Submission by the Interactive Advertising Bureau (IAB) Australia

Scams -

Mandatory Industry Codes

The Treasury

February 2024

Contents

About IAB Australia

The Interactive Advertising Bureau (IAB) Australia Limited www.iabaustralia.com.au is the peak trade association for digital advertising in Australia.

IAB Australia was established in 2005, incorporated in 2010 and is one of 45 IAB offices globally. IAB globally is the leading trade association for developing digital advertising technical standards and best practice.

Locally there is a financial member base of approximately 180 organisations that includes media owners, platforms, media agencies, advertising technology companies as well marketers. The board has representation from the following organisations: Carsales, Domain, Google, Guardian News & Media, Meta, News Corp Australia, Nine, REA Group, Seven West Media, Yahoo.

IAB Australia's charter is to grow sustainable and diverse investment in digital advertising in Australia by supporting the industry in the following ways:

- Advocacy
- Research & resources
- Education and community
- Standards

The Charter includes a focus on standards that promote trust, steps to reduce friction in the ad supply chain; and ultimately improve ad experiences for consumers, advertisers and publishers.

Executive Summary

- IAB thanks the Government for the opportunity to make this submission on behalf of the digital advertising industry.
- The digital advertising ecosystem plays a central role in Australia's economy and society. It is a significant funding component of the internet, enabling the delivery of free online content, products and services to all Australians. It grows businesses, supports 450,000 jobs, contributes $94 billion to GDP and provides $55.5 billion annual consumer benefits.
- The automation of advertising that the online environment has enabled has fundamentally changed the advertising industry in the last 10-15 or so years. The ease, speed and relatively low cost with which advertisers can access audiences has opened a wide range of opportunities for both businesses and consumers. 44% of digital advertising spend comes from the SME segment of the economy, with SMEs receiving 61% of the sector's benefits. These businesses can now reach domestic and international consumers wherever their business is in Australia, and consumers can access a much broader range of products and services as a result.
- IAB Australia and our counterparts globally have been concerned about the risks to both businesses and consumers arising from scam ads for more than a decade. Scams can lead to devastating consequences for consumers, can cause significant damage to legitimate businesses, and undermine the sustainability of the digital advertising ecosystem. These risks have grown as consumers and businesses have moved online and the sophistication and nature of scams continue to evolve.
- Minimising scams in digital advertising is a priority for IAB members. IAB's main efforts in reducing scam activity have been through the creation and coordination of technical standards for the open programmatic ecosystem at an international level (see section 3 for an explanation of the distinction between open and closed environments). These technical standards are a critical step in preventing fraudulent ads being propagated throughout the open web ecosystem. They are continuously evolving in response to developments in technology and changes (or new threats) in the ecosystem. These standards are set out in section 2 and Appendix A. In addition to open-web technical standards, IAB also develops industry best practices, guides and other resources to assist the industry to minimise scam activity.
- Our key concern with the proposed scams framework as set out in the consultation paper is that the definition of 'digital communications platform' is exceptionally broad and captures very diverse businesses. We do not think a detailed set of code obligations could be applied equally to this group of businesses. Within digital advertising platforms, businesses vary significantly in what they do, the technologies they use, and how or the extent to which they interact with other providers in the supply chain. For this reason, obligations under the framework will need to be framed so that they are relevant to the particular platform and within the capability or control of the platform to undertake. What constitutes 'reasonable steps' will be highly dependent on the platform, and may change over time.
- The definition of 'scam' is also broader than the stated intention in the paper. It should unequivocally exclude misleading or deceptive practices and 'unauthorised fraud' that does not involve deception of a consumer into 'authorising' the fraud, and should not capture misuses of personal information dealt with under privacy law. We provide further comments on the framework in section 4.
- Given the complexity of the online advertising ecosystem, any regulation in this area would benefit from close collaboration with industry. We recommend setting up an online advertising taskforce or forum, to enable close engagement with industry on issues of concern pertaining to digital advertising, and to develop a shared understanding and evidence base on such issues.

1. Introduction

1.1 Economic value of digital advertising

The digital advertising ecosystem plays a central role in Australia's economy and society. It funds the delivery of free online content, products and services to all Australians, grows businesses, supports 450,000 jobs and contributes $94 billion to GDP. Over 70% of total advertising is now online.[1]

Digital advertising supports industry sectors including retail, finance, automotive, FMCG, technology and real estate, amongst others. It is an essential enabler of growth across Australia's digital economy. Total Australian digital advertising expenditure has increased from $3.1 billion in 2021 to now $14.2 billion, with the industry posting a growth rate of 2% in 2020, 36% in 2021 and 9% in 2022.[2]

It also sustains and promotes growth of small and medium sized businesses (SMEs) which contributes significantly to the health of the Australian economy. The automation of advertising that the online environment has enabled has fundamentally changed the advertising industry in the last 10-15 or so years. The ease, speed and relatively low cost with which advertisers can access their customers has opened a wide range of opportunities for both businesses and consumers. 44% of digital advertising spend ($5.7n) comes from the SME segment of the economy, with SMEs receive 61% of the sector's benefits.[3] These businesses can now reach domestic, and international, consumers wherever their business is in Australia, much more easily and at a relatively lower access cost, and consumers can access a much broader range of products and services as a result.

1.2 Value of digital advertising to consumers and society

In addition to benefits to the economy, the digital advertising industry provides significant benefits to consumers and Australian society at large.

For Australian consumers, digital advertising has fuelled an expanding online ecosystem of information, news and entertainment content, as well as social and search services, free of charge.

