Keeping you connected.

pivotel
connected everywhere

20 March 2024

SMS Sender ID Registry Consultation
Communications Services and Consumer Division
Department of Infrastructure, Transport, Regional Development, Communications and the Arts
GPO Box 594
Canberra ACT 2601

By email: SMSSenderID@infrastructure.gov.au

RE: Consultation on Mandatory vs. Voluntary SMS Sender ID Registry

About Pivotel

Pivotel is a Mobile Network Operator (MNO) that provides mobile and satellite communications. It holds a carrier license issued by the Australian Communications and Media Authority in accordance with the Telecommunications Act 1997 (Cth) ("Telco Act"). It has points of interconnect in the major Australian cities and international points of interconnect in Auckland, Los Angeles and New York.

The Pivotel group comprises Pivotel Group Pty Limited and its wholly-owned subsidiaries, including but not limited to:

1. Pivotel Satellite Pty Limited;
2. Pivotel Mobile Pty Limited; and
3. Pivotel Communications Pty Limited

For this submission, they are referred to severally and collectively as "Pivotel".

Pivotel provides wholesale messaging services to its customers, including facilitating application-to-person (A2P) SMS services.

Pivotel welcomes initiatives across the industry to combat scams. Pivotel participated in the Communications Alliance working committee, which prepared the Reducing Scam Calls and SMs Code. Pivotel is also involved in various forums and committees to help combat scam, including the initial consultations with the ACMA on the establishment of the SenderID registry and the Scam Telecommunication Action Taskforce (STAT).

Pivotel has also led the industry in the development of innovative filtering solutions to prevent scam calling and SMS. In addition, Pivotel has conducted a proof-of-concept trial, called SecureSMS, which enables messages from organisations to be authenticated by the calls to action (CTAs) included in messages sent using pre-registered Sender IDs. Further details can be found in Pivotel's response to the ACMA Sender ID Registry consultation.

Do you support the introduction of a voluntary or mandatory SMS Sender ID Registry for alphanumeric sender IDs? Why?

It is Pivotel's position that a Sender ID Registry can only comprehensively protect against the fraudulent use of sender IDs when it is mandatory. Such a Registry could then function as a whitelist of approved sender IDs for the industry which facilitates the delivery of A2P SMS.

In previous conversations with the ACMA, we have discussed the fact that businesses use a finite number of legitimate sender IDs. By comparison, there is no limit to the permutations of illegitimate sender IDs. Scammers currently exploit legitimate and trust-inducing sender IDs to establish credibility and misappropriate the SMS messaging identities of legitimate organisations.

A voluntary system would necessitate a comprehensive blacklist of all potentially fraudulent sender IDs to also be developed. It is not feasible to maintain a blacklist like this, which is essentially infinite in scale. Furthermore, it would not be realistic to expect such a system to provide sufficient sender ID controls to satisfy the industry, the Regulator and the Australian public.

There will however be concerns about implementing a mandatory Sender ID Registry due to the challenges of scaling it to support the diversity and volume of legitimate A2P SMS traffic.

As part of this consultation, it should be considered that the use of A2P SMS generates significant value and efficiency for organisations, consumers and constituents. A mandatory Registry should seek to avoid any unreasonable expense, complexity or administrative burden on those facilitating and using A2P SMS legitimately.

The initial pilot phase of the Sender ID Registry seeks to rely on 'trusted source' or 'verified route' information to determine the legitimate use of a registered sender ID. Whilst this may be feasible for businesses using simple, single-hop supply chains direct to one of 4 MNOs, Pivotel does not believe that any larger scaling of this model is workable.

A mandatory Registry using this model would need to expand the responsibility of verifying legitimate use of sender IDs to likely hundreds of originating carriage service providers (CSPs), many without an Australian presence. Major complications will quickly arise with organisations using multiple providers to send messages using the same sender ID, and common sender IDs wanting to be used by multiple organisations. This is regular and standard practice in the industry. Transitory CSPs beyond the first 2 hops will need to assume compliance of the CSPs before them, creating ample opportunities for bad actors to introduce scam messages. Should transitory CSPs seek to be included in this verification process, complexity would be increased exponentially.

