To: Tony Robinson, Director
Scams Taskforce
Market Conduct and Digital Division
The Treasury
Langton Crescent, PARKES ACT 2600
By email: scamspolicy@treasury.gov.au; tony.robinson@treasury.gov.au

Monday January 29, 2024

Dear Mr. Robinson,

The Digital Industry Group Inc. (DIGI) wishes to thank you for the opportunity to provide input on the *Scams – Mandatory Industry Codes Consultation Paper*, released in November 2023 (the Consultation Paper).

As you would be aware, DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia. DIGI's founding members are Apple, Discord, eBay, Google, Linktree, Meta, Microsoft, Snap, Spotify, TikTok, Twitch, X (f.k.a Twitter) and Yahoo. DIGI's vision is a thriving Australian digitally-enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected.

DIGI works to promote Australians' online privacy, safety and security, which helps to protect against a range of harms, including scams and fraud. That work includes developing industry codes of practice for the digital industry. DIGI co-led the development of mandatory codes required under the Online Safety Act, and both developed and oversees *The Australian Code of Practice on Disinformation and Misinformation* (ACPDM).

DIGI has long supported the establishment of the National Anti-Scams Centre (NASC) and is proud to be represented on its Advisory Board, and its Data Integration and Technology Working Group. We are supportive of the 'ecosystem' approach the NASC takes to foster close collaboration between industry and government. As scams can span multiple services, regulatory approaches should be holistic in involving a range of relevant industries across the private sector as well as consumer bodies, regulators and law enforcement.

DIGI's relevant members have longstanding, multi-pronged anti-scam efforts that include enforced restrictions to rapidly combat scams. This could include through proactive detection, in-product reporting and customer service, as well as digital literacy efforts to reduce Australians' susceptibility to scams. They also invest significantly in cyber security that protects consumers against a range of harms, including scams. Their restrictions on scams also include spam, fraud and other deceptive conduct – including phishing, impersonation and misrepresentation – on organic content as well as paid content and advertising. Many of them work closely with other companies and governments, including with the ACCC's Scamwatch program and the National Anti-Scam Centre, to both identify and act on trends in scams and criminal behaviour. We have used ***Section 6*** of this submission to provide an overview of some of this work.

DIGI shares the Government's goal in seeking to lift the bar to ensure robust and effective approaches to scams in relevant industries. DIGI agrees with the Government that industry codes, if well drafted, have the potential to create greater accountability around this work. However, obligations should be proportionate, consistent with other laws and appropriate for different services. The specific approach to sector-specific code development (i.e. voluntary vs. mandatory, industry-drafted vs. regulator drafted) is extremely important in determining whether this goal can be met effectively. As we outline in ***Section 5***, drawing on DIGI's first-hand experience in developing both

mandatory and voluntary codes for the digital industry, we see strong consumer benefit from an industry-led approach.

Crystal clear obligations for industry, along with clear responsibilities for regulators, mean better outcomes for consumers. DIGI believes that systemic improvements to the proposed regulatory regime need to be made in multiple areas to ensure that clarity. This includes refining: 1) the definition of what constitutes a 'scam' under this proposed regulatory regime (**see *Section 1***); 2) the sectors to which the regime applies, in order to ensure a targeted and proportionate approach (**see *Section 2***); 3) the duplication of obligations in the proposed overarching framework within the Competition and Consumer Act (CCA) (**See *Section 3***) and 4) the sector-specific obligations to improve attainability (**See *Section 4***). With regard to 1, 2 and 4, **we believe that an industry-led approach to code development, with close collaboration with the ACMA, will significantly improve industry's ability to set anti-scam measures that serve Australian consumers**.

While our submission is focused on the areas outlined above, we also have questions about the premise of the reform approach that considers digital platforms, including social media services, as an equal vector as the banking and telecommunications sector in relation to scams. For example, the ACCC's report 'Targeting Scams: Report of the ACCC on scams activity 2022' found that phone calls and SMS text messages were the top contact methods employed by scammers, accounting for 62% of reported scams, with 'internet' accounting for 6%, social networking accounting for 6%, and email accounting for 22%[1]. Scammers adjust their tactics to circumvent security measures, and can shift between different modes of communication. While contact methods may change over the course of a scam's lifecycle, scam losses *always* occur through banks or the exchange of cryptocurrency which means that anti-scam interventions within the banking industry are likely to be of greatest benefit to consumers. **DIGI encourages a further evidence base in making determinations about the service-level, and sub-sectoral, scam interventions that will have maximal consumer benefit for Australians.**

We thank you again for the opportunity to contribute our views to the Consultation Paper, and related engagements with your team. We hope that the information enclosed is useful to you as you further consider the approach to these complex issues. I encourage you to continue to draw upon DIGI as a resource as this reform process continues, and please do not hesitate to contact me should you have any questions about this submission.

Best regards,

Sunita Bose
Managing Director, DIGI
sunita@digi.org.au

Table of contents

[1] ACCC, T*argeting scams: report of the ACCC on scams activity 2022*, (April 2023), Summary infographic: https://www.accc.gov.au/sites/www.accc.gov.au/files/2023-04/23-18GRH_Targeting%20scams%20Media%20infographic_D01_0.jpg

Section 1: Scope of scams definition

1. Clarifying the definition of scams

1.1. If the aim of this reform process is to 'lift the bar' in counter-scam measures across designated sectors, then those sectors must be provided with clear obligations that they can operationalise. A precise and appropriate definition for what is, and is not, a 'scam' is the foundation for this clarity.

1.2. DIGI is concerned that the current definition, as set out below, does not provide this clarity, and is therefore overbroad and unworkable:

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

1.3. The Consultation Paper indicates that the definition is modelled on the definition of fraud as defined under the Commonwealth Fraud Control Policy (CFCP)[2], as set out below. While any definition would require a process of workshopping with relevant industries, we consider the CFCP definition to be a more effective and implementable starting point.

'fraud is defined as 'dishonestly obtaining a benefit or causing a loss by deception or other means'.'

1.4. That is because there are additional elements in the Consultation Paper's definition, beyond the CFCP definition, that make it extremely difficult for the digital industry to implement, without considerable overcorrection. These elements are set out below.

'obtain personal information'

1.5. DIGI assumes that proposed definition's inclusion of 'personal information' refers to to the Privacy Act, where personal information is defined as:

[2]Attorney General's Department (2017), *Commonwealth Fraud Control Framework*, https://www.ag.gov.au/sites/default/files/2020-03/CommonwealthFraudControlFramework2017.PDF

The Privacy Act defines 'personal information' as:
'Information or an opinion about an identified individual, or an individual who is reasonably identifiable:
a) whether the information or opinion is true or not; and
b) whether the information or opinion is recorded in a material form or not.'[3]

1.6. Including personal information lowers the bar in the definition of a scam such that it could technically cover a message that says 'Hi I'm Jim, what's your name?', where Jim is not the sender's name, rendering this dishonest, and because a name is personal information, and the request could be considered an invitation. This example is also used to underscore that not all personal information can be used to perpetrate a successful scam. For example, a name or email address or phone number alone are unlikely to enable the obtainment of benefit or causing of loss, unless further information is provided to, or obtained by, the scammer.

1.7. Furthermore, we note that the definition of 'personal Information' is in flux, due to the ongoing reform process of the Privacy Act. The Government's response to the Privacy Act Review indicates its intention to include clarifications that personal information is an expansive concept that includes technical and inferred information (such as IP addresses and device identifiers) if this information can be used to identify individuals[4]. DIGI has not seen evidence to suggest that technical or inferred information, along with many other categories of personal information, could directly assist the perpetrator of a scam in causing a financial loss.

1.8. The obtainment of personal information might certainly be the *means* by which a loss or benefit is obtained, but it should not be considered the scam itself. The actual financial loss is of greater consequence to consumers than the initial communication. By conflating these two issues, the Government also conflates data breaches with scams, confusing obligations under this scheme with those under the Notifiable Breaches Scheme.[5] DIGI recommends the removal of 'personal information' from the definition of a scam, and a greater focus on the obtainment of financial benefit.

'invitation, request, notification or offer'

1.9. The Fraud Control Policy definition focuses on the *obtainment*, rather than an invitation, request or notification to *obtain*. Therefore, it does not appear to include unsuccessful requests where the person exposed to the scam does not engage, whereas the Consultation Paper proposed definition does include this scenario.

