber and WhatsApp were the most common platforms used by scammers to communicate with the victims*".[1] Any messages sent through such platforms will continue to reach customers even with the Proposed Solution in-place. Scammers may well migrate to such platforms if they find that some of their SMS messages are being blocked by the Proposed Solution.

<u>Blocking legitimate SMS messages:</u>

9. In addition, it is likely that legitimate SMS messages could end-up being blocked by the Proposed Solution. For example, discussions on loans between two parties (e.g., a relationship manager and a potential new client) may end-up being flagged as suspicious, and end up being blocked.

[1] Quoted from the Singapore Police Force's Annual Crime Brief 2020.

10. To use an analogy, spam filters used by email providers are similarly not fool-proof, and may erroneously classify some legitimate emails as spam. In such cases, the email user may not notice that legitimate emails have been filtered unless they check their spam folders.

11. However, the Proposed Solution sits at a network level, and any SMS messages that are filtered will be blocked entirely. The intended recipients will not know that such SMS messages have been sent (unless alerted by the sender), they cannot review the SMS messages blocked, or request any "unblocking".

12. It is therefore important to note that, while MNOs could implement the Proposed Solution, they cannot be required to justify why certain SMS messages have, or have not, been blocked. All blocking will be done by the deployed solution, based on its capabilities.

Public education campaign:

13. Given the issues highlighted above, we respectfully submit that a public education campaign will be needed on the Proposed Solution, to highlight the issues involved. This is needed to avoid giving the public a wrong impression that the Proposed Solution is fool-proof, thereby creating a false sense of security.

Scope of proposed blocking:

14. The proposal indicates that the Proposed Solution would cover all forms of SMS messages, including:

- P2P messages sent between private parties in Singapore; and
- Application-to-person ("**A2P**") messages, whose Sender IDs are already meant to be registered with the SSIR.

15. We strongly believe that P2P messages sent locally should not be subject to scanning. Our understanding is that the vast majority of scam-related SMS messages originates internationally (the Police have publicly stated that "*at least 90 per cent of scams in Singapore originate from overseas*"[2]*)*. There is therefore little benefit in subjecting all local SMS messages to scanning, when they do not appear to be an area of concern. We elaborate further on our concerns below.

16. We also question the need for scanning A2P messages if the Authority is already intending to mandate the registration of all Sender IDs through the SSIR. The setup of the Proposed Solution will involve significant time and effort. This will not be justifiable if the SSIR is meant to be implemented by the end of the year.

[2] Straits Times, 29-August 2022.

Review of inter-personal SMS messages:

17. As highlighted above, we have serious concerns about having the Proposed Solution scan P2P messages sent between private parties in Singapore. Additionally, we believe that it is unnecessary to have a process that flags "*potentially suspicious*" SMS messages for further review by technical personnel. This creates significant personal data protection issues, even if anonymisation is carried out. While anonymisation could strip the sender and recipient details, nothing stops parties from sending personal details directly within the body of the SMS message.

18. Today, the public treats SMS messages as a secure and private way of exchanging information. In many cases, the public will use SMS messaging to disclose personal and sensitive information. This could include medical information sent by healthcare organisations, or credit card information exchanged between customers and merchants. It will not be feasible to strip out such personal data within the message body itself.

19. If SMS messages could end-up being reviewed by MNOs' personnel, we are concerned that this could significantly compromise the trust in the use of SMS services. As such, any manual review of SMS messages should be made optional for the MNOs. This addresses the personal data concerns associated with conducting manual reviews.

Technical issues:

20. Today, SMS users enjoy a high QoS standard. The Authority's statistics show that nearly 100% of all SMS messages are delivered within 15 seconds.[3] However, implementing the Proposed Solution could result in a fall in the QoS enjoyed by customers as the content of each SMS messages will need to be screened before they can be delivered. If delays are encountered in SMS delivery, this could cause OTPs to "time-out" and fail, thus disrupting the delivery of services to customers.

21. To prevent unnecessary reductions in the QoS enjoyed by customers, we strongly believe that local P2P messages should not be scanned. In addition, A2P messages will already be subject to the SSIR requirement. Hence, there is also no need to scan such SMS messages.

22. Reducing the volume of SMS messages that are scanned by the Proposed Solution will mitigate any negative impact on the QoS for SMS message delivery.

23. Separately, the Authority has indicated that there will be a "*database of malicious links*" which MNOs are required to scan against. It will be necessary to ensure that the size of the database is manageable, with links removed once blocking is no longer needed. There must be an upper limit to the size of any database, and the Proposed Solution will need to work within a reasonable threshold.

---

[3] Reference: https://www.imda.gov.sg/infocomm-media-landscape/research-and-statistics/sms-performance/sms-performance-measurement-for-2021.

Conclusion:

24. In summary, StarHub's key points are as follows:

- A public education campaign will be needed, to highlight the issues involved with the Proposed Solution. In particular:
    - A large number of scam SMS messages may not be blocked by the Proposed Solution. Scammers will keep evolving their tactics to avoid any filter, and any solution will need to play "catch-up" to cover new scam tactics. Any blocking will have to be on a best-efforts basis, based on the capabilities of the solution deployed.
    - Depending on the settings of the Proposed Solution, legitimate SMS messages may be blocked.
    - Other messaging platforms (already used for scams) will not be covered by the Proposed Solution. Scammers will switch to such (unregulated) platforms to carry out scams.

  Public education will be critical in managing customer expectations, and avoiding a misplaced sense of security amongst the public.

- The Proposed Solution should not apply to the following types of SMS messages:
    - Local P2P messages, as the bulk of all scam messages originates from overseas. Scanning such messages also creates unnecessary personal data protection issues.
    - A2P messages, which will already be regulated under the Authority's SSIR regime.

  Limiting the scope of SMS messages to be reviewed will also minimise any negative impact to the QoS for SMS services.

- We seek confirmation that any manual review of "suspicious" messages is optional. Today, the public treats SMS messaging as private and secure. This reputation will be adversely impacted if the content of SMS messages could end up being reviewed by the MNOs.

- Any database of malicious links will need to be reasonably sized to ensure that it works with the Proposed Solution.

25. StarHub is grateful for the opportunity to comment on this matter, and we appreciate the Authority's consideration of our comments.