Consumers highly value this. According to analysis commissioned by IAB Australia, the average Australian consumer is willing to pay $544 annually to access currently free ad-supported digital services and content.[4] This equates to provision of a benefit of $8.8 billion to consumers annually in ad-supported digital content and services – and approximately $1100 per household.

The ad-supported online ecosystem also provides significant benefits to society more broadly. It connects communities, supports democracy through free access to news content, provides increased access to job opportunities, education and financial information in addition to entertainment content and supports a thriving second-hand marketplace.

According to a recent consumer survey, 78% of survey respondents indicated that digital content and services enable them to more easily stay in contact with friends and family. This was as high as 81% in regional areas. Importantly, for consumers on annual incomes below $50,000, the value they attribute to content and services that are freely available was roughly double that of consumers with annual incomes of over $80,000.[5]

---

[1] PwC, *Online Advertising Expenditure Report*, 2023. See: https://iabaustralia.com.au/research-and-resources/advertising-expenditure/

[2] Ibid.

[3] PwC, *Ad'ing Value: The impact of digital advertising on the Australian economy and society*, 2022, 4-5.

[4] Ibid.

[5] Ibid.

1.3 Problem of scams in advertising

IAB is concerned that scams are a growing threat to Australian consumers and businesses. The ACCC's Report, '*Targeting scams: report of the ACCC on scams activity 2022*',[6] (the Targeting Scams Report) sets out concerning statistics in relation to scams, including losses of $3.1 billion in 2022 – an 80% increase on total losses recorded in 2021.

IAB supports the goal stated in the Consultation Paper (the Paper), of making Australia a harder target for scam activity and less attractive to scammers, reducing scam losses and impacts.[7] In addition to the substantial harms to consumers, scams also lead to significant business losses and damage the health of the digital advertising ecosystem. For this reason, IAB has already done a significant amount on work developing technical standards for the open programmatic ecosystem, to prevent and disrupt scams, which we set out in section 2.

While the below diagram from the Targeting Scams Report suggests the percentage of scams coming in via paid-for digital advertising compared to other methods is relatively small,[8] from a volume perspective (we assume paid-for digital advertising is a subset of the 6% of scams that the Report attributes to the internet and/or may also be a subset of the 6% attributed to 'social networking/online forums'), the significant recent increase in scams impacting both consumers and businesses is a serious concern.

Having said that, in crafting a scams regulatory framework, it will be important to ensure that obligations are placed appropriately, in accordance with where the problem lies, the role that various participants play, and the level of control they have in relation to a scam ad.

In addition, the framework will need to balance the many benefits that the digital advertising ecosystem, and the technologies that enable it, has given businesses and consumers; with the risks that arise from doing business online.

[6] ACCC, *Targeting scams, Report of the ACCC on scams activity 2022*, April 2023; See: https://www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-reports-on-scams-activity
[7] Consultation Paper, 6.
[8] Targeting Scams Report, 3.

1.4 Approach taken in this submission

This submission focuses on the issues raised in the Consultation Paper from the perspective of paid-for digital advertising. 'Paid-for digital advertising' captures advertising where advertisers pay inventory owners to display their ads to a particular audience. Paid-for advertising comprises both paid-for advertising transmitted via the open-programmatic supply chain (where the technology used is common to all industry participants who choose to use it, and the transmission of an ad may involve multiple platforms collaborating to provide B2B services) as well as paid-for advertising transmitted in closed environments or walled gardens (where platforms own the relationship with the advertiser and end user). While this submission discusses both, the technologies and relationships underlying them differ, which has implications for the application of a regulatory framework. We note that IAB's technical standards have been developed for and apply primarily to the open programmatic supply chain. Closed environments will have their own applicable technology.

The remainder of this submission is set out in 3 parts:

- Section 2 sets out the industry's ongoing efforts to combat scams and ad fraud and provides an overview of IAB's technical standards.
- Section 3 sets out the implications of the proposed scams framework for the digital advertising ecosystem in the context of how the digital advertising ecosystem functions.
- Section 4 provides specific comments on aspects of the proposed framework.

2. Industry efforts to combat scams and ad fraud

The digital advertising industry has been concerned about the risks to both businesses and consumers arising from scams for more than a decade, and has collaborated on a range of global technical standards to reduce vulnerability to fraud and to minimise scams being propagated throughout the open programmatic supply chain throughout this time.

In this section we set out these technical standards that are currently available to participants in the open programmatic ad tech supply and demand chains. They work by reducing scams being transmitted B2B, and as a result also reduce scams being delivered to consumers. They enable the source of the fraud to be identified quickly so that action can be taken by businesses to block the relevant ads.

We note that this section is focussed on collaborative industry efforts in relation to open programmatic advertising, rather than the work individual organisations may have taken in closed environments.

2.1 IAB Tech Lab

IAB Technology Laboratory (Tech Lab) is as a global technical standards body that was established in 2014 for the purpose of developing and managing foundational technologies and standards that enable growth and trust in the digital media ecosystem.[9] . IAB Tech Lab is comprised of engineers, product and technical experts from digital publishers, ad technology firms, agencies, marketers, and other member companies and focuses on industry solutions for brand safety and ad fraud; identity, data, and consumer privacy; ad experiences and measurement; and programmatic effectiveness.

Tech Lab works with local IAB country chapters to develop guidelines, write specs, develop technology and provide services in an effort to develop alignment and standardisation across the industry, and to ensure the industry can seamlessly support the digital economy, including across borders.

IAB Tech Lab also maintains a transparency centre to assist in rapid, cost-effective implementation of IAB standards, and establishes test platforms for companies to evaluate the compatibility of their technology solutions with IAB standards. This is critical for interoperability of IAB technical standards with other technologies in the digital advertising supply chain.

