



Ms. Shellie Davis
Head of the Scams Taskforce
Scams Taskforce
Market Conduct Division
By email: ScamsPolicy@treasury.gov.au

Tuesday October 1, 2024

Dear Ms. Davis,

The Digital Industry Group Inc. (DIGI) thanks you for the opportunity to provide our views on the *Treasury Laws Amendment Bill 2024: Scams Prevention Framework* (The Framework), as advanced in the Framework's Exposure Draft, Exposure Draft Explanatory Materials (Explanatory Memorandum), and the *Scams Prevention Framework: Summary of Reforms* (Summary of Reforms).

By way of background, 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, Meta, Microsoft, Spotify, Snap, TikTok, Twitch, X 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 is committed to the Government's mission to make Australia a harder target for scammers. DIGI has long supported the establishment of the National Anti-Scams Centre (NASC) and is proud to be represented on its Advisory Board, and various working groups. We are supportive of the 'ecosystem' approach the NASC takes to foster close collaboration between industry and government, and believe this model can be further enhanced irrespective of the Framework. As scams can span multiple services, approaches should be holistic, involving a range of relevant industries across the private sector as well as consumer bodies, regulators and law enforcement. **Accordingly, DIGI is supportive of a cross-economy approach in encouraging industry action across different sectors.**

As you are aware, from our extensive engagement with Government on this effort, on July 26, 2024, DIGI launched *The Australian Online Scams Code* (AOSC)¹. The AOSC is a proactive effort from the digital industry in line with the Government's wider legislative agenda in scams, and an important step in realising the Government's 2022 pre-election commitment for a social media scams code. DIGI has sought a collaborative approach with the Government to the development of this code, by offering avenues for feedback through workshops and the provision drafts. Accordingly, as this work demonstrates, **DIGI is supportive of requirements to create sector-specific codes for greater accountability for relevant industries to uplift their anti-scam activities.**

The AOSC has widespread adoption across the mainstream digital industry, with Apple, Discord, Google, Meta, Snap, TikTok, Twitch, X and Yahoo as signatories. The AOSC contains clear, implementable guidelines for the sectors intended to be designated under The Framework – social media, paid search engine advertising and direct messaging services. It also includes social media services with peer-to-peer

¹ DIGI, *The Australian Online Scams Code*, www.digi.org.au/scams

marketplaces, and email, which we understand are not intended to be designated initially. In working with the digital industry on this proactive approach, DIGI developed 38 clear commitments grouped under the following nine themes: 1) *Blocking*: Deploy measures to detect and block suspected scams; 2) *Reporting*: Have a simple and quick route for users to report possible scams; 3) *Takedowns*: Take quick action against verified scam content and scammers; 4) *Advertising*: Deploy measures to protect people from scam advertising; 5) *Email and messaging*: Deploy specific measures to protect people from scams in emails and private messages; 6) *Law enforcement*: Engage with law enforcement efforts to address scams; 7) *Intelligence sharing*: Contribute to public-private and cross-sectoral initiatives to address scams; 8) *Communications*: Provide information about scam risks and support counter-scam efforts; 9) *Future proofing*: Contribute to strategy development and future proofing exercises to stay ahead of the threat. **The AOSC provides a globally interoperable model that we recommend the Government draw upon in developing the mandatory sectoral digital industry code.**

As demonstrated by DIGI's work on the NASC and the AOSC, we are supportive of both the economy-wide approach and sector-specific obligations that the Framework seeks to introduce. Throughout this submission, DIGI advances a range of specific suggestions for how the Framework can better achieve these goals. Some of the concerns detailed in our submission include:

1) Duality of obligations under the Framework

We are concerned that the Framework contains a set of prescriptive obligations in primary legislation designed to apply to a wide range of industries, in addition to forthcoming obligations that will be set out in sectoral codes through subordinate legislation – creating two sets of obligations, two sets of regulators, and two sets of penalties. Further, a company can be in breach of the obligations in the primary legislation while complying with all of the obligations in the subordinate legislation's sectoral code. While there is no longer time in this term of Government to develop the promised mandatory codes, the solution is not to rush a pseudo code through the overarching legislation, with limited industry input through an extremely short consultation period. **Instead, the primary legislation should focus on enabling the development of mandatory codes that outline robust, sector-specific obligations for regulated entities, which would support and remain consistent with the delivery of the Government's commitments.**

While DIGI advances a wide range of specific suggestions in improving the implementation of obligations proposed in the primary legislation in this submission, ultimately we believe strongly that **the Framework should not itself contain obligations, other than the obligation for entities to comply with the codes. DIGI's specific suggestions in relation to obligations should be considered by regulators developing the mandatory codes.** We consider that the prescriptive obligations in the primary legislation are currently inapt for all three sectors, and may also be unsuitable to the sectors that the Government intends to bring into the Framework in future, namely superannuation funds, digital currency exchanges, other payment providers, and transaction-based digital platforms like online marketplaces.