For a sources-based Registry model to be effective, it would need to index every legitimate route servicing every registered sender ID. To make this mandatory would create a challenge similar to a fraudulent sender ID blacklist, being the number of possible permeations is essentially infinite. This is also before considering the dynamic nature of A2P SMS routing. An attempt to scale such a model to a mandatory system will undoubtedly result in complex, confusing and ultimately unworkable rules. This is more likely to discourage the use of alphanumeric sender IDs entirely, rather than encouraging businesses to control and protect their SMS messaging identities.

A mandatory Sender ID Registry represents an opportunity to establish an environment where consumers can rely on an alphanumeric sender ID as a key trust indicator. Ensuring their use can be simple, while tightly controlled, is vital to fully realising this public safety benefit.

The model should be designed to make participation easily accessible for all organisations, and establish clear and straightforward rules that CSPs at all layers of the A2P SMS supply chain can follow.

What, if any, transition arrangements are required?

Although scam SMS is a substantial issue that requires significant attention and effort to minimise, it should be considered in the broader context that it typically represents less than 0.1% of total A2P SMS traffic (per information available to Pivotel). Disruption efforts should be targeted towards scammers, while minimising any impact to legitimate traffic.

Whilst Pivotel's position is that a mandatory arrangement for the Sender ID Registry is needed, we acknowledge the necessity of a voluntary period to allow for system development, participant engagement, model testing and rule creation. It is encouraging that the ACMA recognises that a phased and cautious approach is required for a successful roll-out of Australia's Sender ID Registry. We agree with the ACMA's current strategy and view the voluntary period as a pragmatic step toward establishing an appropriate end-state model.

Pivotel suggests that the Sender ID Registry model should evolve away from a system requiring the indexing of allowable source or route permeations used by each sender ID. We strongly believe that this will become unmanageable for the Registry and CSPs. The issue of infinite possible source combinations is exacerbated further by the dynamic nature of how A2P SMS is routed. Such a Registry would be attempting to contain a boundless system that is constantly changing. The Registry model needs to leverage fundamentally finite and stable parameters for it to scale to an effective, workable and fit-for-purpose mandatory model.

Pivotel continues to hold the position that the best parameter to support a finite list of legitimate sender IDs is an equally finite list of legitimate calls to action (CTAs) that businesses may include in their A2P SMS messages. This should include URL domains, email domains and telephone numbers.

CTAs are the critical vector by which a scammer directs a potential victim to an environment where fraud can be perpetrated. This could be a fake website, a WhatsApp chat, an email conversation, etc. All scams originating from an SMS require a fraudulent CTA to be presented to a potential victim for the scam to be executed. Removing the ability for an SMS to include a fraudulent CTA instruction dramatically reduces the usefulness of SMS to scammers. This eliminates the primary source of harm that potential victims of SMS scams are exposed to.

Pivotel has created a proof-of-concept to demonstrate this idea, and the importance of understanding the sender IDs that businesses use and any CTAs they might include in their messages.

The PoC, SecureSMS, is being run as a scam-reporting tool. Participants from three major Australian banks, an Australian postal service, a toll provider, and an Australian police force can access real-time data on SMS impersonation scams, which was previously considered unobtainable.

The sender ID and CTA information required from these PoC participants is basic and largely static. This has proved to be immensely powerful when paired with existing scam filtering technologies already in use. Scam messages purporting to be from their organisations are easily detected. Upon request, we can provide more information or a demonstration of our SecureSMS PoC.

Pivotel encourages the ACMA to consider collecting CTA information from organisations seeking to register their sender IDs in the Registry. A Sender ID Registry based on whitelisted sender IDs and CTAs has a clear path towards enabling an effective yet manageable mandatory system. It requires registration of a limited number of basic parameters, which organisations seeking to responsibly use A2P SMS should know and understand.

As a voluntary system, this model would require sender IDs to be linked with CTAs to enable protections. Under a mandatory system however, this would not be necessary.

The end-state solution would contain a whitelist of sender IDs and CTAs. Organisations of all sizes and technical proficiency could easily update this. CSPs can use this information to establish simple allow/block rules in their firewalls. Furthermore, the mechanic could be easily adapted to support numeric sender IDs, which will likely be where scammers quickly migrate once alphanumerics are sufficiently controlled.

Should the Department have further questions, we would be more than happy to assist.

Yours Sincerely

[redacted]

[redacted]

Executive Head of circuit4®,
Pivotel's Business Telecommunication Services Division