'designed to'

1.10. Similarly, it is unclear why 'design' is included as an element here, and whether this is intended to bring the concept of 'dark patterns' into a statute; industry should not be required to make determinations based on estimations of intent.

---

[3]OAIC (2017), *What is personal information?*, https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/what-is-personal-information#:~:text=The%20Privacy%20Act%20defines%20'personal,a%20material%20form%20or%20not.
[4]Attorney-General's Department (28/09/2023), Government response to the Privacy Act Review Report, https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF, p.5
[5]OAIC, *Notifiable data breaches*, https://www.oaic.gov.au/privacy/notifiable-data-breaches

1.11. Aligning upon a definition of a scam will require further workshopping with a wide range of sectors, including the digital industry. Further consideration will also need to be given to whether the scope covers business-to-business (B2B), as well as business-to-consumer (B2C) scams. In this context, we note that in recent consumer protection reforms relating to unfair contract terms, 'consumer' includes SMEs up to 100 employees. DIGI would be happy to facilitate the participation of our members in such a workshop to further aid clarity in this area.

2. Sector-specific definitions

2.1. In this workshopping, consideration might also be given to whether sector-specific definitions are more effective than overarching definitions, for the purposes of enforcement, similar to the approach taken in the *Reducing Scam Calls and Scam Short Messages (SMs) Code* for the telecommunications sector (the Telecommunications Code), developed by Communications Alliance.

2.2. In the Telecommunications Code, scam calls are characterised by high volume from a particular 'Calling Line Identification', and scams SMS are often characterised by a high volume of messages to a large number of B-Parties (i.e. potential victims/recipients).[6] In a similar vein, we consider it important for any code in the digital platforms sector to be premised on a definition of in which a scam is systemic and where there is a threshold of volume. This will focus industry action where there is the highest impact on Australian consumers.

2.3. Additionally, having definitions sit within the sector-specific obligations, rather than any overarching regulatory framework, enables the definitions to more nimbly evolve as scammers' methods and tactics evolve. This way, changes to the definitions would not require the passage of amendments to legislation through parliament, but rather could be advanced within industry-led code review processes.

3. Broader regulatory take-down powers

3.1. Once a definition of 'scam' is aligned upon, DIGI urges the Government to provide the ACCC with takedown powers on relevant services of known scams. We consider that this would complement and provide a natural progression to the victim engagement work that the NASC is already undertaking.

3.2. As well as directly serving Australian consumers, this would provide industry with necessary clarity in relation to their sector-specific scams obligations. The absence of such definitional clarity and takedown powers may put industry in an uncertain position in relation to its obligations. This would be a contrast to the Class 1 codes under *the Online Safety Act 2021* where the Office of the eSafety Commissioner has related takedown powers over all Class 1 content. At face value, scams can often resemble legitimate direct conversations, and a wider purview is necessary for service providers to conclusively determine if it is a scam. eSafety takedown requests therefore provide a useful complement to platforms' own work, because they can bring additional real-life context.

3.3. DIGI understands that the Australian Securities and Investments Commission (ASIC) has takedown powers in relation to investment scam websites, but that other scam websites currently pose a regulatory gap. We also understand that the ASIC scheme has been effective in removing approximately 20 investment scam and phishing

[6] Communications Alliance Ltd, *Industry Code C661:2022Reducing Scam Calls And Scam SMs*, https://www.commsalliance.com.au/__data/assets/pdf_file/0015/72150/C661_2022.pdf

websites a day, and has been bolstered by its close collaboration with the fusion cells of the NASC, through which several of our members participate.[7]

3.4. We note that there would need to be appropriate safeguards on ACCC takedown powers; for example, these might be limited to specified URLs, with an appeals mechanism for owners of content that is removed. Empowering the ACCC with the power to remove known scams from digital and other services is a crucial piece of the puzzle in achieving the NASC's overarching strategy to make Australia a harder target for scammers.

Summary of recommendations in Section 1

A. DIGI encourages a further evidence base in making determinations about the service-level scam interventions that will have maximal consumer benefit for Australians.

B. Aligning upon a definition of a scam requires further workshopping with a wide range of sectors, including the digital industry. DIGI would be happy to facilitate the participation of our members in such a workshop to further aid clarity in this area.

C. Noting Recommendation 1B (i.e. Section 1, Recommendation B), we consider the Commonwealth Fraud Control Policy definition to be a more effective and implementable starting point than the scam definition advanced in the Consultation Paper.

D. DIGI recommends the removal of 'personal information' from the definition of a scam.

E. The definition should focus on the *obtainment* of financial benefit, rather than an invitation, request or notification to obtain, nor any associated design.

F. Consideration might also be given to whether sector-specific definitions are more effective than overarching definitions, for the purposes of enforcement.

G. Similar to the Telecommunications Code in force, any code in the digital platforms sector should be premised on a definition of scam which is systemic and where there is a threshold of volume, in order to focus industry action where there is the highest impact on Australian consumers.

H. DIGI urges the Government to provide the ACCC with takedown powers on relevant services of known scams. As well as directly serving Australian consumers, this would provide industry with necessary clarity in relation to their sector-specific scams obligations.

[7] The Hon Stephen Jones MP (2/11/2023), *Media release: Thousands of scam investment websites removed in takedown blitz*, https://ministers.treasury.gov.au/ministers/stephen-jones-2022/media-releases/thousands-scam-investment-websites-removed-takedown

Section 2: Scope of services covered

4. Breadth of definitions

4.1. Prior to the Consultation Paper's release, Minister Stephen Jones' announcements and commentary on this proposed code have consistently described this code as relating to social media services[8]. However, we understand that the proposed overarching regulation, and sector-specific obligations are intended to apply not just to social media services, as was originally announced by Minister Jones, but to a far broader array of 'digital communications platforms', described in the Consultation Paper as:

'content aggregation services – online services whose primary function is to collate and present content to end-users from a range of online sources

connective media services – online services whose primary function is to enable interaction between two or more end-users.

media sharing services – online services whose primary function is to provide audio, audio-visual or moving visual content, including advertising content, to end-users.'

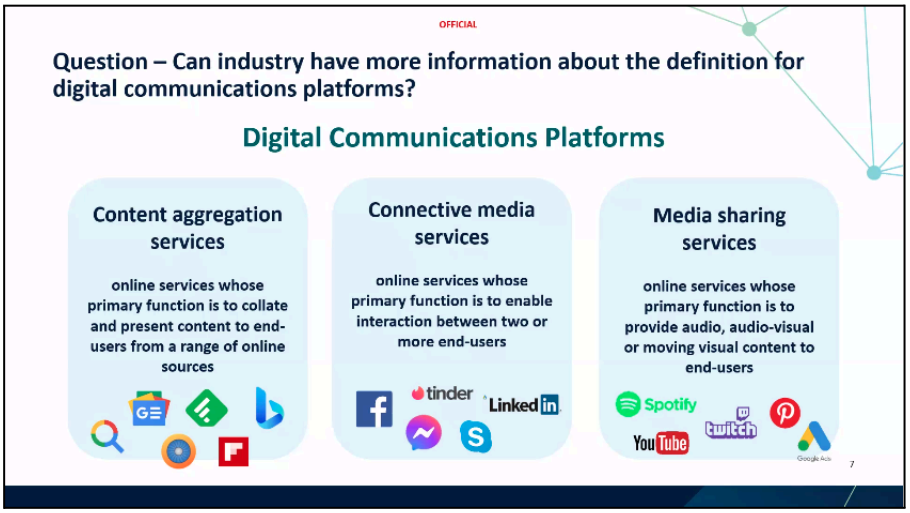
4.2. In this section, we provide input on the proposed scope of services that we believe is of utmost importance in order to develop effective, clear and implementable anti-scam measures that lift the bar across relevant industries. In short, we believe that the Consultation Paper's definitions of services are not conducive to targeted and effective interventions in relation to scams. The approach to defining the services in scope of this Bill has the potential to extend this regulatory scheme to an extremely broad range of services, including those that present low or limited risk. Measures that are appropriate for social media services may not be appropriate for products in this broader range of services.