2) 'Reasonable steps' should be determined in mandatory codes

Under the Framework's primary legislation, companies face penalties up to the greater of \$50 million or 30 percent of turnover that hinge on varying interpretations – by companies, consumers and regulators – of the concept of 'reasonable steps' in the primary legislation. Noting our recommendation above, **to the extent that any concept of 'reasonable steps' remains in the primary legislation, what constitutes 'reasonable steps' must be outlined in mandatory sector-specific codes.** Crystal clear obligations for industry, along with clear responsibilities for regulators, mean better outcomes for consumers.

3) Excessive and impractical reporting requirements

Under the Framework, entities face penalties up to the greater of \$10 million or 10 percent of turnover, if they do not share information about potential scams with the regulator. High penalties in the context of a low and vague threshold for reporting will lead to the ACCC being inundated with millions of reports about potential scams. Scams are often perpetrated by criminals offshore, and global companies may be reporting large volumes of information about international actors beyond the reach of the ACCC. It is unclear what the ACCC will do with all of that information, how they will receive it, and how they will use it to inform consumers about potential scams. Reporting requests should be scoped towards clear outcomes, including what meaningful actions will be taken with the information that is shared. This is the best outcome and most practical scenario for both industry and the regulator. **The Government must both narrow the scope of this reporting, and consult on the related technical and operational requirements for receiving reports, before any such requirement is legislated.**

4) Questions regarding consumer redress

DIGI is supportive of an economy-wide approach, and strengthening accountability in the digital industry. However, it is important to recognise that digital platforms, including social media services, are not an equal vector as the banking and telecommunications sector in relation to scams. According to Australians' reports to Scamwatch in 2023, text message remains the most popular method of choice for scammers (34 per cent), followed by phone call (27 per cent)². 5.8 percent of contacts came from 'online forums', which includes a much wider range of websites including professional trading websites, of which social media is a quantifiably unknown subset. While scammers will move seamlessly across limitless numbers of online forums, their final step always involves theft through financial services, after securing the victim's financial information. In 2023, bank transfer was the most reported payment method with \$212 million in reported losses. Anti-scam interventions within the banking industry are therefore likely to be of greatest benefit to consumers.

Yet, it is evident that the Government has developed a bespoke model that rejects the model that has been implemented in the United Kingdom, where a mandatory reimbursement model for banks has been introduced for consumers. While it appears that there has been intense and ongoing consultation since 2022 with the Australian Banking Association on the Framework³, the same level of consultation has not occurred with other regulated industries about the model. Under the proposed Australian scheme, there could be a protracted examination through an external dispute resolution body of different companies' relative roles in the scammers' attack, in order to determine possible redress. Unlike the UK scheme, that could take years for any form of reimbursement for people who have lost their life savings because of the sheer number of different services scammers exploit in their complex attack chain. DIGI has included its conceptualisation of the scam attack chain in Image 1, below. **Any novel model, without international precedent, takes time to get right; it cannot be rushed into law soon after a three week consultation period in pre-election haste.** We are concerned that the Government is proposing to legislate mechanisms for consumers to be directly compensated by platforms for scam related losses without providing any necessary detail about the boundaries and circumstances in which consumer compensation would be considered appropriate, and how it might be shared across different regulated and non-regulated entities.

² April 2024, ACCC, *Targeting Scams 2023*,
<https://www.accc.gov.au/system/files/targeting-scams-report-activity-2023.pdf>

³ Documents released under the Freedom of Information Act,
<https://treasury.gov.au/sites/default/files/2024-09/foi-3675.pdf>

There is an opportunity for the Government to legislate a clear, future-proofed, economy-wide approach to combat scams. We hope DIGI's analysis of the Framework advanced in this submission will be closely considered in that effort, and we look forward to further engagement and work with you toward our shared goal of making Australia a harder target for scammers.