2.2 IAB Technical Standards

IAB Technical standards play a significant role in preventing, detecting and disrupting scams, and making the digital advertising ecosystem safer and more transparent for advertisers and publishers as well as consumers.

IAB Technical Standards are voluntary technical standards, incorporated in a suite of digital files and protocols which enable participants in the open programmatic supply and demand chains to identify who they are transacting with. By doing this, they provide functionality, transparency and aid protection against fraudulent activity, when adopted.

Sell-side Transparency & Anti-Fraud Standards

[9] https://iabaustralia.com.au/guideline/iab-tech-lab-standards-specifications/#:~:text=Established%20in%202014%2C%20the%20IAB,in%20the%20digital%20media%20ecosystem.

The first of the sell-side standards, ads.txt, was introduced in 2017 and there have been various updates, extensions and additions to the sell-side standards since that time (for example, to apply to mobile and apps).

Broadly, the sell-side standards enable advertisers and advertising intermediaries to identify legitimate sellers of inventory and their intermediaries in the programmatic supply chain. They prevent intervention in transactions by fraudulent actors seeking to steal advertiser spend and inventory owner revenue (please refer to Appendix A for an explanation of the mechanics of how they do this), and prevent scam ads reaching consumers.

These standards are effective anti-fraud tools used to prevent:

- Domain spoofing – impersonation of businesses via a fake website or email domain or substitution of a genuine URL with a fraudulent one, for example by using malware.
- Arbitrage - purchasing and reselling of impressions at a higher price.

Prior to ads.txt, bad actors could intervene in transactions, stealing revenue from inventory owners and making ad spend a waste of money for advertisers. If a buyer wanted to find out whether a company was an authorised seller of inventory, it had to contact every inventory owner directly to find out whether a platform was authorised to resell their inventory. Ads.txt automated this process, enabling buyers to simultaneously determine authorised resellers and avoid transactions with unauthorised companies. While they are not infallible in all circumstances, they are widely accepted as significantly reducing the risk of fraudulent transactions.

Buy-side Transparency & Anti-Fraud Standards

The buy-side standards introduced the equivalent of the sell-side standards for the benefit of sellers in mid-2021. They enable inventory owners and their intermediaries to identify legitimate buyers of inventory and their intermediaries in the programmatic demand chain. They also enable quick identification of threat actors when attacks occur. [10]

By making buyers easily traceable and identifiable, they prevent fraudulent ads being propagated throughout the supply chain. This can lead to theft of brand assets such as logos, design elements and other creative. The standard known as 'buyers.json' is designed to prevent bad actors posing as legitimate companies and introducing ransomeware, spyware or bots designed to generate fake ad impressions into the ad tech ecosystem.[11]

Buyers.json enables publishers and SSPs to identify the source of a scam ad, identify who introduced fraudulent creative into the bid system and take appropriate action to protect themselves and their users (eg bad actors can then be blocked).[12] It assists companies in securing their online transactions.

In addition to detection of scams, the buy-side transparency standards can also assist with other functions such as tracing low-quality ads or identifying transaction process inefficiencies.

Adoption rates and industry endorsement

The Tech Lab standards have varying adoption rates which reflect their length of time in market. The original ads.txt standard now has an adoption rate of over 90%.[13] Adoption of the new buy-side standards, launched in April 2021, has not yet been properly assessed however IAB Australia understands the rate of adoption remains relatively low at this stage.

[10] https://iabtechlab.com/security-fraud/
[11] See for example https://iabtechlab.com/press-releases/iab-tech-lab-releases-new-buy-side-transparency-specifications-for-public-comment/ ; https://iabaustralia.com.au/buy-side-trans-standards-update-explainer/
[12] Ibid.
[13] https://digiday.com/marketing/ads-txt-adoption-grows-enforcement/

The process of adoption of these standards by industry is however a global effort and IAB is working with its members and international counterparts to progress this process. Tech Lab, the international network of IABs and IAB Australia all recommend and promote use of all buy-side as well as sell-side standards. IAB Australia has called for the adoption of these transparency standards in a number of public forums,[14] and promoted their adoption to the Australian industry via the *Australian Digital Advertising Practices*,[15] conferences, papers, white papers and educational sessions.[16]

To assist with adoption, IAB Tech Lab publishes extensive implementation guides including examples of how the specifications are relevant to different types of participants in the industry, [17] as well as the Transparency Centre in which publishers and technology vendors can verify the structure of their readable files.[18]

These standards are endorsed across the industry, for example, the recently published results of the second PwC study commissioned by ISBA in the UK encouraged the use of Ads.Txt – which it found had a "measurable impact on limiting unauthorised selling of ad inventory".[19]

We set out each of the buy-side and sell-side standards, as well as other transparency measures developed by industry in Appendix A.