4.3. DIGI encourages further workshopping with the digital industry about the scope of services relevant to the proposed regulatory framework, and associated definitions. Additionally, we recommend that definitions of sectors captured are set out in the industry-specific codes, rather than in primary law, in order to ensure more dynamism as sectors evolve, and to negate the need for legislative amendments.

4.4. DIGI and its members appreciated the opportunity to participate in industry engagement roundtable discussions with Treasury and the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA), and to receive further information about the intent behind the Consultation Paper by way of a slide presentation, shared with recipients. In order to contextualise the analysis in this section, we have included the slide in reference to 'digital communications platforms' as *Image 1* (below).

[8] The Hon Stephen Jones, (16/6/2022), *National Consumer Congress Speech*, https://www.stephenjones.org.au/media-centre/speeches/national-consumer-congress/; The Hon Stephen Jones (7/11/2022), *Transcript: Assistant Treasurer launches National Anti-Scams Centre*, https://www.ausbanking.org.au/transcript-the-hon-stephen-jones-mp-assistant-treasurer-and-minister-for-financial-services/

Image 1: Slide presented December 19, 2023



'Content aggregation services'

4.5. Per Image 1, we understand that 'content aggregation services' is intended to capture services such as Google Search, Google News, Feedly, Bing and Flipboard.

Search engines

4.6. DIGI does not consider that organic search results should be in scope. From our discussions with relevant members, DIGI is not aware of a prevalence of scams being perpetrated via organic search results. DIGI encourages a further evidence base in making determinations about the service-level scam interventions that will have maximal consumer benefit for Australians, including with respect to organic search results. It is important to emphasise the distinction between organic search results, and sponsored results which are the product of advertising services (which we discuss in 4.26).

4.7. Search engines are not well placed to identify scams, as they do not have the same signals about the provenance of a website as its web host or owner. While search engines routinely remove webpages if required by law, and would welcome a direction from a regulator to remove a webpage that has been found to be perpetrating scams, they generally cannot themselves determine that a website is perpetrating a scam.

4.8. Search engines also cannot rely on notices from the public alone in relation to scams, which may be used by business competitors to suppress legitimate competitor businesses. There is a real risk that obligations on search engines would lead to the over-removal of search results to the detriment of genuine businesses. However, if the page is removed at its host, any link from search results will be broken and will update. This underscores the importance of more comprehensive regulatory takedown powers in relation to scams, as detailed in Section 1, paragraph 3.

4.9. In the context of these challenges with search engines, it is important to note that the Standing Council of Attorneys-General last year advanced amendments to Part A of the Stage 2 Review of the Model Defamation Provisions that include two conditional, statutory exemptions from defamation liability for a narrow group of internet

intermediaries, including search engines in relation to organic search results[9].

4.10. DIGI recommends that a similar exemption be extended to organic search results, noting that any restrictions on advertising services could be used to extend to sponsored search results.

News aggregators

4.11. DIGI also does not consider services like Google News, Flipboard and Feedly to present a high risk of scam content, as their primary purpose is to connect audiences with publishers, particularly news content. We are not aware of evidence that makes such services at risk of being exploited by scammers.

4.12. We would not consider it a proportionate response for news aggregation services to adopt the ecosystem-wide nor sector specific obligations proposed in the Consultation Paper, nor do we consider the provision of a scams reporting channel on news aggregation services to be in line with consumer expectations when using such services.

4.13. We recommend a reconsideration of whether news, music, audiobooks and podcast aggregators or services present a high risk of scams, based on further evidence gathering, and an exclusion of these services from the scope of the regulatory framework.

'Connective media services'

4.14. Per Image 1, we understand that 'connective media services' are intended to capture services such as Facebook, Tinder, Messenger, Skype and LinkedIn.

4.15. While each of these types of service may be said to 'enable interaction' between end-users, there are vast differences between these services' specific purposes and functions. This creates significant challenges if Government intends for the sector-specific codes to impose a single set of mandatory obligations that individual service providers cannot opt in and out of, according to their particular functions and associated risk profile. For example, we question whether there are many, if any, specific anti-scam obligations that ought to apply to both a dating service like Tinder and a VoIP-based videotelephony service like Skype. From consultation roundtables, DIGI understands there is not an intention to identify a different set of obligations associated with each of the sub-categories. Given the issues raised above, we seek written clarification of this intention.

Blurred categories

4.16. Furthermore, it is unclear how such services that *also* 'collate and present content to end-users', such as publisher content, might readily identify themselves as 'connective media services' as opposed to 'content aggregation services', or 'media sharing services' if their offering includes audio-visual content. For example, Facebook, LinkedIn, Twitch and YouTube enable connection but also the presentation of content from a range of online services, and have been categorised differently in Image 1. It will be extremely challenging for such services to determine the category that applies to them.

[9] Standing Council of Attorneys-General (SCAG), Standing Council of Attorneys-General (SCAG) communiqué – December 2022],
https://www.ag.gov.au/about-us/publications/standing-council-attorneys-general-communiques

4.17. Even if there is a distinction advanced between a service's primary and ancillary function, this will not lend meaningful clarity to services with multiple and evolving functions.

Messaging services

4.18. It is important to emphasise that messaging on 'over-the-top' (OTT) services does not work in the same way as SMS and MMS, and are less of a vector for scams. As noted, the ACCC's report 'Targeting Scams: Report of the ACCC on scams activity 2022' showing that while phone calls and SMS text messages were the top contact methods employed by scammers, accounting for 62% of reported scams, social networking and online forums accounted for just 6%[10].

4.19. Consideration needs to be given to how the obligations between different types of private messaging services align, in light of similar consumer expectations, and varying architecture. Any obligations need to also consider the consumer expectation of encryption for these services, and the central importance of encryption in ensuring cyber security and scam mitigation efforts.

4.20. Serious consideration must be given to the fact that Australians do not expect proactive scanning of their private messages. Research conducted by Resolve Strategic in 2022, commissioned by DIGI, asked Australians what types of digital services should be scanned for 'restricted content', as a result of industry or government policy. Just over half of Australians reported that scanning publicly accessible posts and websites would be acceptable, but only a minority said this would be acceptable with more private files, messages and accounts. In particular, the scanning of emails, direct messages and files held on physical device was considered unacceptable for over two-thirds of Australians[11].

4.21. DIGI understood from the roundtable discussion held with relevant stakeholders on December 6, 2023, that there is an intention that email be out of scope. DIGI's members that provide email services implement highly effective anti-scams measures; for example, Google and Yahoo's mail services both block 99.9% of dangerous emails before they reach users every day, which includes emails containing phishing links or harmful malware[12]. However, should the intention be to exclude email, then the definition of 'connective media services' requires revision, as we interpret it to encompass email.

'Media sharing services'

4.22. Per Image 1, we understand that 'media sharing services' are intended to capture services such as Google Ads, Pinterest, Spotify, Twitch and Youtube.

4.23. Again, DIGI considers there to be major differences between each of these types of services, and that their risk profiles and levels of control will be vastly different.

---

[10] As above, *ACCC, Targeting scams: report of the ACCC on scams activity 2022*

[11] Resolve Strategic (2022), Consolidated Industry Codes of Practice for On-line Class 1 Content Community Research, https://digi.org.au/wp-content/uploads/2023/10/R220719-DIGI-CA-Project-Class-1-Sep-2022-Survey-Results-PUBLIC-RELEASE-5.pdf, p. 23

[12] Google Workspace, (10/2/2021) *New research reveals who's targeted by email attacks*, https://workspace.google.com/blog/identity-and-security/how-gmail-helps-users-avoid-email-scams

Music, audiobooks & podcasting services

4.24. DIGI seeks an evidence-base for the inclusion of such a broad set of categories, as we consider that there is currently a lack of proportionality in imposing strict anti-scam measures on services that primarily offer licensed professional created content such as music and audiovisual content such as, for example, Spotify. We are not aware of any suggestions that these services provide a vector for scams. DIGI is concerned that the misplaced allocation of resources on services where the incidence of scams is low will divert trust and safety resources away from other more relevant issues on such services that may be of higher concern to their users.

4.25. As noted, we recommend a reconsideration of whether news, music, audiobooks and podcast aggregators or services present a high risk of scams, based on further evidence gathering, and an exclusion of these services from the scope of the regulatory framework.

