Sender ID registry targeted consult – ABA response

Questions

Support

Do you support the introduction of a Sender ID registry? Why/why not?

Yes – we believe a senderID registry could be an extremely useful tool for protecting businesses and consumers from scams.

While the ABA acknowledges that an SMS Sender ID registry will not stop all SMS scams, it will address a frequently exploited weakness in the scams ecosystem. The register will enable telecommunications providers and organisations to better understand what the legitimate traffic of organisations looks like, and in turn more easily identify and disrupt the illegitimate traffic imitating them to commit crimes such as scams.

Recent media by our member National Australia Bank, claim that protections on their voice call Caller ID and SMS Sender IDs resulted in a 50% drop in fraud and 70% reduction in financial losses. NAB takes action to help stop spoofing scams - NAB News.

- **Model**

Do you have views on a potential model? Should a model permit voluntary registration of alphanumeric Sender IDs OR require all such IDs to be registered?

Scammer will always probe for the weakest link in the value chain. Registering all such identifiers will make Australia a harder target for scammers to exploit via this methodology.

The ABA believes that a mandatory model similar to the model implemented in Singapore should be used as a voluntary system will leave weaknesses in the system. It is recommended that a pragmatic approach would be to allow a voluntary phase while the system is being constructed and tested before moving to a mandatory registry.

Singapore started their (latest) registry in March 2022, and as of 31 January 2023, if a Sender ID isn't registered, replaces the Sender ID with "Likely-SCAM", an approach which will surely encourage any organisations that haven't yet registered, to register. After 6 months, all non-registered Sender IDs will have their messages blocked entirely.

Like in Singapore, the senderID registry could commence as a voluntary system, allowing those brands most effected or concerned by message identity to commence the pilot program, however, an important caveat that the ABA believe will be crucial to success is that is mandatory for telcos to comply with the rules of the registry from its conception. As systems are developed and processes refined to support the registry, a timeline should be given to transition to a mandatory system that would allow all parties currently or wishing to legitimately use alphanumeric senderIDs to do so.

Overall, an initial voluntary system will ensure the PoC is up and running to provide risk mitigants within a timely manner before phasing to a mandatory regime.

What minimum information would a registry need to contain to be effective, e.g. alphanumeric Sender IDs and associated brand, brands' providers, technical details etc?

Engagement will need to occur with the telecommunications industry to work through the technical considerations and nuances of fuzzy matching and identification.

In addition to SMS sender IDs, could a registry also allow trusted brands to register phone numbers used to send SMS messages to customers?

The ABA is broadly supportive of allowing trusted brands to register phone numbers, however, we recommend consultation will telcos and large corporates to understand potential technical constraints on the effectiveness of how this is implemented. We understand some businesses may use SMS aggregators for A2P (Application-to-person) messaging, query if this may affect this proposal.
It is suggested to ensure the success and timeliness of the program, there be a phased approach of commencing with senderID before implementing telephone numbers.

If a registry is voluntary, could industry supplement the protections offered by the registry by blocking any SMS using alphanumeric Sender IDs that include a URL in the text body? N/A – ABA supports a mandatory approach
If a voluntary model is adopted, how could SMS scams using alphanumeric Sender IDs that are close, but slightly different to, registered IDs be addressed? Fuzzy matching could be used to identify and disseminate to the relevant member for further analysis.
Delivery
Who should operate and administer a registry? Government, industry or outsourced? Why? The ABA believes it is important that the registry is implemented by the government or regulator, as this entity should have the powers to enforce registry rules.
By what mechanism should registry details be provided to telcos? ABA recommends further technical consultation, including how the mechanism can support automation, security and efficiency of process.
Are there specific security concerns or recommendations that should be considered for a registry? The transfer and storage of the information needs to be secure.
Would you support interim or staged implementation of a registry if it means consumer safeguards are in place sooner? Yes.
Benefits and impacts
What would be the benefits, including financial and social? As noted above, recent media by our member National Australia Bank, claim that protections on their voice call Caller ID and SMS Sender IDs resulted in a 50% drop in fraud and 70% reduction in financial losses. During our Economic Crime Forum and associated workings groups other members continue to seek to implement such protections. [NAB takes action to help stop spoofing scams - NAB News]
What impacts, including costs, may be involved for your organisation? Please provide detail. This program has the potential to minimise the impact of scams and other cyber crime on the payments ecosystem.
Are there potential impediments to consider? Ensuring all telcos comply with the rules of the registry, and ensuring there is legal power to require brands and Government to participate.
Regulatory and cost recovery
Should compliance with the registry be enforceable (by a regulator)? Yes – the scam issue requires all participants in the scam value chain to comply to the same minimum standards. Scammers will move to the next identified weakest link. Note however this is not a silver bullet solution. Industry commentary from jurisdictions where a sender ID registry has been implemented suggest scammers have adopted the use of SIM farms to exploit P2P messaging routes for A2P traffic and avoid the SMS registry protection.
How could a funding model work if a registry operated on a cost neutral basis to govt? Should brands, telcos or both meet any costs? The ABA believes that if a SMS Registry is considered a public benefit, then there should be a review of the governments cost recovery principles and guidelines to consider the case for some public funding.
If a registry is in place, where should consumers complain if they receive SMS scams using registered alphanumeric Sender IDs?

The ABA believes that notifications from both consumers or brands about SMS scams received or impersonating should be ideally provided to the registry operator who would have an efficient process to block, investigate, and take further action. We suggest this could be ACMA or the NASC.

Scam disruption

What has been your/parent company's experience using any O/S model or provider-level registry?

N/A

What strategies do you currently use to combat brand impersonation in SMS? How could a Sender ID registry enhance or complement them?

Many of our members are already working with telecommunications providers to place protections on their voice call Caller ID and SMS Sender IDs and identify suspect communications.

Other

How many different alphanumeric sender IDs do you currently use to send text messages to your customers?

N/A

Are there other matters that may assist the ACMA to provide advice on the implementation of a Sender ID registry in Australia? Please provide detail.

All areas of the scam lifecycle should be consulted and included in the co-design.

Multinationals involved in the UK and the Singapore programs who have operations in Australia could be consulted to provide feedback on the pros and cons of the systems which they have/are involved in.