Evolution of industry standards

IAB technical standards are continuously evolving in light of technological developments to support a healthy and sustainable digital media and advertising environment. IAB Tech Lab has 17 different working groups focussed on different aspects of the digital advertising ecosystem. Advancing and producing technical standards to combat ad fraud, supply chain transparency and enhanced security is one of IAB Tech Lab's key and ongoing focus areas across the working groups.[20] Some of the developments in relation to these standards are summarised in Appendix A below. A full list of these technical standards and any recent updates are available on IAB Tech Lab's website.[21]

2.3 Other initiatives and industry best practices

In addition to technical standards, IAB Australia develops industry best practices and resources to assist businesses to address a range of issues, including scams. These include:

- The Australian Digital Advertising Practices (ADAPs) set out a range of best practices for businesses to take to minimise ad fraud.[22] The ADAPs are a cross-industry agreed set of practices, endorsed by the AANA (advertisers), MFA (agencies) and IAB. They are due to be updated in the coming year.
- The digital ad-fraud handbook explores practical issues around ad fraud and sets out a range of best practices and recommendations that have been collaboratively developed by the IAB Australia Standards and Guidelines Council.[23]

---

[14] For example see IAB Media Release, IAB Australia Calls for Digital Industry to Adopt Transparency Standards, July 2020.
[15] For example see: https://iabaustralia.com.au/adaps-2020/
[16] Ibid.
[17] See for example: https://iabtechlab.com/wp-content/uploads/2021/03/Implementation-Guide-buyers-json-demandchain-object.pdf
[18] https://iabtechlab.com/software/transparency-center/
[19] https://www.isba.org.uk/knowledge/second-programmatic-supply-chain-transparency-study
[20] https://iabtechlab.com/standards/#:~:text=IAB%20Tech%20Lab%20produces%20global,our%20work%20related%20to%20identity.
[21] https://iabtechlab.com/standards/
[22] https://iabaustralia.com.au/adaps-2020/
[23] https://iabaustralia.com.au/resource/digital-ad-fraud-handbook/

3. Implications of the proposed scams framework for the digital advertising ecosystem

How inventory is purchased, the nature of the relationship that exists between a platform and the scam advertiser, and the nature of the technology used to transmit an ad between advertiser and consumer, will all impact what steps are most appropriate or feasible for a particular platform or inventory owner to take in relation to a scam ad.

This part of the submission will set out the implications of the proposed scams framework in the context of how the digital advertising ecosystem functions.

3.1 How ads are bought and sold

There are a large range of different digital 'paid for' advertising space formats, which exist across both web and app environments. These include:

- Display advertising – banner advertising in the header, footer or sidebar of a website or app, which may be static, interactive or video.
- Video advertising – displayed before, during or after video content or as standalone video ad content.
- Native advertising – which blends in with digital content (for example, this can ap
- pear as sponsored content).
- Social advertising – advertising on social media platforms.
- Influencer advertising – a form of social media advertising involving endorsements and product placements from people with 'influence' or a large following.
- Search engine marketing – advertising that appears on search engine results pages.
- Connected TV advertising – advertising that is delivered via a streaming service that can reach viewers on that service via multiple platforms (eg TVs, laptops, desktop computers, tablets and mobile devices).
- Digital audio advertising – ads in digital audio content such as podcasts, streamed music and digital radio.
- Digital out-of-home – ads displayed in public space, for example digital billboards.

All of these formats can be used by advertisers or their agencies or representatives to reach audiences as 'paid-for advertising' – which may be transmitted either programmatically or using a platforms' own technology (within a 'closed environment'). When advertisers purchase ad space or inventory, they can choose to transact in a number of ways, including via direct buys, indirect buys using an intermediary, or via self-service options. In addition, they may choose to advertise on platforms that use open RTB protocols ('open programmatic') or platforms that use their own 'closed' technology. Some platforms may use both. Some advertisers may (and often do) advertise a campaign on a number of platforms via various of these options.

These different options involve different ways of transmitting an ad between advertiser and consumer. Some of the key distinctions that are important to bear in mind are set out below.

Direct vs Indirect buys

At a high level, ad space can be sold either:

- **Directly** to an advertiser, via a 'real-world' or 'human' relationship between the inventory owner and advertiser, for example, via a sales team. The advertiser may opt for this if it wants to purchase more specific (for example, premium) inventory.
- **Indirectly** - through an intermediary such as an ad network or DSP, or if the process of selling and buying advertising space occurs exclusively by automated technology, typically using some form of real-time data and/or algorithms within the trading process.[24] The process for indirect sales generally involves the advertiser choosing inventory, placing an order with the inventory owner (or intermediary) on agreed terms and parameters, and the inventory owner then executing the order.

In relation to both direct and indirect deals, ads and inventory are increasingly being exchanged with the aid of automated technology, known in the industry as 'programmatic' technology. However, in the case of direct sales, while programmatic technology may be used, a 'real world' relationship still exists between the advertiser and inventory owner. By contrast, with 'indirect' sales, this is not necessarily the case.

Indirect vs Self-service

In indirect sales, while there is no 'real-world' relationship between the advertiser and inventory owner, there may still be a 'real-world' relationship between the advertiser and an intermediary, for example, an ad network or a DSP, who manages the buying process on behalf of the advertiser (note, a contractual relationship would also exist in the latter case).

Self-service buys however are a subset of indirect buys where there is no 'real-world' relationship with either an inventory owner or an intermediary (although there will be a contractual relationship with one or the other). Self-service buys have become increasingly popular in recent years as they reduce time, cost and friction for the advertiser, and have made the process of advertising a product or service much more accessible. This has been hugely beneficial to small and medium businesses (as outlined in section 1 above), and as a result also to consumers who benefit from more options for goods and services being advertised. However, it has also provided opportunities for malevolent actors to manipulate the technology to commit fraud.

