DECISION ISSUED BY THE INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY

ON

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

14 October 2022

BACKGROUND

1. Scammers have been masquerading their SMS sent to Singapore mobile users by using the same alphanumeric sender identification ("**Sender ID**") used by bona fide businesses and other entities (herein referred to as "**Organisations**"). The aim is to deceive Singapore mobile users to divulge sensitive information to the scammers, where the scammers can then access the mobile users' accounts, thereby resulting in financial loss to these mobile users.

2. With the surge in scam SMS, in March 2022, IMDA set up the Singapore SMS Sender ID Registry ("**SSIR**")[1]. The SSIR acts as a central body for the registration of Sender IDs to be used in Singapore. It is currently a voluntary regime, where Organisations that wish to protect their Sender IDs ("**Protected Sender IDs**") can register with the SSIR. Therefore, the public is still subject to spoofed SMS, using non-registered Sender IDs (e.g., from Organisations that choose not to register, or Sender IDs that do not belong to any Organisation).

3. On 15 August 2022, IMDA issued a public consultation on a proposal to make Sender ID registration a requirement for all Organisations that choose to use Sender IDs (i.e., the "**Full SSIR Regime**"). The aim was to further secure the SMS communications channel for Singapore consumers.

4. At close of consultation on 14 September 2022, IMDA received strong interest from Organisations and SMS service providers. These were via written replies as well as through engagement sessions with trade associations and industry associations, including the Singapore Business Federation, the Association of Small and Medium Enterprises, the Singapore International Chamber of Commerce, the Asia Pacific Carriers' Coalition, the Airlines Operators Committee and the Board of Airline Representatives in Singapore (each a "**Respondent**" and collectively, "**Respondents**"). IMDA thanks all Respondents for their comments and feedback.

5. Most of the Respondents welcomed progressing to the Full SSIR Regime to better protect Singapore mobile users and Organisations from spoofed SMS. Some Respondents have asked for tweaks at the margins to the proposals to cater to business needs. These are elaborated below.

[1] The SSIR is operated by the Singapore Network Information Centre ("**SGNIC**"), a wholly owned subsidiary of IMDA. As of 14 October 2022, around 210 Organisations and over 40 Aggregators have signed up with the SSIR. More details can be found on SGNIC's website: https://www.sgnic.sg.

FULL SMS SENDER ID REGISTRY REGIME FOR SINGAPORE

Transition to Full SSIR Regime: Minimise Risk of Legitimate Unregistered Sender IDs from being Dropped

IMDA's Consultation Proposal

6. IMDA proposed for all Organisations that send SMS with Sender IDs to Singapore mobile users to register their Sender IDs with the SSIR, and only use SMS service providers or SMS aggregators ("**Aggregators**") that participate in the SSIR.

Summary of Responses

7. Some Respondents expressed concerns that at the point of cut over from voluntary to Full SSIR Regime, there may be Organisations (e.g., overseas businesses) that may still not be aware and not register their Sender IDs with SSIR. Their SMS will thus be dropped under the Full SSIR Regime.

IMDA's Assessment and Decision

8. IMDA notes the concerns of legitimate SMS being dropped. To cater to such cases, IMDA will allow Aggregators to create a common Sender ID "*Likely-SCAM*". All SMS with unregistered Sender IDs will be replaced with the "*Likely-SCAM*" Sender ID and be channelled into this SMS thread. This will be in place for around 6 months from the start of the Full SSIR Regime as a transition measure. IMDA believes there are merits to this transition approach:

   a. Singapore mobile users can still receive SMS from legitimate Organisations if the Organisations do not register in time;

   b. Affected Organisations will be alerted by their customers or Aggregators that their Sender IDs have been changed to "*Likely-SCAM*" and they must now register with SSIR to be able to use their own Sender ID; and

   c. Singapore mobile users will be alerted to be vigilant when receiving SMS with the "*Likely-SCAM*" Sender ID, as SMS in the "*Likely-SCAM*" SMS thread may come from unknown sources and may still contain scam messages – this *"Likely-SCAM"* header functions like the "spam bin" in emails, and Singapore mobile users should exercise caution when accessing its contents.