Best regards,



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

Image 1: A typical scam 'attack chain'

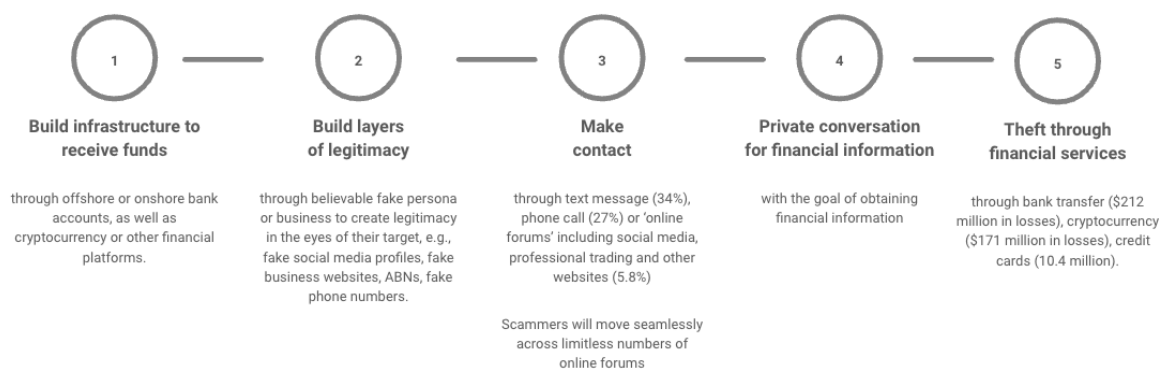


Table of contents

Image 1: A typical scam 'attack chain'	4
A. Missing elements in the legislation	6
1. Empowering the NASC to provide consumers and companies with real-time information	6
2. Global leadership to pursue scammers	7
3. Empowering the ACCC to remove non-investment scams	7
Summary of recommendations in Section A	8

B. Division 1: Scope	8
4. Scope of services	8
Social media services	8
A risk-based approach	10
Functionalities within services	10
Messaging services	11
Matters considered before designation	12
5. The definition of a scam	12
'obtaining personal information'	13
'Indirect attempt'	14
'engage an SPF consumer'	15
The impact of overcorrection	15
6. Definition of an 'SPF consumer'	15
7. Actionable scam intelligence	16
Internal thresholds of suspicion	16
Consistent application of terminology	16
8. Extraterritorial application	17
Summary of recommendations in Section B	17
C. Division 2: Overarching principles	19
9. Overarching considerations	19
Avoiding a dual-set of obligations	19
Role of sectoral codes in determining reasonable steps	20
10. SPF Principle 1: Governance	20
Obligations triggered after a single report	20
Annual certification	21
Arming scammers with unprecedented information	21
Record keeping	21
11. SPF Principle 2: Prevention	21
Mandating consumer profiling	22
12. SPF Principle 3: Detect	22
'As it happens'	22
Consumer profiling	23
Reasonable steps	23
13. SPF Principle 4: Report	23
High volumes of reports	23
14. SPF Principle 5: Disrupt	25
Reporting concerns	25
Warnings	25
Need for regulatory takedown powers	25
Safe harbour scheme	26

15. SPF Principle 6: Respond	26
Internal dispute resolution	26
External dispute resolution	26
Summary of recommendations in Section C	27
D. Division 3: Sector-specific codes	28
16. Sector specific codes are central to driving uplifts	28
Summary of recommendations in Section D	30
E. Division 4: EDR for the SPF	30
17. External dispute resolution (Division 2 & Division 4 combined)	30
Summary of recommendations in Section 3	32
F. Division 5: Regulating the SPF	32
18. The role of the ACMA for the digital platforms sector	32
Summary of recommendations in Section F	33
G. Division 6: Enforcing the SPF	33
19. Enforceable undertakings	33
20. Penalty regime	33
Summary of recommendations in Section G	34

A. Missing elements in the legislation

1. Empowering the NASC to provide consumers and companies with real-time information
 - 1.1. Outlined in this section of the submission are elements that we consider to be missing from the Framework, and the Government's wider response to scams, in order for it to be a holistic and effective approach.
 - 1.2. The Government has invested \$58 million in funding to complete the setup of the National Anti-Scam Centre (NASC) over the next two years, designed to share information across sector and disrupt scammers⁴. Yet the NASC is not mentioned in the Framework nor the Explanatory Memorandum. The Summary of Reforms indicates that 'The framework will strengthen the work of the National Anti-Scam Centre (NASC)', but it is unclear how this will be done. Consumers and companies should clearly understand the role of the NASC under the new framework. The NASC should be at the centre of an ecosystem approach, providing timely information to companies and consumers to intercept scammers' efforts.
 - 1.3. DIGI recommends that any actionable reports shared with the NASC, through the Framework or the NASC's existing operations, be used to develop a public, searchable