Advertising services

4.26. In relation to advertising services, the consideration of appropriate scam measures must recognise the inherent differences between closed and open ecosystems. In 'closed ecosystems' that are operated by a single entity, the provider can set the rules for entry to their ecosystem and take action independently of other actors. For example, action can be taken regarding the onboarding of onsite advertising and its presentation to users. Relevant DIGI members have broad-ranging advertising policies that prohibit or restrict a long list of illegal and potentially harmful goods and services.

4.27. Risk-based approaches for different types of advertising services will vary. For example, there should be different checks and balances encouraged depending on the nature of the advertising service i.e. whether it serves a long tail of advertisers, if it works with a small number of agencies and brands, or if it offers the opportunity for a wide range of advertisers to serve self-service ads online.

4.28. There may be some sector-specific obligations that may be more effective in a closed ecosystem, rather than in an open ecosystem, which requires a greater understanding of various intermediaries and the extent of their control. In 'open ecosystems', like programmatic advertising, collective action is needed by each entity in the supply chain, such as the advertiser, demand side platform, supply side platform and publisher. Intermediaries in the programmatic supply chain are limited in their capacity to singlehandedly address fraudulent advertising. There are a wide range of existing transparency technical standards that are currently available to participants in the open web programmatic ad tech supply and demand chains, and we encourage the Government to undertake further exploration of these with the Interactive Advertising Bureau (IAB).

4.29. In addition to the UK Online Charter for digital platforms (explored in Section 4), the UK Government has established the public-private Online Advertising Taskforce which has been considering how to address fraud and other illegal advertising in the open programmatic supply chain and on news and other content sites.[13] DIGI encourages similar deeper sub-sectoral analysis of advertising services to inform appropriate scams interventions.

[13] UK Department for Culture, Media & Sport, *Online Advertising Taskforce action plan - GOV.UK*, https://www.gov.uk/government/publications/online-advertising-taskforce-action-plan/online-advertising-taskforce-action-plan

5. Inconsistency and applicability of definitions

5.1. DIGI recognises that these three definitions have been adopted from the draft Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023. We have previously registered concerns about the lack of clarity in the definitions of services under the Misinformation Bill, which we have detailed in DIGI's corresponding submission[14]. It is unclear why these definitions have been proposed in relation to scams. Based on our expertise with regard to mis- and disinformation, as the developer and administrator of the ACPDM, there are fundamental differences between scams and misinformation that should guide the regulatory scope. For example, perpetrators of disinformation are motivated by influencing perceptions at large scale through services that enable mass distribution, whereas perpetrators of scams are financially motivated and therefore the services they choose to exploit will differ.

5.2. Additionally, DIGI is concerned that there is inconsistency with respect to both the services considered to be within scope of the proposed framework for scams and across the differing regulatory frameworks that either already apply or are being contemplated for implementation with respect to the digital industry.

5.3. The digital industry must be provided with consistent terminology in relation to any code development exercises, especially given the range of codes in contemplation for the industry. We note significant variations between the proposed definitions of the digital industry in the Consultation Paper, and under the Misinformation Bill, *The Online Safety Act 2021* and other potentially relevant frameworks for segmenting the digital industry in being contemplated by ACCC in its *Digital platform services inquiry Interim report No. 5 – Regulatory reform*[15].

5.4. To elaborate, under the Online Safety Act, the digital industry is divided into eight sections: providers of social media services (defined around online social interaction between 2 or more end-users), providers of relevant electronic services (includes any services with messaging, and gaming), providers of designated internet services (includes all websites), providers of internet search engine services, providers of app distribution services, providers of hosting services, providers of internet carriage services, and persons who manufacture, supply, maintain or install certain equipment (includes retailers).

5.5. In practice, this means that services like Facebook, LinkedIn and Twitch would consider themselves 'social media services' under the Online Safety Act; however, per the groupings advanced in Image 1, these same services are distributed across 'connective media services' and 'media sharing services'. This inconsistency creates confusion about the relevance and applicability of different sets of obligations.

6. Impact of breadth and inconsistency on scams

[14] DIGI, Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 (18/08/2023), https://digi.org.au/wp-content/uploads/2023/10/Final-submission-on-exposure-draft-of-Communications-Legislation-Amendment-Combatting-Misinformation-and-Disinformation-Bill-2023-1.pdf

[15] ACCC, *Digital platform services inquiry Interim report No. 5 – Regulatory reform,* https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry%20-%20September%202022%20interim%20report.pdf, p. 105

6.1. The Consultation Paper states that the goal of a whole-of-ecosystem approach is to 'lift the bar' for businesses in key sectors. While DIGI agrees with the goal, we are concerned that the approach to defining the ecosystem in relation to digital platforms is akin to an approach of 'boiling the ocean', where uplifts will be marginal (and may result in high costs for many firms), in comparison to a more targeted approach focused on a subset of more relevant services. That is to say, a narrower approach can see the development of more relevant and proportionate measures to specific services, and lends itself to a more consistently effective approach.

6.2. DIGI recognises the diversity of the digital platform services sector, and the related challenge in developing definitions for related regulatory instruments. One approach to overcome this challenge is to adopt the approach taken in the UK of a voluntary code that applies to major players in the ecosystem. Should the Government be concerned that a voluntary approach may not include key players in the ecosystem, it could solve this problem through empowering the regulator to direct a company to adopt an existing industry code or for it to develop and adopt an equivalent.

Summary of recommendations in Section 2

A. DIGI encourages further workshopping with the digital industry about the scope of services relevant to the proposed regulatory framework, and associated definitions.

B. DIGI recommends that definitions of digital industry sectors captured be set out in the industry-specific codes, rather than primary law, in order to ensure more dynamism as sectors evolve, and to negate the need for legislative amendments.

C. DIGI understands there is not an intention to identify a different set of obligations associated with each of the sub-categories (i.e. 'content aggregation services', 'connective media services', 'media sharing services'). We seek written clarification of this intention.

D. DIGI recommends that a similar exemption be extended to organic search results as the Model Defamation Provisions, noting that any restrictions on advertising services could be used to extend to sponsored search results.

E. We recommend a reconsideration of whether news, music, audiobooks and podcast aggregators or services present a high risk of scams, based on further evidence gathering, and an exclusion of these services from the scope of the regulatory framework.

F. Consideration needs to be given to how the obligations between different types of private messaging services align, in light of similar consumer expectations, and varying architecture, with attention to the consumer expectations for encryption – which protects against scams – and in relation to proactive scanning.

G. In relation to advertising services, DIGI encourages deeper sub-sectoral analysis of advertising services to inform appropriate scams interventions, in line with the approach in the UK.

H. The digital industry must be provided with consistent terminology in relation to any code development exercises, especially given the range of codes in contemplation for the industry.

I. In order to overcome the challenges associated with developing definitions for the digital industry, the Government should consider whether the UK model of a voluntary instrument confined to leading industry players may prove more effective.

J. Should the Government be concerned that a voluntary approach may not include key players in the ecosystem, it could empower the regulator to direct a company to adopt an existing industry code or for it to develop and adopt an equivalent.

Section 3: Considerations for proposed overarching framework

7. Avoiding duplication and ensuring clarity in obligations

7.1. DIGI understands that the proposed framework includes a hybrid approach of primary legislation under the Competition and Consumer Act (CCA), and sector specific obligations for digital platforms that could potentially sit under other regulation, such as the Broadcasting Services Act (BSA).

7.2. DIGI believes that sector-specific obligations will be sufficient in creating clarity and lifting the bar across designated sectors. We strongly question the value-add of having a mirrored set of categorised enforceable principles-based obligations set out in the CCA, especially ones that need to be drafted to apply to highly disparate sectors.

7.3. We understand from presentations from DITRDCA and Treasury to industry that the proposed amendments to the CCA are designed to establish the framework, tie together the various components, establish which industries must participate, create cross-sector consistency and promote consumer certainty.

7.4. However, DIGI considers that these same four objectives could be met through more refined amendments to CCA to empower relevant regulators to:

- 7.4.1. Enable the designation of applicable sectors;
- 7.4.2. direct a company to adopt an existing industry code, or for it to develop an equivalent;
- 7.4.3. empower the relevant regulator with code and standard-making powers, or oversight powers over industry-led codes;
- 7.4.4. empower the relevant regulator with information gathering powers in relation to scams.