It is also important to note though, as we have previous submitted to Government in the context of the Safe and Responsible AI review,[25] in addition to enabling modern digital advertising practices, and giving rise to risks that the technology can be used to commit fraud, automated technology and machine learning models also provide solutions to this issue. They are critical and commonly used in detecting and preventing ad fraud, and there are constant developments in this technology which industry adopts on an ongoing basis.[26]

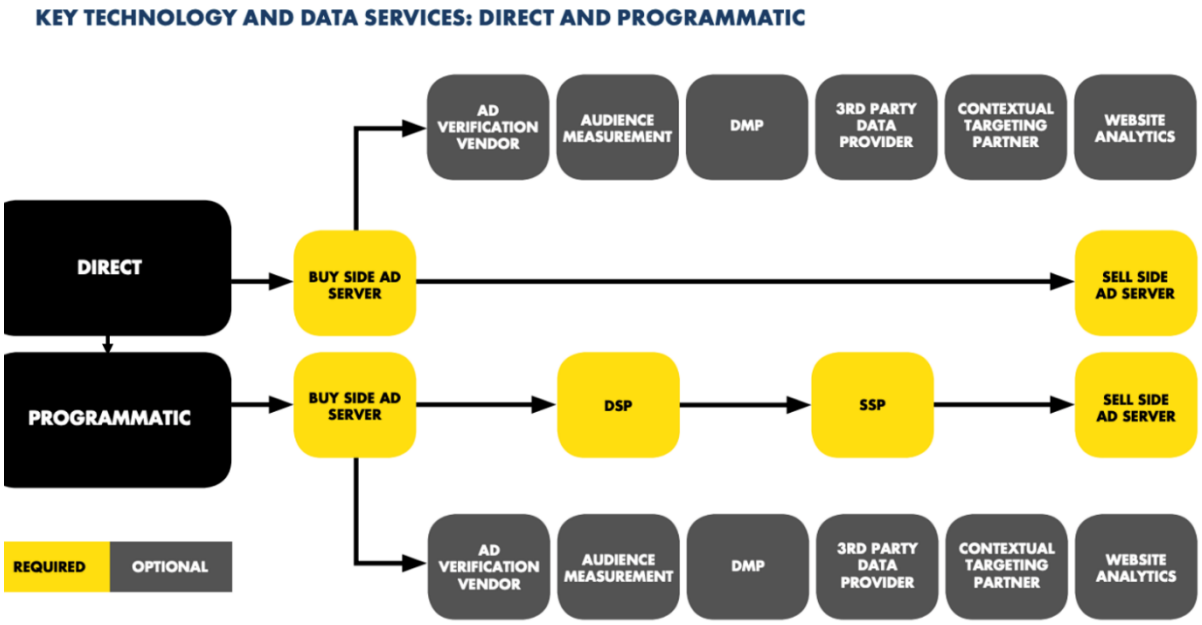
Open vs Closed technology

In addition to different buying and selling options, the distinction between open and closed programmatic technologies is also an important factor when considering what obligations are appropriate or feasible for a particular platform under a scams framework. Programmatic technology can be divided into two main categories:

[24] PwC, *Ad'ing value*, 38.
[25] IAB submission, *Safe and responsible AI*, 2023. See https://iabaustralia.com.au/guideline/iab-australia-submission-safe-and-responsible-ai/
[26] For example using advanced pattern recognition, real-time monitoring, user behaviour analysis, predictive analysis and ad verification and authentication.

- ‘open programmatic’ – uses open RTB protocols, which is a publicly available environment and is accessible to all buyers and sellers.
- ‘closed’ or ‘walled garden’ environment – where a digital platform uses its own technology to automate the digital advertising process.

Platforms may use one or both of these technology options. Whereas in closed environments, platforms own the relationship with both the end user and the advertiser, in open programmatic buying and selling, an ad may pass through several different platforms (independent entities) between the advertiser and the consumer. In this case, the platform where the ad is displayed may not have a direct (or contractual) relationship with either the advertiser or the end user. This has implications for the role they can play in relation to scam ads and therefore also, how any regulation should be framed. Below is a simplified diagram which illustrates this.



**Source, IAB, MFA, AANA, Australian Digital Advertising Practices.*

3.2 Implications for the proposed scams framework

In IAB’s experience, scammers generally do not use ‘real world’ purchasing options, to propagate scam ads. Generally, scammers are more likely to attempt to corrupt the digital advertising ecosystem by attempting to manipulate self-service access points by creating a fake or fraudulent account and/or distributing fake or fraudulent content.

Regardless of whether there is a ‘real-world’ interaction, where there is a direct relationship between an advertiser and a platform (in the sense that there are no intermediaries), the platform is generally in a better position to take steps to verify the advertiser, noting that verification is not fail-safe in that, scammers may still be able to circumvent verification processes, particularly on platforms operating at scale. Generally, however, verification will reduce the likelihood of scams coming into the ecosystem.

Taking steps to verify an advertiser will not however be feasible for all platforms involved in the process of transmitting an ad between an advertiser and a consumer. As illustrated above, in the case of ‘open programmatic’, there may be numerous platforms involved in transmitting an ad between

advertiser and consumer. In that case, the platform that has the most direct relationship with the advertiser will generally be best placed to take steps to verify the advertiser.

However, platforms that act as intermediaries may take other steps, in-line with what is most appropriate in the context of their role in the supply chain and the technology that they use, to minimise risk of scam material passing through their platform. For example, they may adopt IAB Technical Standards (see section 2), other technology solutions, or use fraud detection tools to filter out scam material.[27]

In the case of open programmatic, platforms such as content publishers will not have control over when or where on their platform a specific ad is placed, or to who it is delivered, which will also have implications for removal or take down processes.

In summary, the various ways that ads can be bought and sold has implications for the proposed obligations that attach to the broad category of 'digital communications providers' set out in the Consultation Paper, and what they can feasibly do to detect, disrupt and remove scam ads. Not all obligations will be appropriate for all 'digital communications providers' (See section 4 below).