Organisations must use a Valid UEN when Registering with SSIR

IMDA's Consultation Proposal

9. IMDA proposed that all Organisations that send SMS with Sender IDs must directly register their Sender IDs with SSIR. To do so, Organisations must first present a valid identification, i.e., the local unique entity number ("**UEN**") as issued by relevant government agencies.

Summary of Responses

10. Most Respondents agreed that the approach to use UEN for SSIR registration is reasonable.

11. Some Respondents noted that some Organisations use 3rd party *Merchant Aggregators* to manage and send SMS on their behalf. They have requested for such *Merchant Aggregators* to be able to register Sender IDs with the SSIR and use the registered Sender IDs to send SMS with Sender ID on behalf of various Organisations.

12. Some Respondents have also suggested allowing law firms and firms providing secretariat services to register Sender IDs with the SSIR, which will then be used by their clients, i.e., the Organisations.

IMDA's Assessment and Decision

13. IMDA would reiterate that the purpose of requiring Organisations to register their Sender IDs is to ensure that only bona fide Organisations can use Sender IDs to send SMS to Singapore mobile users. The registrant of the Sender IDs must therefore have full control over the use of the Sender IDs and be held accountable for the Sender IDs they register. This ensures that the registrant and the sender of the SMS is the same entity for every Sender ID.

14. Where any party (e.g., *Merchant Aggregator,* law firm, firm providing secretariat services) registers Sender IDs on 3rd party Organisations' behalf, such party will have no control over the SMS that these 3rd party Organisations send using the registered Sender IDs. On the principle that the registrant of the Sender IDs must have full control over the use of the IDs and must be held accountable for the Sender IDs they register, IMDA will not allow parties such as *Merchant Aggregators,* law firms or firms providing secretariat services to register Sender IDs for use by 3rd party Organisations. However, such parties are allowed to register Sender IDs with a valid UEN, where they will have full control over how the Sender IDs will be used and are held accountable for the Sender IDs registered.

15. IMDA would also clarify that overseas Organisations can register for Sender IDs under their local affiliates, provided the local affiliates are able to comply with SSIR registration requirements, i.e., register with the SSIR with a valid UEN.

Assignment of Sender IDs

IMDA's Consultation Proposal

16. IMDA proposed that Organisations with the valid identification (i.e., the UEN) can register with the SSIR, and protect the Sender IDs they wish to use when sending SMS to Singapore mobile users.

Summary of Responses

17. Some Respondents sought clarification on the assignment process that the SSIR will adopt for Sender IDs, especially if more than one Organisation registers the same Sender ID with the SSIR.

18. Some Respondents also sought clarification on the types of Sender IDs that will require registration with the SSIR.

IMDA's Assessment and Decision

19. SSIR will assign Sender IDs on a first-come-first-served basis, and may clarify with registrants if they have a trademark or other legitimate claim to the Sender ID. This means that Organisations need to register the Sender IDs they want to protect (as per the voluntary SSIR regime today). Sender IDs already registered under the current voluntary SSIR will continue to be registered under the Full SSIR Regime, unless Organisations decide to deregister them.

20. To protect Singapore mobile users from spoofed SMS messages, and Organisations from having their Sender IDs spoofed, the Full SSIR Regime will need to apply to any alphanumeric Sender ID sent to Singapore mobile users, including Application-to-Person ("**A2P**") SMS originating from local and overseas, as well as telecommunication operators' own Sender IDs.

21. Typically, Person-to-Person ("**P2P**") SMS refers to SIM-based SMS sent via SIM cards and the Sender ID is tied to a unique mobile number. The Full SSIR Regime will not apply to P2P numeric Sender IDs used by mobile phone users registered with their respective mobile operators, including P2P traffic originating from overseas.

Fees for Registration with SSIR

IMDA's Consultation Proposal

22. IMDA proposed for the SSIR fees today, i.e., (a) one-time set up fee of $500; and (b) annual fee of $1,000 a year for up to 10 Sender IDs that Organisations wish to protect[2], to remain unchanged under the Full SSIR Regime.