⁴ ACCC media release, *ACCC welcomes funding to establish National Anti-Scam*, accessible at Centre <https://www.accc.gov.au/media-release/accc-welcomes-funding-to-establish-national-anti-scam-centre>

database of known scams that consumers and companies can use to investigate whether something is a scam in real-time. The NASC is already privy to verifiable scams through its existing work – it now needs to consider how it presents the information it holds in a public-facing way, which should be the focus of the \$44 million allocated to the NASC in the federal budget for a 'technology build'⁵. Any further information obtained through the framework should aid the NASC in that effort. We note that there is some precedent to this model in the 'investor alert list' maintained by the Australian Securities and Investments Commission (ASIC) on the publicly available Moneysmart website.⁶

2. Global leadership to pursue scammers

- 2.1. Scams are increasingly a product of organised crime networks located offshore. Australians need stronger leadership and action by the Australian government and law enforcement to work with foreign governments to prosecute and disincentivise the rise of sophisticated organised crime networks that lure victims into labour conditions to conduct scams.
- 2.2. In the context of the information that would be gathered under the Framework, and through existing work from the NASC, the Government should indicate how it intends to use this information to stop scammers at the source through work with foreign governments.

3. Empowering the ACCC to remove non-investment scams

- 3.1. The exposure draft proposes a 'multi-regulator model' where multiple regulators have powers in relation to scams, yet it does not appear that any regulator can actually issue requests to take down non-investment scam content.
- 3.2. Mainstream companies, like DIGI's members and the signatories of *The Australian Online Scams Code*, have longstanding policies to remove scam content. However, gaps remain for:
 - 3.2.1. less mainstream services without such policies;
 - 3.2.2. cases where companies do not have enough information to verifiably conclude that content is a scam – in such cases, strong penalties could incentivise the removal of legitimate small business activity.
- 3.3. Today, ASIC only has takedown powers in relation to investment scam websites – and removes up to 20 scam websites a day.⁷ The Government has acknowledged the key role the ASIC takedown scheme has played in reducing scam losses on an annual basis.⁸

⁵ ACCC media release, *ACCC welcomes funding to establish National Anti-Scam*, accessible at Centre <https://www.accc.gov.au/media-release/accc-welcomes-funding-to-establish-national-anti-scam-centre>

⁶ ASIC 2024, 'Investor alert list', <https://moneysmart.gov.au/check-and-report-scams/investor-alert-list>

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>

⁸ ACCC 2024, *Targeting Scams 2023 - Observations on declining losses*, p.7 <https://www.accc.gov.au/system/files/targeting-scams-report-activity-2023.pdf>

Despite this, the legislation does not propose takedown powers for other scam types (e.g. impersonation scams).

- 3.4. DIGI urges the Government to provide the ACCC with the power to issue takedown requests to 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.
- 3.5. 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 is 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 digital and other service providers to conclusively determine if something is a scam. eSafety takedown requests therefore provide a useful complement to platforms' own work, because they can bring additional real-life context.
- 3.6. We note that there would need to be appropriate safeguards on ACCC's powers to issue takedown requests, including a requirement for takedown requests to specifically identify pieces of content and/or accounts on the recipient's service, and for the ACCC to provide a mechanism for owners of content that is removed to appeal to the ACCC if they believe the takedown request was invalid.
- 3.7. 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 overarching strategy to make Australia a harder target for scammers.

Summary of recommendations in Section A

- A. DIGI recommends that any actionable reports shared with the NASC, through the Framework or the NASC's existing operations, be used to develop a public, searchable database of known scams that consumers and companies can use to investigate whether something is a scam in real-time.
- B. In the context of the information that would be gathered under the Framework, and through existing work from the NASC, the Government should indicate how it intends to use this information to stop scammers at the source through work with foreign governments.
- C. DIGI urges the Government to provide the ACCC with the power to issue takedown requests with respect to specifically identified content and accounts associated with known scams on relevant services, expanding the current ASIC investment scam takedown scheme to other scam types (e.g. impersonation scams).

B. Division 1: Scope

4. Scope of services

- 4.1. We welcome the further refinement of sectors subject to the Framework from the proposals contained in the Consultation Paper. This section covers considerations in relation to the regulated sectors subject to the framework.