7.5. We do not see this duplication of obligations, nor regulators, in other comparable legislation. For example, the Online Safety Act contains mandatory industry-led codes, and regulator-led standards should the regulator determine that codes do not meet requirements; these codes and standards are enforced by the eSafety Commissioner. The Online Safety Act also contains the Basic Online Safety Expectations (BOSE) that sits alongside these codes as voluntary principles-based obligations, for which the same regulator who oversees the industry codes can request information from service providers.

7.6. We are confident that the objectives in 4.3 can be met without establishing a secondary set of obligations, and a secondary regulator, and a secondary penalty regime.

8. Multi-regulator model

8.1. The approach outlined in 7.4 eliminates the confusion for industry and consumers associated with a multi-regulator regime with two sets of enforceable obligations, and potentially halves the cost for Australian taxpayers by consolidating responsibilities within a single regulator, as opposed to two regulators.

8.2. DIGI agrees that the ACMA is the most appropriate regulator for the digital industry. We are concerned about the effectiveness and the operation of a multi-regulator oversight and enforcement model. Rather than the ACCC enforcing a mirrored set of obligations to the ACMA, we consider that a more value-additive role for the ACCC would be to empower them with takedown powers over scams cross-sectorally, as noted.

8.3. With regard to the possibility of an industry funding model, or industry levies, in light of the cross-sectoral and cross-platform nature of scam activity, we envisage challenges in fairly attributing industry responsibility. DIGI recognises that large online platforms are rightly held to a high level of public scrutiny. As a result of that and their depth of technical expertise, we posit that the anti-scam investments made in this portion of the sector exceed those in some high risk portions that do not have as much experience nor the same levels of public scrutiny. While we believe the regulator should be well-resourced, cost-recovery may not be the best approach for these reasons, and that it may unintentionally incentivise enforcement actions.

9. Penalties

9.1. Particularly in light of the definitional ambiguities outlined in Section 1 and Section 2, and the cross-sectoral and cross-platform nature of scams, DIGI considers the proposed penalties to be extremely high. DIGI understands that the CCA provides penalties for non-compliance for the greater of: *'$50 million; three times the value of the benefit obtained, or 30 per cent of the corporations adjusted turnover during the breach'*.

9.2. Not only is this quantum of penalty extremely high, we believe it is wholly disproportionate to non-compliance with many of the proposed principles-based or sector-specific obligations, especially those with general requirements where full compliance may be subject to interpretation (e.g. the proposed general requirement for businesses to implement 'anti-scams systems').

9.3. While the paper states that the 'Government and regulators will work through the necessary arrangements to avoid two regulators taking simultaneous action against a breach under the Framework', DIGI recommends that the dual-penalty regime be removed in favour of a penalty regime enforced by the relevant sectoral regulator.

9.4. With substantial penalties under the CCA applying in circumstances where platforms fail to take action on scams, and with a lack of definitional clarity as to what constitutes a scam (as discussed in Section 1), we expect that the penalties will result in a substantial increase in platforms over-correcting to avoid the risk of breaching the CCA and facing fines. With the concentration of Australian retail trading around key moments (e.g. Black Friday, Boxing Day), the removal of an advertisement for scam review on the basis of a vexatious complaint for just a period of 24-48 hours could have a material impact on that business. Taking into account the impact of over-correction on legitimate business activity, we encourage a proportional or tiered penalty framework where fines are levelled for serious breaches or systemic failures.

10. Commentary on specific obligations

10.1. DIGI encourages attention to the preliminary commentary we have provided on the proposed overarching obligations, as set out below. However, more broadly, we recommend that the overarching obligations be removed and that this commentary is reflected in the evolution of sector-specific obligations.

Proposed ecosystem-wide obligations in the CCA	**DIGI preliminary commentary**
Prevention • *A business must develop, maintain, and implement an anti-scam strategy that sets out the business' approach to scam prevention, detection, disruption and response, based on its assessment of its risk in the scams ecosystem.* • *A business must take all reasonable steps to prevent misuse of its services by scammers, so that an undue burden is not placed on consumers or other market participants to prevent scams.* • *A business must implement anti-scam systems that are responsive to new products, services, designs, technologies, and delivery channels.* • *A business must provide their consumers or users with information about how to identify and minimise the risk of being scammed.* • *A business must train staff to identify and respond to scams.*	### Over focus on prevention 10.2. The word prevention appears seven times in the proposed ecosystem-wide obligations in the CCA. DIGI is concerned that the prevention of scams is not attainable, but rather the mitigation of user engagement is a more realistic goal for digital platforms, depending on the nature of the service that they offer. We observe that prevention is not a core theme of the existing telecommunications or banking obligations. 10.3. Knowledge of a scam is required in order for action to be taken. Unless the definition of a 'scam' is set with a level of volume (like the definitions in the telecommunications code), 'prevention' is not possible for a regulatory standard, particularly one that attracts penalties. ### Anti-scam strategies 10.4. DIGI is concerned that the proposal to provide an anti-scam strategy is duplicative of any reporting that may need to occur under the sector-specific obligations. 10.5. Noting the Consultation Paper's acknowledgement that publication would not be required, we emphasise that any publication of these strategies may compromise the confidentiality of companies' anti-scam strategies, which

	would provide scammers with information to advantage their criminal activity. 10.6. If there is a requirement for board-level sign off, this would not enable the necessary evolution of strategies to nimbly counter ongoing evolutions in the tactics used by perpetrators of scams. 'Reasonable steps' 10.7. DIGI is concerned that the standard that 'a business must take all reasonable steps' is inherently subjective, and is likely to lead to disagreements between individuals and companies around what they consider that they are undertaking reasonable steps. It is preferable to have specific and easily implementable measures that business can adopt. These measures could be easily evolved and adapted if included in an industry-led code that can be more readily updated than legislative amendments.
Detection and disruption • *A business must seek to detect, block and prevent scams from initiating contact with consumers.* • *A business must seek to verify and trace scams where scam intelligence has been received.* • *A business must act in a timely manner on scam intelligence received through information sharing, consumer reports, complaints and other means.* • *Where a business receives intelligence that a consumer is or may be a target of a scam, the business must take steps to disclose this to the consumer in a timely manner to minimise the risk of consumer harm or loss.*	Proportionality & attainability 10.8. As noted above, it is unrealistic to ask all companies to 'prevent' and 'block' scams from initiating contact with consumers. Obligations need to set an attainable standard. 10.9. We also question the proportionality of some of the detection and disruption measures for services where the incidence of scams is low. There is a heavy technological lift and cost to implement effective proactive detection of scams.

• *A business must provide their consumers or users with tools to verify information in real time.*	NASC-built consumer tools 10.10. Specifically, the provision of 'tools to verify information in real time' is not possible for all services intended to be covered by the regulatory regime; it is also unclear to us what such tools would actually entail. The development of such tools would be necessarily limited to the data on singular services. DIGI considers that a more effective way to enable consumers to verify information in real time would be for the NASC to develop a consumer-facing database of known scams that consumers can use to investigate the veracity of an offer. Only the NASC has the cross-sectoral purview to develop such tools effectively.
Response (obligations with respect to consumers) • *Where a consumer has identified they have been affected by a scam, businesses must take all reasonable steps to prevent further loss to the consumer and treat consumers fairly and consistently.* • *A business must have user-friendly, effective, efficient, transparent, and accessible options for consumers or users to report a scam, including people not directly targeted by a scam.* • *A business must have user-friendly, effective, transparent, and accessible complaints handling processes for consumers or users to make a complaint about how a scam report was handled or in relation to a business's response to scam activity (including steps taken to prevent, detect, disrupt and respond to scam activity).* • *Where a consumer escalates concerns with a business, they should be dealt*	Responding to scams 10.11. DIGI reiterates its concerns about the standard that 'a business must take all reasonable steps' as noted in 10.7. 10.12. As in all areas, DIGI is concerned that there is duplication in relation to 'response' obligations with those being proposed in the sector-specific obligations, and that such granular obligations would be more appropriate within the latter. 10.13. Scam complaints push companies to make determinations about scams. When there is no ACCC takedown power that assists the industry in making confident determinations (as discussed in Section 1), we are concerned about the risk of over-correction to avoid penalties.