Summary of Responses

23. Some Respondents submitted that the current fees would be high, especially for smaller Organisations, which may spend less than $1,000 a year for SMS services.

IMDA's Assessment and Decision

24. IMDA notes the feedback and will lower the annual charge to $200 per year for each ID. This is to cater to the needs of smaller Organisations, which IMDA notes may only require 1 or 2 Sender IDs.

25. The one-time set up fee of $500 remains unchanged[3].

Implementation Timeline

IMDA's Consultation Proposal

26. IMDA recognised that the requirements under the proposed Full SSIR Regime would require transition by Organisations and Aggregators sending and managing SMS with

[2] Prices listed do not include the applicable Goods & Services Tax.

[3] Prices listed in paragraphs 24 and 25 do not include the applicable Goods & Services Tax.

Sender IDs to Singapore mobile users today. To allow sufficient time for Organisations and Aggregators to adjust, IMDA proposed to provide a transition period starting in October 2022 before the Full SSIR Regime commences in December 2022.

27. IMDA proposed to commence the Full SSIR Regime from December 2022. This would mean that from December 2022, Organisations would not be able to send SMS with unregistered Sender IDs to Singapore mobile users, as they would be dropped by Aggregators handling the SMS. Similarly, Aggregators not participating in the SSIR would no longer handle SMS with Sender IDs meant for Singapore mobile users.

Summary of Responses

28. The Respondents welcomed the ability to commence transition in October 2022.

29. Some Respondents with larger networks of Aggregators submitted that they would require more time to make necessary operational arrangements for transition.

IMDA's Assessment and Decision

30. With the aim to protect Singapore mobile users in mind, IMDA intends to have the Full SSIR Regime implemented as soon as possible to better secure the SMS communications channel from spoofing. However, IMDA notes the industry feedback for more time to transition.

31. To balance industry's request for more time, with the urgent need to protect Singapore mobile users from spoofed SMS messages, IMDA will therefore commence transition from 31 October 2022, but delay the implementation of the Full SSIR Regime by 1 more month to 31 January 2023. Coupled with the availability of the *"Likely-SCAM"* Sender ID which acts as a "spam bin" for around 6 months from the start of the Full SSIR Regime, this will help to allay concerns for Organisations that may need more time.

SUMMARY OF IMDA'S DECISION

32. IMDA will proceed to implement the Full SSIR Regime on 31 January 2023.

33. The key parameters of the Full SSIR Regime are summarised as follows:

Full SSIR Regime	Details
A. Scope	1. All Organisations that wish to send SMS messages with Sender IDs must register with the SSIR. Only registered Sender IDs will reach Singapore users – all non-registered Sender IDs will be blocked. 2. This will cover **all** alphanumeric Sender IDs chosen by Organisations, including: a. A2P SMS originating from local and overseas; and

Full SSIR Regime	Details
	b. The telecommunication operators' own Sender ID SMS. 3. This will **not** apply to P2P SMS traffic (domestic and international).
B. What Organisations need to do	1. **Organisations** that send SMS with Sender IDs to Singapore mobile users must: a. Register Sender IDs with the SSIR; and b. Only use Aggregators that participate in the SSIR. **I. Registration** 2. All Organisations that send SMS with Sender IDs must first present a valid identification, i.e., the local unique entity number ("**UEN**"), as issued by relevant government agencies. 3. Organisations with the valid identification (i.e., the UEN) can then register with the SSIR, and protect the Sender IDs they wish to use when sending SMS to Singapore mobile users. 4. Foreign-based businesses can obtain a UEN by registering with the Accounting and Corporate Regulatory Authority ("**ACRA**"). A foreign business can either register as local subsidiary or register as a foreign branch office. Foreign-based businesses can then register for Sender IDs with SSIR via their local subsidiary or foreign branch office as long as the local subsidiary / foreign branch office can present a valid UEN. Companies registered with ACRA will have to comply with the statutory and disclosure requirements of the Companies Act. 5. Other non-business Organisations (e.g., charity organisation, societies, religious bodies) can also register with the relevant agencies that will issue UEN to these specific types of organisations. 6. The Organisation registering the Sender IDs with SSIR must have full control over the use of the IDs and be held accountable for the Sender IDs it registers. This means that parties such as Merchant Aggregators, law firms and firms providing secretariat services, cannot register

