Scam Taskforce
Market Conduct and Digital Division
The Treasury
Langton Crescent, Parkes ACT 2600

Via e-mail: scamspolicy@treasury.gov.au

5 March 2024

To the Scam Taskforce,

SBS submission – *Scams – Mandatory Industry Codes* consultation paper

The Special Broadcasting Service (**SBS**) appreciates the opportunity to respond to the *Scams – Mandatory Industry Codes* consultation paper (the **Consultation Paper**). Whilst we note the consultation period has passed, SBS wishes to make a submission given the potential impact of the proposals on SBS and its services and audiences.

SBS appreciates the need for well-designed measures to mitigate risks and protect consumers from harms arising from scams. As noted below, scam advertising has impacted SBS's online services and audiences, and we are therefore supportive of appropriate measures being put in place.

However, any regulatory interventions must be appropriate to the circumstances of how these scams are reaching consumers, and the varying levels of control capabilities that industry participants have over the appearance of scams.

This submission will demonstrate that obligations to control scams through online advertising (**ads**) are best applied to demand-side programmatic advertising platforms and, to a similar extent, supply-side programmatic advertising platforms; and that SBS's services should be excluded from the scope of obligations.

Nature of the problem and role of SBS

SBS notes that its online services would appear to fall within the definition of 'media sharing services' (**MSSs**) in the Consultation Paper, which are a subset of 'Digital Communications Platforms'. A range of obligations are then proposed to apply to the Digital Communications Platforms including MSSs, as part of the Scams Code Framework (the **Framework**) set out in the Consultation Paper.

The risk of scams being present on SBS's own online services (websites and apps) arises from malicious online ads that comes through the *open* programmatic supply chain. This is the single most likely way that scam ads would reach SBS audiences, as explored in further detail below.

None of SBS's own online services provide any functionalities for end-users to upload, post, or generate any content or interactive activity with other end-users. In other words, no scams arising from malicious content or activity can be uploaded or generated by end-users of SBS's own online services.

The Framework's future sectors and future sector-specific codes should exclude SBS

We note that the Consultation Paper sets out that future sectors and future sector-specific codes are to be determined by Government. Aside from the specific risk outlined above, other SBS services, while currently not in-scope of the Framework, being SBS's linear broadcast television and radio services, are inherently extremely low risk in relation to scams and should not be subject to further regulation. Robust, effective and long-standing regulatory mechanisms and controls are already in-place for these services.

SBS's broadcast content and programs are professionally produced and subject to an extensive, accessible, transparent and long-standing protective and accountability framework. Any third-party ads on these SBS linear services must also comply with a range of Advertising Codes made by the AANA (Australian Association of National Advertisers) and administered by the advertising regulator, Ad Standards. SBS's television ads must also be classified and reviewed by ClearAds[1], to ensure compliance with relevant advertising rules and regulations.

In addition to this, SBS's Code of Practice (the **SBS Code**, publicly available here), applies across platforms, and is registered with the regulator, the Australian Communications and Media Authority (ACMA). The ACMA has the power to investigate and make findings regarding potential breaches of the SBS Code. Other key control mechanisms include, but are not limited to, SBS's rigorous editorial protocols and checks—applicable to all SBS content, and the SBS Code of Conduct with which all SBS staff must comply.

This submission therefore focuses on scams through online ads—in particular, those through the open programmatic supply chain.

Online scam ads and how they reach SBS audiences

Programmatic demand side platforms (**DSPs**) register and support advertisers to manage their campaigns prior to sending their ads to supply side platforms (**SSPs**) (and eventually to publishers/inventory providers such as SBS). DSPs and SSPs are critical points of control in the supply chain for online ads. It should be emphasised that MSSs (such as SBS), which serve ads to end-users, have relatively limited capability (outside of those made available to us by SSPs) to control or restrict appearance of specific ads, when compared to the capability of DSPs (or SSPs themselves; both of which include large-scale market participants). Therefore, dealing with scams closer to the beginning of the supply chain, utilising the market intermediaries' (DSPs' and SSPs') capability, would be the most effective, and efficient (including in relation to cost) regulatory approach.