The proposed framework should recognise that what constitutes 'reasonable steps' by a platform will be highly dependent on the role of the particular platform in the supply chain, and their technological capabilities.

4. Specific comments on proposed framework

While we support the introduction of a scams legislative framework in-principle, including obligations on digital platforms where appropriate, we have some concerns in relation to the framework as described in the Consultation Paper (in addition to our concerns outlined above), that we set out in this section.

4.1 Oversight and multi-regulator model

The Consultation Paper proposes that the framework would include an overarching regime in primary law, such as the *Competition and Consumer Act 2010*, which would set mandatory obligations to take action to address scams, as well as sector-specific mandatory codes, containing additional, tailored obligations on businesses to prevent, detect, disrupt and respond to scams.[28]

While we are not opposed to the approach in principle, we would note that the list of obligations proposed to be included in the overarching framework is extensive (and some seem to be framed as obligations rather than broad principles),[29] and they seem to overlap with the list of obligations proposed to be included in the sector specific code(s) for digital communications platforms.[30] For example, the reporting obligations read very similarly under both he ecosystem-wide principes and the platform specific obligations, and the record keeping obligation in the ecosystem-wide principles reads as an obligation rather than a principle.

In our view, if this two-tiered framework is pursued, greater clarity will be needed in relation to both the overarching expectations/principles, as well as how these apply to specific digital communications platforms' services. Duplicating similar obligations in both tiers would risk inconsistent interpretations

[27] https://iabaustralia.com.au/resource/digital-ad-fraud-handbook/
[28] Consultation Paper, 8.
[29] Consultation Paper, 12
[30] Consultation Paper, 21.

of the obligations by regulators and courts and would lead to confusion amongst businesses and consumers.

4.2 Definition of Digital Communications Platform

As outlined above, one of our key concerns is the scope of platforms that obligations will be attached to under the definition of 'digital communications platform'. In our view, consideration should be given to narrowing the definition and tailoring the obligations under the framework so that they are relevant to the particular platform and within the capability or control of the platform to undertake.

A risk with the current approach is that 'digital communications platforms' as defined in the Consultation Paper, are a very diverse set of businesses. We are not convinced that a prescriptive set of code obligations could be applied equally to this group of businesses. In our view, there will likely be a trade-off between breadth of scope of the framework and the specificity of the obligations under it.

From an advertising perspective, as noted above, when a scam enters the digital advertising ecosystem, there may be different paths that an ad may take between the advertiser and the inventory owner. In the case of open programmatic advertising, there may be several platforms involved (eg the ad may pass through from advertiser to DSP to buy-side ad server to sell-side ad server to SSP to inventory owner). In the case of a walled garden environment, the path between advertiser and inventory owner is generally less complex because they own the relationship end-to-end, which may result in greater ease of compliance with certain of the proposed regulatory obligations.

In both cases, scams enter the system at the point where the ad is uploaded/ingested into the system. However, what steps are appropriate or 'reasonable' for a platform to take in response may differ according to the nature of the platform. In the case of a platform in the open programmatic supply chain, different platforms in the chain have different roles. For example, those that do not have a direct relationship with the advertiser would rely on the platform that does, to take reasonable steps in relation to vetting or verification. However, platforms throughout the chain may take measures, adopt technologies or protocols, or have processes in place to detect and limit scams and/or communicate with other platforms in the supply chain where they become aware of a scam, in accordance with industry best practices.

Any proposed framework should take this into account and not impose obligations that are not appropriate or relevant in the circumstances. For example, the proposed obligation on digital communications platforms to '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',[31] would not be an appropriate obligation for a platform that did not have a direct relationship with an advertiser/user.

Similarly, 'user-friendly and accessible methods for consumers to take action where they suspect their accounts are compromised or they have been scammed' – will not be equally relevant for all digital communications platforms. Where they are relevant, what is an appropriate method may differ depending on the type of platform (for example, for some it may be pointing consumers to another platform or the NASC, rather than an internal complaints mechanism).

[31] Consultation Paper, 21.

Similarly, the requirement to maintain an anti-scam strategy and train staff on how to respond to scams should not be disproportionately burdensome, in circumstances where the risks associated with scams are particularly low.

For these reasons, we do not think it is feasible to apply the extensive obligations set out in the Consultation Paper, let alone more detailed obligations in a mandatory code, equally to the broad range of digital communications platforms that would likely fall under the definition set out in the Paper.

4.3 Definition of scam

The Consultation Paper provides that the definition of 'scam' is:

> '*a dishonest invitation, request, notification or offer, designed to obtain personal information or a financial benefit by deceptive means*.'

We are concerned that this definition is broader than the intention as set out in the Consultation Paper. For example, the paper implies that the definition is intended to be limited to scams where the consumer is involved or duped into authorising the fraud (excluding data breaches, hacking, etc), however this may need to be made clearer in the proposed definition which; a) does not refer to 'a consumer', and b) includes 'notifications'.. 'designed to obtain a financial benefit by deceptive means', which may not clearly distinguish unauthorised fraud.

The paper also provides that the definition is "not intended to include consumer disputes about misleading and deceptive practices relating to the sale of goods and services, other than where a seller profile or website is not legitimate."[32] We agree that it should not cover misleading and deceptive practices, which are covered under the ACL, however, we are not convinced that these are unequivocally excluded from the proposed definition.

In addition, including 'personal information' in the definition risks conflating scams with privacy law breaches. Appropriate regulatory reforms in relation to misuses of personal information are currently being considered under the Privacy Act review and should not be captured here.