Full SSIR Regime	Details
	Sender IDs, for that Sender ID to be used by 3rd party Organisations. 7. The SSIR registration fees are: a. One-time set up fee of $500; and b. Annual $200 per Sender ID. 8. The SSIR will assign Sender IDs on a first-come-first-served basis, and may clarify with registrants if they have a trademark or other legitimate claim to the Sender ID. **II. Select SMS Aggregators** 9. Organisations sending SMS with Sender IDs will need to choose Aggregators that are licensed by IMDA and registered with the SSIR to handle these SMS to be sent to Singapore mobile users. See Annex A for the current list of aggregators.
C. What Aggregators need to do	1. All Aggregators that handle SMS with Sender IDs to be sent to Singapore mobile users must first be licensed by IMDA. a. Aggregators must minimally obtain a Services-Based Operations (Class) licence from IMDA; b. Any local company or foreign branch office registered with ACRA can apply with IMDA for a Services-Based Operations (Class) licence, and the registration fee is a one-time charge of $200; and c. Regulatory requirements will include, amongst others, to (i) verify that the Organisations are bona fide; (ii) collect and verify the UEN of these Organisations as part of their Know Your Customer ("**KYC**") process; and (iii) ensure that the proper client onboarding process takes place.
D. Transition timeline	1. Organisations can start to register with the SSIR from 31 October 2022 onwards.
E. Implementation timeline	1. IMDA will implement the Full SSIR Regime on 31 January 2023. 2. From 31 January 2023, IMDA will allow Aggregators to create a common Sender ID *"Likely-SCAM"* to allow SMS

Full SSIR Regime	Details
	with unregistered IDs to be channelled into this SMS thread. a. The *"Likely-SCAM"* thread will stay open for around 6 months from the start of the Full SSIR Regime. b. Thereafter it will be closed and all SMS with Sender IDs that are still not registered by then will be blocked.

ANNEX A

List of Participating Aggregators under SSIR (as of 14 October 2022)

1. 8X8 International Pte Ltd
2. Alibaba Cloud (Singapore) Pte Ltd
3. AMCS SG Private Limited (Amazon Media Communications Services)
4. Ann Consulting Pte Ltd
5. Asiatel (S) Pte Ltd
6. CM Telecom Singapore Pte Ltd
7. Crystal Net Pte Ltd
8. EC Web Pte Ltd
9. Etisalat Wholesale Asia Pacific Pte Ltd
10. Fort Digital Pte Ltd
11. GENIQ Pte Ltd
12. Green Packet Global Pte Ltd
13. Hello Technology Pte Ltd
14. Hoiio Pte Ltd
15. IBASIS Singapore Pte Ltd
16. Infinite Convergence Solutions Inc
17. Infobip Mobile Services Pte Ltd
18. M1 Limited
19. Macro Kiosk Pte Ltd
20. Maven Lab Private Limited
21. Messagebird Pte Ltd
22. Micro Cloud Technology Pte Ltd
23. Mobilenet Technologies Pte Ltd
24. Momentum Inc Pte Ltd
25. NCS Pte Ltd
26. Netlynx Communications Pte Ltd
27. NEXMO Pte Ltd
28. NextGen Mobile Pte Ltd
29. Orange Gum Pte Ltd
30. Pacific Synergy Pte Ltd
31. SendQuick Pte Ltd
32. Simba Telecom Pte Ltd
33. Sinch Singapore Pte Ltd
34. Singtel Mobile Singapore Pte Ltd
35. SMSDome Pte Ltd
36. StarHub Mobile Pte Ltd
37. Syniverse Technologies Network Solutions (Singapore) Pte Ltd
38. Talariax Pte Ltd
39. Tata Communications International Pte Ltd
40. Telesign Singapore Pte Ltd
41. Toku Pte Ltd
42. Twilio Singapore Pte Ltd
43. Whispir Pte Ltd