There is a significant power imbalance between the publisher/inventory providers such as SBS and the dominant market intermediaries such as Google (which is both a DSP and an SSP). This further emphasises the appropriateness of applying regulatory controls to the larger market participants. For example, SBS's relevant contractual agreement with Google is not open to negotiation and is only available on a 'take it or leave it' basis. SBS therefore has limited ability to influence the extent to which Google verifies or checks the advertisers and their ads.

As a DSP, Google allows advertisers to set up accounts and, through the programmatic supply chain, display their ads on SBS's online services' inventories, without any visibility or prior approval from SBS. There have been instances of scams being displayed on SBS online services through Google's DSP to SSP technology, including scams that intentionally disguised as an SBS content subscription service. This raises the question whether sufficient checks of the advertisers are

[1] https://clearads.com.au/

currently undertaken by Google. As an example, the Framework could include further requirements for DSPs to implement additional and improved checks of the legitimacy of the advertisers and their ads.

In dealing with scams, DSPs (and similarly SSPs) are at comparatively better positions in the supply chain, and have significantly more capability to take preventative steps—in particular, when compared to the (supply chain) position and capability of MSSs including SBS. SBS sits at the end of the supply chain, and the limited measures available to it to deal with scams are comparatively slow, inefficient, costly, and much less effective. This is due to the very nature of programmatic advertising, and not due to any failure on the part of SBS to take appropriate measures including removal and blocking.

SBS utilises a 'category blocking' mechanism, available through SSPs. (For example, this mechanism allows SBS to also choose to prevent sexually explicit ads on its online services.) However, there have been instances when the mechanism does not work properly, and unwanted ads still appear on SBS's online services. SBS therefore, additionally utilises a third-party technology, at its own expense, to further control ads on its services, providing another layer of protection for end-users. This taxpayer-funded expense can be avoided, if appropriate controls are in place at DSPs and SSPs.

In other words, regulatory intervention will be more effective, and efficient if the measures are applied to programmatic DSPs, and to a similar extent the programmatic SSPs.

It is appropriate that regulatory obligations do not apply to SBS and similar services. Adherence to the proposed new obligations would divert resources further away from SBS's principal function of producing public interest content, pursuant to SBS's legislated Charter (for which it received a limited amount of public funding).

Detailed comments regarding the regulatory proposals put forward in the Consultation Paper are set out in this submission's Appendix.

SBS also wishes to state its support of the submission and recommendations put forward by the Interactive Advertising Bureau (IAB) Australia in response to the Consultation Paper.

Should you have any queries, please do not hesitate to contact Holly Brimble (A/g SBS Head of Regulatory and Government Affairs) at holly.brimble@sbs.com.au.

Yours sincerely,

Clare O'Neil
SBS Director of Corporate Affairs

Appendix – SBS's comments in response to the Consultation Paper's proposed possible digital communications platform specific obligations

Proposal in the Consultation Paper	SBS's comments
Prevention	
• A provider of a digital communications platform must implement processes to authenticate and verify the identity and legitimacy of business users and advertisers, to prevent users from selling or advertising scam products and services on the platform.	• When compared to the measures able to be undertaken by DSPs (and similarly, by SSPs), the measures able to be undertaken by MSSs including SBS are relatively slow, inefficient, costly, and much less effective, This is due to the very nature of programmatic advertising, and not due to any failure on the part of SBS to take appropriate measures including removal and blocking. • Adherence to the proposed new obligations would divert resources further away from SBS's principal function of producing public interest content, pursuant to SBS's legislated Charter (for which it received a limited amount of public funding). • These proposed processes will be more swift, effective, and efficient (including in relation to cost) if applied to the open programmatic supply chain participants which sit closer to the sources of scam ads (DSPs, and to a similar extent, SSPs). These are generally large-scale market participants including Google—with very significant in-house capabilities, comprehensive research and development programs, and a vast economy of scale to more effectively implement any additional or enhanced scam-related processes. They also often hold large databases of potential scammers and can thus potentially disrupt scam activities closer to (or sometimes at) the beginning of such activities. Another example of a large-scale market intermediary, as an SSP, is Microsoft—which also possesses very significant in-house capabilities, among other things outlined above. • By the time scams reach SBS, the current rectification actions or processes available include removal, and blocking of the scam advertisers. Whilst SBS takes appropriate steps once it detects or has been alerted to scam ads, these are relatively late processes and there is a risk that harm may have already been caused to end-users/consumers. • The rectification of scams at SBS relies on a series of human interventions including identification of