with fairly and promptly, and consumers should be given access to information about dispute resolution options where applicable.	IDR/EDR 10.14. DIGI also notes questions about the nature of the Internal Dispute Resolution (IDR) and External Dispute Resolution (EDR) expectations, when these structures are not currently established for the digital platforms sector. DIGI would welcome the opportunity to further engage with the Government in relation to these questions.
Reporting (obligations to regulators and other businesses) ● *A business must take reasonable steps to notify other businesses, the NASC and relevant regulators promptly of intelligence about suspected or identified organised large-scale scam activity as well as rapidly emerging or cross-sectoral scam activity.* ● *A business must share data and information on the incidence of scams, and action taken in response, with designated industry bodies, law enforcement and regulators, and the NASC.* ● *A business must keep records of incidences of scams, and the action taken in response.* ● *A business must respond to an information request from the ACCC within the timeframe specified.*	Data sharing considerations 10.15. DIGI supports cross-sector collaboration and an ecosystem approach to addressing scams. While we see benefits in deepening this collaboration through the NASC, we are concerned that the framework proposes to legislate within the CCA the sharing of data. 10.16. DIGI recommends that information sharing be led by the NASC, and should be focused on industry best practices and learnings in scam mitigation and redress, rather than involving the sharing of any user data. This will also serve to drive industry improvements at a large scale. Because digital platforms' scam efforts are encompassed within broader privacy and security policy prohibitions and enforcement actions, this can complicate the data quality about Australian scams specifically. 10.17. To the extent that user-level data can assist in the resolution of specific scams, and where it cannot be provided voluntarily by industry, the NASC should also consider how it works

more closely with law enforcement to support the successful investigation and prosecution of offenders. Over time, this approach may also serve as an effective deterrent to perpetrators of scams.

10.18. It is also worth noting that digital platform services are managing complaints at a large scale, and cannot reasonably share information about all scams, unless there is a specific service identified that is encouraged to take action, or a threshold of user impact.

10.19. While data gathering is a valuable exercise, from a statistical perspective, it is unclear what additional data reporting will drive in terms of insights and understanding. It is unclear what industry bodies, for example, could do with this information. We note that the Government already monitors and effectively identifies key aspects of scams via a range of other mechanisms.

Record keeping

10.20. The proposed requirement to keep records of (presumably all) incidences of scams and the action taken in response is likely to be unreasonably onerous and impracticable to comply with for most businesses, especially attempted scams that are immediately removed through automated processes. These requirements should be clarified or limited to defined circumstances.

Information sharing

10.21. We question the need for information requests from both the ACCC and the ACMA in relation to scams responses, and question whether this is an

	efficient and cost-effective use of public resources. We recommend that scams-related information gathering powers be confined to sector-specific regulators.

Summary of recommendations in Section 3

A. DIGI believes that sector-specific obligations will be sufficient in creating clarity and lifting the bar across designated sectors. We strongly question the value-add of having a mirrored set of categorised enforceable principles-based obligations set out in the CCA, and recommend that these obligations be removed.

B. However, DIGI considers that the Government's objectives with the overarching framework could be met through more refined amendments to CCA to i) empower relevant regulators to enable the designation of applicable sectors; ii) direct a company to adopt an existing industry code, or for it to develop an equivalent; iii) empower the relevant regulator with code and standard-making powers, or oversight powers over industry-led codes; iv) empower the relevant regulator with information gathering powers in relation to scams.

C. Rather than the ACCC enforcing a mirrored set of obligations to the ACMA, a more value-additive role for the ACCC would be to empower them with takedown powers over scams cross-sectorally, per Recommendation 1H. Additionally, the ACCC could be provided with the powers to designate sectors to develop sector-specific obligations.

D. DIGI does not recommend an industry funding model, or industry levies, because the cross-sectoral and cross-platform nature of scam activity would result in challenges in fairly attributing industry responsibility.

E. DIGI recommends that the dual-penalty regime be removed in favour of a penalty regime enforced by the relevant sectoral regulator.

F. In the context of the impact of industry over-correction on legitimate business activity, we encourage a proportional or tiered penalty framework where fines are levelled for serious breaches or systemic failures.

G. DIGI encourages attention to the commentary we have provided on the proposed overarching obligations. However, more broadly, we recommend that the overarching obligations be removed and that this commentary is reflected in the evolution of sector-specific obligations.

H. DIGI considers that a more effective way to enable consumers to verify information in real time would be for the NASC to develop a consumer-facing database of known scams that consumers can use to investigate the veracity of an offer. Only the NASC has the cross-sectoral purview in Australia to develop such tools effectively.

I. DIGI recommends that information sharing be led by the NASC, and should be focused on industry best practices and learnings in scam mitigation and redress, rather than involving the sharing of any user data.

J. The NASC should consider how it works more closely with law enforcement to support the successful investigation and prosecution of offenders. Over time, this approach may also serve as an effective deterrent to perpetrators of scams.

K. Record-keeping requirements need to be clarified or limited to defined circumstances in order to ensure proportionality, such that businesses are not required to record all incidences of scams, many of which are promptly intercepted.

L. DIGI recommends that scams-related information gathering powers be confined to sector-specific regulators.

Section 4: Creating clear obligations for industry

11. Principled-based, risk-based & global approaches

11.1. The digital industry is arguably the most diverse sector economy-wide. It stands in stark contrast to banks and telecommunications providers that provide relatively homogenous product offerings in comparison.

11.2. This diversity is why principled-based obligations that can be flexibly applied in the proposed framework are critically important. This diversity also necessitates risk-based approaches to encourage obligations that are proportionate to the prevalence and addressability of scams on a range of services.

11.3. In our view, the proposed sector-specific obligations in the Consultation Paper do not strike the right balance of being principles and risk-based. While DIGI refutes the need for a dual set of obligations, and noting the specific concerns we have detailed in Section 3 about the proposed overarching obligations, conceptually we consider the proposed CCA obligations to be set at a more principled level than the proposed sectoral obligations. In comparison, the proposed sectoral obligations are too granular and prescriptive to be relevant nor feasible to the range of services intended to be in scope.

11.4. DIGI encourages the Australian Government to closely review the measures The UK Online Fraud Charter, which was released on November 30, 2023[16] and therefore postdates the development of the Consultation Paper. This charter was developed by the industry association TechUK and the Charter's signatory services and the UK Government: Amazon, eBay, Facebook, Google, Instagram, LinkedIn, Match Group, Microsoft, Snap, TikTok, X (f.ka. Twitter) and Youtube. While the measures are most relevant to these signatories, they provide an indication of an achievable, principles-based and risk-based standard in the digital industry.

11.5. The UK Online Fraud Charter is particularly relevant in light of the global nature of such companies' trust and safety operations. While DIGI's relevant members readily respond to Australian complaints, architecting an Australia-specific solution will pose challenges when counter-scam measures from multinational companies are generally centrally managed from overseas offices.

11.6. In relation to the UK Online Charter, the UK Government calls out 'the successes of previous voluntary charters with the retail banking, telecoms and accountancy

[16]UK Home Office (30/11/2023), Online Fraud Charter, https://www.gov.uk/government/publications/online-fraud-charter-20

sectors'. We encourage the Australian Government to better understand the reasons why the UK Government has opted for voluntary codes.

11.7. Noting that the ACMA is identified as the potential regulator for the digital industry, DIGI encourages a graduated approach that is consistent with the ACMA's compliance and enforcement policy, where a voluntary code is developed in the first instance, before the development of co-regulatory obligations, and before making changes to primary law[17]. In relation to the digital industry, we are surprised that the framework proposes primary law changes and co-regulatory obligations in the first instance, without first exploring self-regulatory codes.

11.8. Furthermore, DIGI notes that Minister Rowland, in her National Press Club address on November 22, 2023, indicated that Australia is in the advanced stages of establishing a new online safety and security memorandum of understanding with the UK which will increase bilateral engagement, and to 'share and learn from our close allies to ensure our regulatory interventions are measured, targeted and evidence-based'[18]. Closely reviewing the applicability of the UK Online Charter in Australia would be consistent with the spirit of such a memorandum.