We note the paper provides that the definition is 'intended to capture the types of scams identified by the ACCC under its Targeting Scams Report, including but not limited to, common scam types such as investment scams, romance scams, phishing scams, employment scams, and remote access scams". We seek further clarification in relation to the extent of the scams that are intended to be covered. For example, we assume that 'invalid traffic', from sources such as bots, spiders, and other automated programs, would not be captured.[33]

4.4 Reporting obligations

The Consultation Paper provides that:

> *'a business would be required to have a reporting mechanism in place for users to report scams, including in cases where they have identified but not been affected by a scam'…p 15*

As noted above, the type of reporting mechanism that is appropriate in the circumstances will differ depending on the nature of the platform. In some cases, pointing consumers to the NASC may be the most appropriate course of action.

---

[32] Consultation Paper, 10.

[33] IAB Australia, *Digital Ad Fraud Handbook*, June 2023. See https://iabaustralia.com.au/resource/digital-ad-fraud-handbook/

The CP also provides that "*a business would also be required to take reasonable steps to act on scam intelligence shared with it by another business, industry bodies, law enforcement and regulators, including the NASC. This would include acting on intelligence to stop a current scam, prevent further scams from the same source occurring, or to otherwise address the consequences of a scam."* It provides that reasonable steps would include "*warning consumers or users that have also interacted with an identified scam or scammer and providing them with information or advice on actions to take if they have also been affected by a scam*."

While we do not disagree in principle, there may be reasons why a business does not act on a particular scam report, for example, if the veracity of the report cannot be confirmed, or where it cannot be confirmed within a certain timeframe. We seek confirmation that what constitutes 'reasonable steps' would take these matters into account in any proposed code obligations. That is, it may be reasonable in some circumstances, based on the best information available to a digital platform, not to take further steps in relation to a particular ad or advertiser.

We would also note that, to avoid duplication and the NASC being inundated with notifications about the same scams, it may be more efficient for the obligation to report a scam to the NASC to sit with the most relevant organisation (for example, it may not make sense to for an organisation to report the same scam that they have been made aware of by another platform that has already reported the scam, in the absence of any new information).

Again, in our view, the requirements in relation to reporting should not be disproportionately burdensome, in circumstances where the risks associated with scams are particularly low.

4.5 Jurisdictional limitations

Clarification is needed in relation to the application of these obligations to circumstances where there is a connection with Australia, for example, the scam originates in Australia or impacts consumers in Australia. Some platforms may become aware of scams that have no connection with Australia and we assume that these would not be required to be reported.

4.6 Interaction with privacy laws

Clarification is needed that any information sharing requirements under the proposed framework with other businesses or with the NASC would either fall within a 'permitted general situation',[34] or otherwise not breach existing privacy laws.

5. Recommendation

5.1 Lessons from other jurisdictions - closer collaboration with industry

In our view, the complexity of the online advertising ecosystem requires any regulation to be developed in close collaboration with industry. As is perhaps highlighted by this submission, digital advertising is incredibly complex, the businesses involved are incredibly diverse, and the different technologies and purchase paths used (for example open vs closed environments) vary. This has implications for any regulatory framework that is intended to be applied to 'digital advertising' as a whole.

In our view, it would be worthwhile to set up an Online Advertising Taskforce, similar to the one that has been set up in the UK,[35] to enable close engagement with affected stakeholders on issues of

[34] Privacy Act 1988, 16A.
[35] Online Advertising Programme - GOV.UK (www.gov.uk)

concern pertaining to digital advertising as they arise. This would enable Government and industry to work closely together and to develop a shared understanding and evidence base on such issues, to find the best solutions to tackle them, and which could ultimately inform any proposed legislative as well as non-legislative action. The issue of ad fraud could be first on the list for consideration, but others could be considered as relevant.

6. Conclusion

IAB Australia thanks the Treasury for the opportunity to make this submission.

Scams can lead to devastating consequences for consumers, can cause significant damage to legitimate businesses, and undermine the sustainability of the digital advertising ecosystem as a whole. Minimising scams in digital advertising is a priority for IAB members.

We look forward to working with the Government to ensure that the regulatory framework appropriately addresses these issues.

APPENDIX A – TECH LAB STANDARDS

Authorised Digital Sellers Standard (Ads.txt)	Ads.txt is a digital text file added by publishers to their web server in the root domain. The file contains information including the publisher's ID as well as a list of authorised intermediaries/sellers and resellers that are permitted to sell inventory on their behalf. This list can be accessed publicly by going to companyname.com/ads.txt, or advertisers can use the IAB crawler to check if publishers use ads.txt. Ads.txt enables companies to quickly identify authorised resellers (SSPs). Prior to Ads.txt, buyers had to contact every publisher directly to find out whether a platform was authorised to resell inventory for a particular company. Ads.txt enables buyers to simultaneously determine this and avoid transaction with unauthorised SSPs/companies, via the automated processes in a programmatic transaction. Since its first release, there have been a number of updates and improvements to this IAB standard. For example, the original ads.txt standard did not address mobile ad fraud, however this was addressed by an update in 2018, and then a further update enabled it to be extended to apps as well (app-ads.txt).
Sellers.json	Sellers.json is an extension to ads.txt introduced by IAB Tech Lab in 2019 that provides additional transparency through the supply chain. It is also a publicly available file, but is hosted by advertising intermediaries - sell-side platforms (SSPs) and ad exchanges and contains information about all legal entities that the intermediary cooperates with and identifies whether a listed company is a direct seller or an authorised intermediary. It also includes details such as publishers' or intermediaries' domain names and seller IDs.
SupplyChain object	The SupplyChain Object (or schain) is a protocol within OpenRTB that removes anonymity across the supply chain for a particular bid. It works together with ads.txt, app-ads.txt and sellers.json to enable buyers to see all parties who were paid for ad inventory in response to a bid request. It does this using information such as the URL of the seller and the publisher ID. Technically, it does this by mapping participants involved in the sale of a transaction across a chain of nodes that represent each seller. If SupplyChain Object tool is included in a bid request by the advertiser or intermediary on the buy-side, then it provides information about every entity involved in a particular bid-request between advertiser and publisher (not just the direct partners).
Buyers.json	Buyers.json is the equivalent of sellers.json on the buy-side. That is, it provides transparency into the identities of advertisers and buy-side platforms. As with Sellers.json, buyers.json is a publicly available file, hosted by and accessible via the root domains of DSPs. The file contains a list of advertisers and intermediaries it represents. As with sellers.json, it identifies whether a listed company is a direct buyer (advertiser) or other authorised intermediary. It also includes details such as advertisers' or intermediaries' domain names and buyer IDs. In this way it enables sellers to identify who is buying their inventory. Buyers.json enables publishers and SSPs to identify the source of malvertising attacks, identify who introduced a bad creative into the bid system and take appropriate action to protect themselves and their users (eg bad actors can then be blocked).[36]