Proposal in the Consultation Paper	SBS's comments
	the scams (either by SBS staff, its third-party provider, or end-users/consumers), reporting, and rectification actions which include removal and blocking. These steps are relatively slow and inefficient when compared to prevention of scams by DSPs (and to a similar extent, SSPs). The repetitive and manual interventions by SBS staff, and SBS's expense arising from utilising a third-party provider, are also unnecessarily costly to taxpayers.
• A provider of a digital communications platform must have in place processes and methods to detect higher risk interactions, and take appropriate action to warn the user, block or disrupt the interaction, or take other measures to reduce scam activity, content or profiles such as blocking or disabling accounts based on shared intelligence.	• As outlined above, none of SBS's own online services provide any functionalities for end-users to upload, post, or generate any content or interactive activity with other end-users. In other words, no scams arising from malicious content or activity can be uploaded or generated by end-users of SBS's own online services. Therefore, any measures in relation to 'high risk interactions'—as proposed by the Consultation Paper—are not relevant nor applicable to SBS's own online services.
• A provider of a digital communications platform must have in place processes and methods to prevent user accounts from being hacked by scammers, and to restore user accounts to the correct users in a timely manner.	• In relation to protection of user data, including user accounts, SBS takes very seriously and continues to make significant investment in cybersecurity measures, taking into account the relevant laws, industry's best practices and standards. SBS has in place, and regularly updates, its data breach policy and procedures which include reporting of notifiable breaches to the Office of the Information Commissioner (OAIC). It also regularly performs a range of checks of its data security framework, including regular penetration tests—these are in-line with the industry's practice. • SBS also takes very seriously its obligations under the *Privacy Act 1988* (Cth), including the Australian Privacy Principles (APPs), concerning personal information of individuals. Further information is available in SBS's Privacy Policy, here. • Given the extensive regulatory arrangements already applicable to SBS's management of user data, no additional regulatory intervention is needed.
Detection and Disruption	

Proposal in the Consultation Paper	SBS's comments
• A provider of a digital communications platform must have in place methods or processes to identify and share information with other digital communications platform providers and the NASC [National Anti-Scan Centre] that an Australian user is likely to be or is a scammer. • A provider of a digital communications platform must have in place processes to act quickly on information that identifies a user or interaction is likely to be or is a scam, including blocking or disabling the account being used by the scammer.	• As above, these enhanced methods or processes will be more swift, effective, and efficient (including in relation to cost) if implemented by DSPs (and to a similar extent, SSPs).
Response (obligations to consumers)	
• A provider of a digital communications platform must ensure that its platform has user-friendly and accessible methods for consumers to take action where they suspect their accounts are compromised or they have been scammed.	• SBS already has in place, and continues to invest in its robust and industry-leading feedback-handling mechanisms, through which end-users or consumers can report scams present on SBS services. This includes SBS's investment in the industry-leading Zendesk customer service tool, which had been specifically updated in 2022—to ensure the tool appropriately handles online safety matters. • It is relevant to note that 71% of SBS On Demand's technical Zendesk [customer query] tickets, including those about customer accounts, were responded to within only 2hrs.[2] In general, SBS's median full resolution time of queries is at 11 hours and 12 minutes, compared to the industry's 89 hours.[3] • SBS's customer satisfaction regarding its handling of feedback is very high, currently at 85 per cent, compared to the industry's 78 per cent. • Additional regulatory obligations are not warranted.

[2] During Q2 financial year 2023-24**,** source: Zendesk Q2 FY2023-24: (01/010/2023 – 31/12/2023) metrics: Median First Reply Time
[3] During Q2 financial year 2023-24**,** source: Zendesk Q2 FY2023-24: (01/010/2023 – 31/12/2023), All Industry benchmarks are based on global Zendesk data, metrics: Customer Satisfaction and Median Full Resolution Time.

Proposal in the Consultation Paper	SBS's comments
• A business must respond to an information request from the ACMA within the timeframe specified.	• As a regulated Commonwealth entity, SBS already has multiple and transparent reporting obligations. • SBS will continue to work closely with the ACMA in relation to timely responding to any information requests.