12. Commentary on specific proposals

12.1. An industry-led approach to code development (as discussed in Section 5) would enable a deeper exploration of appropriate measures for the sector. While DIGI considers that the code development process is the most appropriate stage for offering input on specific obligations, below we outline some preliminary commentary on the proposals advanced in the Consultation Paper.

Possible digital communications platform specific obligations in Consultation Paper	**DIGI preliminary commentary**
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.* • *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.* • *A provider of a digital communications*	Proportionality & attainability 12.2. DIGI does not consider these measures to be relevant to the whole range of services intended to be in scope. For example, not all digital communications platforms enable interaction, and would have mechanisms to 'detect higher risk interactions'. 12.3. While mainstream services will have robust cyber security measures in place in order to prevent or mitigate the likelihood of hacking, we do not consider outright 'prevention' to

[17] ACMA, *Compliance and enforcement policy*, https://www.acma.gov.au/compliance-and-enforcement-policy
[18] The Hon Michelle Rowland MP, Address to the National Press Club, https://minister.infrastructure.gov.au/rowland/speech/address-national-press-club

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.	be an attainable standard for an enforceable code. Sources of 'truth' 12.4. In relation to the obligation to 'authenticate and verify the identity and legitimacy of business users and advertisers', it is important to emphasise that such obligations rely on industry being provided with an external source of truth. For example, in June 2022, Google introduced a financial advertising policy that requires advertisers seeking to promote financial products and services to be verified through a manual check of their license status with the Australian Securities and Investments Commission (ASIC). This highlights the importance of collaboration between industry and government in addressing scams. DIGI believes that the NASC is well-positioned to provide industry with a 'source of truth' in relation to known scams that should be addressed. Avoiding warning fatigue 12.5. The proposal to 'warn users about suspected or identified scam activity, content or profiles' raises feasibility questions. Should this require a service to notify *every* user that was in contact with a business after a report of a *suspected* scam, services will encounter logistical barriers in relation to the appropriate placement of such warnings, in line with the privacy and communications expectations of their users. Additionally, the threshold of 'suspected' presents a low bar that could negatively impact legitimate businesses.

Detection and disruption • *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 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.*	Data sharing considerations 12.6. We reiterate the points made in relation to data sharing considerations from 10.15 to 10.19, as they relate to this corresponding obligation. 'Is likely to be' 12.7. DIGI is concerned that the threshold of 'is likely to be', used twice in this section, lowers the threshold for action and creates further ambiguity for industry in relation to their obligations in an enforceable code.
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.* • *A business must respond to an information request from the ACMA within the timeframe specified.*	Information sharing 12.8. As noted in Section 3, We question the need for information requests from both the ACCC and the ACMA in relation to scams responses, and question whether this is an efficient and cost-effective use of public resources.

Summary of recommendations in Section 4

A. Sector specific obligations for the digital industry need to be principled-based and risk-based approaches in order to encourage obligations that are proportionate to the prevalence and addressability of scams on a diverse range of services.

B. DIGI encourages the Australian Government to closely review the measures in the UK Online Fraud Charter, which was released on November 30, 2023. While the measures are most relevant to these signatories, they provide an indication of an achievable, principles-based and risk-based standard in the digital industry.

C. In relation to the UK Online Charter, the UK Government calls out 'the successes of previous voluntary charters with the retail banking, telecoms and accountancy sectors'. We

encourage the Australian Government to better understand the reasons why the UK Government has opted for voluntary codes.

D. Noting that the ACMA is identified as the potential regulator for the digital industry, DIGI encourages a graduated approach that is consistent with the ACMA's compliance and enforcement policy, where a voluntary code is developed in the first instance, before the development of co-regulatory obligations, and before making changes to primary law.

E. DIGI encourages close attention to the preliminary commentary we have provided on the proposed overarching obligations. However, we consider the code development process to be the most appropriate stage for offering input on specific obligations.

F. DIGI believes that the NASC is well-positioned to provide industry with a 'source of truth' in relation to known scams that should be addressed.

Section 5: The approach to code development

13. Parity and fairness across sectors

13.1. DIGI notes inconsistencies with the proposals for how a code may be developed for the three priority sectors, particularly on whether the code can be industry-led.

13.2. The Consultation Paper states that the Department of Treasury, would develop the banking sector code, and goes on to say that *'The Framework will also consider the voluntary work being progressed by different parts of industry to address scams, such as the anti-scam initiatives being delivered by the banking sector. The Government may consider lifting effective voluntary scams initiatives into legislation by establishing them as either ecosystem-wide obligations or sector-specific obligations within the Framework, where appropriate.'* DIGI recognises that many of the obligations for the banking sector in the Consultation Paper overlap with the Australian Banking Association's voluntary Scams Safe Accord.

13.3. For the development of the telecommunications code, The Consultation Paper indicates that the telecommunications industry body, the Communications Alliance, would be asked to review its existing Reducing Scam Calls And Scam SMS code in 2024 and consider what changes are required to improve its operation and to ensure consistency with the regulatory framework. DIGI notes that, under obligations that Communications Alliance had set, this code was already due for a review by July 2024.

13.4. In relation to digital platforms, the Consultation Paper begins by proposing a mandatory code that the ACMA would establish. Yet, the Consultation Paper entertains '*an alternative pathway to the ACMA developing obligations would be to allow the digital communications platforms industry to develop a code itself, to be registered and enforced by the ACMA to provide mandatory obligations, if the Government considers the industry code to be consistent with obligations across other regulated sectors.* DIGI strongly urges the encouragement of this pathway, which we consider will be beneficial for Australian consumers, as outlined in paragraph 15.

14. Opportunity for an industry-led approach

14.1. DIGI has extensive experience in code development with digital service providers. We developed *The Australian Code of Practice on Disinformation and Misinformation* (ACPDM), and co-led the development of seven mandatory codes pertaining to Class 1 content under the Online Safety Act. We would welcome the opportunity to discuss our experiences with the Treasury to aid further exploration of codes as a regulatory tool, and code development models.

14.2. There are a range of approaches to codes, with two key variables being whether they are *voluntary* or *mandatory*, and whether they are *industry-led* or *regulator-led*. In Image 2, we provide examples of codes relating to the digital industry divided along these variables. DIGI has been involved in all but one of these examples, and can provide further information about these experiences.

Image 2: Different digital industry code-development models

14.3. In Section 4 of this submission, we have highlighted the advantages of a voluntary code, similar to the approach adopted by the UK Government, which overcomes the difficult questions associated with delineating a consistent scope of relevant services. As noted, this would also reflect the ACMA's graduated approach that is consistent with the ACMA's compliance and enforcement policy[19], where a voluntary code is developed in the first instance, before the development of co-regulatory obligations, and before making changes to primary law. Should the Government be concerned that a voluntary approach may not include key players in the ecosystem, it could solve this problem through enabling the ability for the regulator to direct a company to adopt an existing industry code compliance or for it to develop an equivalent.

14.4. However, should the Government be determined to pursue a mandatory code, we urge the Government to enable an industry-led approach in the first instance. Per Image 2, the majority of codes relating to the digital industry have been industry-led. We encourage dialogue between the Australian Government and DIGI about the role we could play in leading those efforts on behalf of the digital industry.

15. Benefits of an industry-led approach

15.1. An industry-led approach has a number of benefits for Australian consumers. First of all, it is cost effective, as the costs are largely borne by industry, rather than Australian taxpayers.

15.2. Industry-led processes enable closer collaboration with the industry participants that will be subject to the code, which has the effect of ensuring their experiences of what is technically possible and effective is ingrained in the code.

15.3. That close industry collaboration is complemented through deep collaboration with the relevant regulator. For example, in co-leading the Online Safety Act registered codes on Class 1 content, DIGI and Communications Alliance were in close communication iteratively with the Office of the eSafety Commissioner in all stages of the development process.

15.4. Industry associations are also well positioned to strive for a principles-based approach, enabling the future proofing of codes to changes in the digital environment, and encouraging companies to continue to develop innovative solutions to meet their requirements.

15.5. The many critiques of the proposed definitions of scams and digital communications platforms (included in Section 1 and Section 2 of this submission), and the critiques of the proposed measures and their ability to be implemented (included in Section 3 and Section 4 of this submission) serve to underscore the value of an industry-led process, where technology practitioners and industry professionals are reflecting their direct expertise to advance consumer outcomes. DIGI looks forward to the opportunity to discuss this further with the Australian Government.