36

	In addition to malvertising, buyers.json & demandchain object can also assist with tracing and blocking low-quality ads.
DemandChain Object	Demand Chain Object, similar to SupplyChain Object, is an openRTB protocol that removes anonymity across the demand chain for a particular bid. While SupplyChain Object provides this function for advertisers and their intermediaries, DemandChain object provides the equivalent function for publishers and their intermediaries. It works together with buyers.json to enable publishers and sell-side platforms to see all parties in the payment chain for a particular bid for delivery. As with the supplychain object, it specifies every intermediary between the advertiser and the publisher where the impression is served (programmatically). Technically, as with SupplyChain Object it does this by mapping participants involved in a transaction across a set of nodes which each represent a specific entity that participates in the direct flow of payment for an impression and the creative associated with it. Tech Lab is also expected to develop future versions which will include entities who are involved in the transaction but are not involved in payment. If the DemandChain Object tool is included in a bid request by the seller in their SSP, then it provides information about every entity involved in a particular bid-request between advertiser and publisher (not just the direct partners).
Ads Cert 2.0	IAB Tech Lab's Cryptographic Security Foundations Working Group has recently upgraded the ads.cert framework to enable full authentication through cryptography of the user, the device, the publisher, any ad tech intermediaries, and the buyer so as to fully guarantee the integrity of a transaction. These standards are initially focused on SSAI (Server-Side Ad Insertion) transactions for connected TV ads specifically, as recent security research has highlighted schemes where parties have attempted to impersonate SSAI platforms. These schemes are challenging to identify, as traffic appears to originate from the same cloud platforms and hosting providers that service genuine SSAI businesses.
Other Existing Transparency Measures	Call Signs protocol – allows a company to accurately identify other companies involved in a specific ad transaction, thanks to Domain Name System records. Authenticated Connections protocol – gives both advertisers and publishers confidence in the authenticity of the origin of any requests, thereby preventing interference in server-to-server requests. Authenticated Delivery protocol – authenticates the data in a given bid request, allowing buyers and sellers to see if the price or location of a given bid has been tampered with. Authenticated Devices protocol – attests to the legitimacy of the device on which a given ad is being served. IAB Tech Lab has specifically recommended that all SSAI providers immediately implement the Authenticated Connections protocol in particular – and advises both buyers and sellers to start insisting upon this protocol for any CTV transactions as soon as it becomes available to them. For the full set of specifications for ads.cert 2.0 simply click here - https://iabtechlab.com/ads-cert/
Data Label	The IAB Tech Lab Data Transparency standard establishes minimum disclosure requirements for audience data providers. It is intended for: • Providers that collect, segment, and market data as a standalone product

	• Providers that collect, segment, and market data as a coupled / bundled offering along with media • Data marketplaces that broker data between buyers and sellers and represent the "point of purchase" These disclosure requirements are intended to establish a baseline level of transparency for data buyers about aspects of data collection, processing, and modelling that inform data quality and applicability, regardless of buyer use case. These standards are not intended to provide a qualitative grade as to the efficacy ("this segment performs well") or quality ("this segment is highly accurate) of the data in question, but simply surface baseline information that buyers can use to make informed decisions regardless of their data use case. The initiative provides a simple, consistent and easily digested set of standards – allowing sellers to clearly specify where the data comes from, how it was collected and organised, its recency, if it was manipulated or modelled and what rules were used in establishing the data within any particular audience segments. We see the benefits of the Data Label being: • Help educate the industry around what is contained within audience data segments, how they have been constructed, how they are being updated and the recency. • Provide consistency and transparency in terms of the product constituents and naming conventions. • Enable a minimum level of quality assurance in terms of what is being bought and/or utilised. A beta version of the marketplace API is now available managed by IAB Tech Lab to enable easier uploading, maintenance and reporting capabilities – as well as integrations across participating data marketplaces. IAB Australia recommends that publishers and data suppliers start utilising the Data Label for their most traded segments as a commitment to the highest standard of audience data transparency. In turn, buyers and agencies should start recognising those segments for their consistent and transparent approach and increasingly demanding their usage in any future ongoing transactions. Related to these standards is the IAB Tech Lab's compliance program – which is available to any organisation that offers data, whether syndicated separately or bundled alongside with media, and is also open to adoption by data marketplaces where data is bought and sold. Those organisations that complete the compliance program affirm their full commitment to the highest standards of audience data transparency.