CONSULTATION PAPER ISSUED BY

THE INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY

ON

PROPOSALS TO STRENGTHEN SAFEGUARDS FOR SMS MESSAGES TO SINGAPORE USERS: FULL SMS SENDER ID REGIME

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 mandate a registration system for alphanumeric sender identifications ("**Sender IDs**") for Short Message Service ("**SMS**") messages in Singapore.

2. We understand and appreciate the Authority's intentions of preventing the spoofing of Sender IDs through the implementation of a mandatory Singapore SMS Sender ID Registry ("**SSIR**"). However, given the potential number of companies that use SMS Sender IDs, there will be a significant adjustment phase, during which companies learn about, and are onboarded onto the SSIR. It is unlikely that all companies will register their SMS Sender IDs by December 2022, and this will inevitably result in significant disruptions to SMS messages sent to Singaporeans.

3. In addition, a mandatory SSIR regime will cause situations where legitimate SMS messages are blocked. These include:

- SMS messages sent by overseas organisations (which are unaware of the SSIR, or have no interest to join the SSIR).

- Travel-related SMS messages sent to outbound roamers (which will first be sent to the local mobile network operators ("**MNOs**") before routing overseas).

4. The blocking of such SMS messages (which may contain One-Time-Passwords, notifications of changes to aircraft departures; and advisory messages from overseas-based banks of account and/or credit card activity) would be extremely disruptive to the intended recipients of those SMS messages in Singapore. Unfortunately, the MNOs will not be in a position to recover / deliver those blocked SMS messages.

5. If the Authority intends to implement a mandatory SSIR regime, it will need to clearly communicate these drawbacks to the public, and to educate the public on the types of SMS messages that they will no longer receive.

6. As an alternative, the Authority could consider requiring the conversion of all unregistered SMS Sender IDs to a standardised Sender ID (which would be defined by the Authority). This will still allow the SMS messages to be sent to the recipient, while alerting the recipient about the potentially suspicious nature of the message. We understand that this process is already adopted by some countries.[1]

[1] Reference: https://support.plivo.com/hc/en-us/articles/360041448032-Country-Requirements-for-Sender-ID-Registration. From this article, we understand the conversion of Sender ID to a standardised ID is adopted by countries such as India, Indonesia and the Philippines.

7. StarHub's detailed comments on the Authority's proposals are set-out below.

StarHub's Detailed Comments:

Impact of SSIR:

9. Today, a variety companies may send out SMS messages with Sender IDs[2] for different purposes. These will include:

- App providers (to send one-time passwords ("**OTPs**");
- Logistics and delivery companies (for updates on delivery timings);
- Restaurants or other service-related organisations (for reservation handling purposes);
- Airlines (to advise of changes in aircraft departures);
- Banks and finance companies (for advisories on account changes and credit card usage);
- Healthcare providers (for sending of medical or appointment information);
- Insurance companies (for notifications on bills); and.
- Retail organisations (for marketing purposes and to provide updates on orders).

10. It will be operationally very challenging for all such companies to be notified of the SSIR, and to complete registration of their Sender IDs by December 2022. Furthermore, some companies may only send out such SMS messages periodically, and would only discover that their messages are blocked after the mandatory SSIR is implemented.

11. Hence, the implementation of the SSIR by December 2022 will inevitably cause teething issues, and result in disruptions to SMS traffic from December 2022 onwards. These problems will be larger for SMS traffic from overseas companies, which may be unwilling to register with the SSIR.

<u>Blocking of legitimate traffic:</u>

12. In addition, we also foresee that the following types of legitimate SMS messages will be blocked once the mandatory SSIR is implemented:

- SMS Sender IDs from overseas companies that are either unaware or have no intention of registering with the SSIR. For example:

[2] For the avoidance of doubt, our understanding is that this requirement does not apply to sender IDs using numbers, whether short code or otherwise.

- Foreigners in Singapore may have relationships with organisations in their home country, such as banks. These parties may attempt to login to their foreign bank accounts, with OTPs sent to their locally registered numbers. However, these OTPs will be blocked, if they are not registered with the SSIR.

- There are a variety of applications that may use OTP for verification of mobile numbers (e.g., mobile games, education and productivity tools). Most application providers are based overseas, and they may have a small minority of their customers located in Singapore. If the OTP are using Sender IDs, they will be blocked.