[19] ACMA, *Compliance and enforcement policy*, https://www.acma.gov.au/compliance-and-enforcement-policy

Summary of recommendations in Section 5

A. Should the Government choose to advance a mandatory code, DIGI recommends an industry-led code. We encourage dialogue between the Australian Government and DIGI about the role we could play in leading those efforts on behalf of the digital industry.

Section 6: DIGI's members' approaches to scams

16. Bespoke strategies

16.1. At the outset, DIGI wishes to underscore that it is in the digital industry's business interests to protect users from scams; there is a highly diverse market of digital platform services, and negative experiences will see users readily move to other services. This provides the industry with strong incentives to take robust anti-scam measures, and make continued investments in this area. For this reason, technology companies have had long-standing and comprehensive investments in privacy and security to protect consumers.

16.2. It is also important to again emphasise that the digital industry is arguably one of the most diverse sectors. Unlike the other identified industries in this stage of reform (i.e. banking and telecommunications) it does not offer homogenous products, making it less suitable for cross-industry regulatory approaches. Any regulatory approach therefore needs to carefully account for the highly varied nature of the products and services offered.

16.3. Services represented in n DIGI's membership include: Social media services (e.g. Instagram, TikTok, Facebook, Twitch, LinkedIn), video sharing platforms (e.g. YouTube), messaging platforms (e.g. iMessage, WhatsApp, Snapchat, Discord, Skype), email (Gmail, Yahoo Mail, Outlook), marketplaces (e.g. eBay), app stores (e.g. Google Play, App Store), advertising platforms (e.g. Yahoo Advertising, Google Ads), internet browsers (Google Chrome, Apple Safari) and search engines (Google Search, Bing).

16.4. Each of our members have their own highly customised, multi-pronged, bespoke work programs across safety, privacy and security that encompass combatting scams in a manner that is proportionate to the prevalence and addressability of these issues on their service. Nonetheless, DIGI has identified some common themes that are applied proportionately based on the nature of the service, as outlined below.

17. Enforced restrictions

17.1. Relevant member services have Terms of Service and Community Guidelines restrictions on scams and financial fraud. Enforcement actions include content removal and account termination, depending on the nature of the service, the specific policy violation and the information available.

17.2. Often policy restrictions on scams are encompassed within broader restrictions on behaviours in areas such as phishing, impersonation, misrepresentation, deceptive and harmful business propositions, 'platform manipulation' or 'inauthentic behaviour' and unlawful advertising. Their restrictions cover organic and paid content, with different thresholds.

17.3. The reporting categories have to be all-encompassing of many types of abuse taking place across multiple jurisdictions, complicating data quality about Australian scams specifically.

18. Proactive detection

18.1. Enforcement includes proactive detection of spam behaviour, often prior to it being reported by users. This is done using trained algorithms that often capture multiple abusive behaviour types, not just spam.

18.2. For example, all advertisements on Snapchat are run through an automated fraud detection model, with ads detected as fraudulent proactively and automatically rejected. Information from rejected ads is used to enhance the model's capabilities to recognise new fraudulent advertisers and trends. This includes maintaining a list of known fraudulent website domains that are automatically rejected.

18.3. As noted, Google and Yahoo's mail services both block 99.9% of dangerous emails before they reach users every day, which includes emails containing phishing links or harmful malware[20].

19. Reporting tools

19.1. Digital platforms offer their users ways to report scams within their products. Volumes of user reports are managed by digital services at an extremely large scale.

19.2. There are innovations in reporting tools, including cross-sector collaboration. For example, in Apple iMessage, users can report spam messages that may be scams. Depending on a user's carrier and country, they can also use the same reporting tool for SMS and MMS.

19.3. Owing to the scale with which digital platforms operate, there are high volumes of user reports that are actioned. For example, for Google Ads in 2022, 142 million ads were blocked or removed for violating misrepresentation policies[21].

19.4. Several services have escalation pathways for regulators raising complaints on behalf of consumers or business. For example, the eBay Regulatory Portal enables trusted authorities such as the ACCC and the Therapeutic Goods Administration (TGA) to report and remove listings from the eBay marketplace within two hours without further approval from eBay.

20. Customer service

20.1. As well as technological approaches, trust and safety teams of people review user reports. DIGI's founding members are mostly multinational companies, so their trust

[20] Google Workspace, (10/2/2021) New research reveals who's targeted by email attacks, https://workspace.google.com/blog/identity-and-security/how-gmail-helps-users-avoid-email-scams
[21] Google Ads, (29/03/2023), *Our 2022 Ads Safety Report*, https://blog.google/products/ads-commerce/our-2022-ads-safety-report/

and safety teams are global, providing the advantage of them often operating on a 24/7 basis.

20.2. Trust and safety teams largely use email, chat or in-product communication in order to operate sustainably at an extremely large scale. There are often data scientists, engineers and content policy staff working behind the scenes to optimise the approach to scams. A global response is extremely important as scammers operate simultaneously in multiple jurisdictions.

21. Safety by design

21.1. In addition to the enforced restrictions, relevant member services integrate the principle of 'safety by design' to protect Australians from scams, placing consumer protection at the centre of the design and development of their products[22]. Safety by design measures have to be bespoke to different digital services, for example:

21.1.1. eBay places restrictions on buyers and sellers attempting to complete transactions outside of eBay which exposes them to potential scam behaviour. For transactions on platform, eBay provides the eBay money-back guarantee (eMBG)[23] giving protections to consumers for items that don't arrive or match the listing. The eMBG is offered in addition to consumers' rights under the Australian Consumer Law.

21.1.2. Yahoo! Advertising's demand-side advertising platform (DSP) only transacts with major service providers who pay in arrears and are vetted and managed via a direct contact within the company.

21.1.3. Google Ads subjects certain advertisers to an advertiser identity verification program that entails submitting information including identification, and business incorporation documents. In June 2022, Google introduced a financial advertising policy that requires advertisers seeking to promote financial products and services to be verified through a manual check of their license status with ASIC.[24]

22. In-product consumer education

22.1. Where appropriate, the industry works to educate their customers within their products, often to intercept their susceptibility to scams.

22.1.1. For example, TikTok displays public service announcements about scams when users type certain words in the search bar, such as 'investment', as well as banners that appear on relevant videos. These link to safety resources on scams.

22.1.2. Google's Safe Browsing helps protect more than five billion devices from phishing, across the web. Safe Browsing shows warnings about websites it considers dangerous or insecure. The technology is freely available and it is deployed in competing browsers in addition to Chrome (e.g. Firefox, Safari)

[22]Office of the eSafety Commissioner, Safety by Design, https://www.esafety.gov.au/industry/safety-by-design
[23] eBay, eBay Money Back Guarantee, https://pages.ebay.com.au/ebay-money-back-guarantee/
[24] Google Advertising Policies Help, *Financial Services Verification: Relevant Regulators and Enforcement Dates*, https://support.google.com/adspolicy/answer/12390454?hl=en

and across many different platforms, including iOS and Android[25].

23. Digital literacy collaborations

23.1. There are partnerships between the digital industry with consumer organisations and the Government to raise awareness about scams and to increase consumer resilience. Improved digital literacy – particularly to vulnerable Australians – is absolutely essential in improving consumer resilience to scams.

23.2. Many of DIGI's members have contributed content to the Australian Government's *Be Connected*[26] initiative aimed at improving the confidence, skills and online safety of older Australians. eBay has contributed courses including how to avoid or resolve problems such as products not arriving.

23.3. Meta has partnered with the national identity and cyber support service, IDCARE, and the pet scam prevention organisation, Puppy Scam Awareness Australia, to use its platforms to raise awareness about scams.

23.4. Google has worked with the Australian Consumer Communications Action Network (ACCAN) to promote resources on gift card scams, including running a campaign on YouTube[27].

23.5. The information presented here is a high-level overview of some relevant initiatives. DIGI would welcome the opportunity to further present information about these anti-scam initiatives, along with relevant members.

[25] Google, *Making the world's information safely accessible*, https://safebrowsing.google.com/
[26] Australian Government, *Be Connected*, https://beconnected.esafety.gov.au/
[27] ACCAN, *ACCAN's Guide to Stopping Scams,* https://www.youtube.com/user/ACCANvideo