  In both examples, the overseas organisation may be entirely unaware of the SSIR. Even if they were informed of the SSIR, they may not choose to register given the additional regulatory burden and costs, as well as the small customer base in Singapore. This will mean that mobile customers in Singapore could end up being denied access to certain overseas services and applications.

- SMS Sender IDs to roaming customers. SMS messages sent to roaming customers may well first be routed to the local MNOs' networks, before routing overseas to the roamers' location. Hence, any Sender IDs that are not registered with the SSIR may well end up being blocked. Such messages could include:

  - SMS messages about flight information (e.g., an overseas airline informing customers about flight delays).

  - Hotel booking information (e.g., a hotel notifying customers about check-in and check-out timings).

  - Immigration requirements (e.g., foreign Governments notifying customers about new COVID-19 testing and quarantine requirements).

    If such SMS messages are blocked, this could prove to be very disruptive to the activities of Singaporeans travelling overseas.

13. It is important to understand that, if a company (local or overseas) fails to sign-up with the SSIR and has its SMS messages blocked, it will not be possible to the MNOs to "unblock" that message for the customer in Singapore. The only way to ensure that the SMS messages are not blocked is for that company to register with the SSIR, which some companies may be unwilling to do.

Disputes over registration of Sender IDs:

14. As a consequence of the SSIR, it is possible that some companies may have competing demands over the same Sender ID. For example, there are multiple companies selling pizza, and one company may request to register "PIZZA" as an approved sender ID. To avoid such disputes, the Authority will need to come up with clear guidelines on the types of Sender IDs that companies can register, and a process for handling disputes should companies have competing requests for the same Sender ID.

Exclusions from the SSIR:

15. The SSIR only applies to SMS messages, and does not apply to other messaging channels which are used for scams. For example, 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*".[3] Any messages sent through such OTT platforms will continue to reach customers even with the SSIR in-place. It is likely that scammers will actively migrate to such platforms if they find that their SMS messages are being blocked due to the SSIR.

16. It is therefore important to note that customers will still continue to receive messages with alphanumeric headers through other forms of messaging services.

Alternative suggestion:

17. As an alternative suggestion, rather than blocking all non-registered Sender IDs, the Authority could require the conversion of the Sender IDs to a single generic Sender ID. This is an approach adopted by some overseas jurisdictions. Converting the Sender IDs to a single generic Sender ID will still allow potentially legitimate messages to reach customers, while also providing a warning to customers about the potentially suspicious nature of the SMS message.

18. A similar approach has already been adopted for incoming international calls, which are required to be marked with a "+" symbol to clearly show that the call originates from overseas. This approach similarly allows international incoming calls to reach customers, while providing advance indication to the customer that the call is potentially suspicious.

Public education campaign will be needed:

19. Regardless of the approach taken by the Authority, a public education campaign will be needed to inform customers about the impact of the mandatory SSIR. Customers need to be aware that they may not receive legitimate SMS messages, and may not have access to certain services in the future (such as those using OTPs). Customers also need to be made aware that the SSIR does not apply to other messaging applications, and that customers may continue to receive scam messages via OTT applications.

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

20. Furthermore, the Authority should assist to communicate widely that the SSIR initiative will be going ahead by December 2022, to notify all companies that they have to urgently register with the SSIR to prevent blocking of their Sender IDs. Some form of education will also be necessary for overseas-based companies that send SMS messages to customers in Singapore (and who will be unaware of the SSIR regime).

Conclusion:

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

- There are a variety of companies using Sender IDs, and it will be challenging for all companies to register with the SSIR by December 2022. Inevitably there will be disruptions to SMS communications from December 2022 onwards.

- The implementation of the SSIR may well result in legitimate SMS messages being blocked. In particular:

    - SMS messages from overseas companies which are unaware or have no intention of registering for the SSIR.

    - SMS messages sent to roaming customers.

- The Authority will need to have clear guidelines on the types of Sender IDs that can be registered, and as a process to resolve disputes over competing use of Sender IDs.

- The SSIR only affects SMS messages. This will mean that scammers can continue to use other OTT messaging applications to send messages with alphanumeric headers.

- As an alternative solution, the Authority could consider requiring the conversion of non-registered Sender IDs into a single generic Sender ID. This allows the SMS message to reach the customer, while warning the customer that the message is potentially suspicious. A similar approach has been adopted for incoming international calls.

- Public education efforts will be needed to inform customers about the impact of the SSIR, and that scams may continue via other OTT messaging applications. The Authority also needs to reach out to companies (including overseas-based companies), to inform them of the urgent need to register for the SSIR.

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