Social media services

- 4.2. We note that the Exposure Draft indicated that electronic services (within the meaning of the *Online Safety Act 2021*), such as social media services (within the meaning of that Act) may be designated. The Online Safety Act has a broad definition of social media services as those with *'the sole or primary purpose of the service is to enable online social interaction between 2 or more end-users; (ii) the service allows end-users to link to, or interact with, some or all of the other end-users; (iii) the service allows end-users to post material on the service'*.⁹

Reference material: Online Safety Act definition of 'Social Media Service'

(1) For the purposes of this Act, social media service means:

(a) an electronic service that satisfies the following conditions:

- (i) the sole or primary purpose of the service is to enable online social interaction between 2 or more end-users;
- (ii) the service allows end-users to link to, or interact with, some or all of the other end-users;
- (iii) the service allows end-users to post material on the service;
- (iv) such other conditions (if any) as are set out in the legislative rules;

or

(b) an electronic service specified in the legislative rules; but does not include an exempt service (as defined by subsection (4)).

Note: Online social interaction does not include (for example) online business interaction.

(2) For the purposes of subparagraph (1)(a)(i), online social interaction includes online interaction that enables end-users to share material for social purposes.

Note: Social purposes does not include (for example) business purposes.

(3) In determining whether the condition set out in subparagraph (1)(a)(i) is satisfied, disregard any of the following purposes:

- (a) the provision of advertising material on the service;
- (b) the generation of revenue from the provision of advertising material on the service.

Exempt services

(4) For the purposes of this section, a service is an exempt service if:

- (a) none of the material on the service is accessible to, or delivered to,

⁹ Online Safety Act 2021, see Section 13.

*one or more end-users in Australia; or
(b) the service is specified in the legislative rules.*

- 4.3. It must be underscored that there is an enormous breadth of services covered under the Online Safety Act's definition of 'social media services'. As 'social media services' is defined broadly to encompass interaction between 'two or more end users', this definition is by no means limited to large, mainstream social media services. It encompasses a wide range of services, such as local and small business community forums, educational technology, business forums, health support forums, games, news services and any blogs with comments enabled.
- 4.4. The compliance requirements required under the Framework, and the associated penalties, are not appropriate nor proportionate for this extremely wide range of services. As one example, mental health organisations operate online community forums on topics relating to anxiety and depression where Australians can share their experiences and connect;¹⁰ while it is certainly possible that a user of such a forum could post a link to entice vulnerable Australians to a scam, there are questions as to whether such an organisation should have the same extremely onerous scam reporting obligations and penalties as other digital platforms.

A risk-based approach

- 4.5. While we broadly support regulatory consistency, definitions adopted in one context may not be fit for purpose in another, and care should be taken to ensure the scope of covered services is appropriate for the purposes of the relevant legislation.
- 4.6. Given the diversity of services encompassed in 'social media services', a risk-based approach may be advanced in the sectoral codes through a framework that allows entities to assess their risk profile. There are existing such frameworks, such as within DIGI's work in the development of the Class 1 codes under the *Online Safety Act*, relating to class 1A and 1B material. Under those codes, a provider of a social media service must assess the risk posed to Australian end-users that class 1A and 1B material will be accessed, distributed, or stored on the service must determine if their risk profile is either Tier 1, Tier 2, or Tier 3.
- 4.7. Some of the factors identified in the Framework's objective assessment of 'reasonable steps' could be applied to determining a risk-based approach, such as the size of the regulated entity, the services of the regulated entity, their consumer base, and the specific types of scam risk they face may be relevant to determining their risk profile.

Functionalities within services

- 4.8. It is currently unclear whether certain functionalities of the one digital service are caught under the Framework and not others, and how the designation might apply in such services. For example, we understand that marketplaces are not intended to be designated in the first tranche of regulated entities under the Framework; that makes it unclear whether social media services with peer-to-peer marketplaces are in scope. As

¹⁰ See example: Beyond Blue, *Online forums*,: <https://forums.beyondblue.org.au/>

another example, it is unclear whether a messaging service embedded within an excluded service, such as a marketplace, would be included in the designation of 'messaging services'.

- 4.9. The designation instrument for the digital industry requires extensive and meaningful consultation with the digital industry to incorporate a risk-based approach, and the varied functionalities offered within a service. **Consideration of these matters must be brought forward ahead of the passage of the Framework** to ensure its design does not have unintended consequences.

Messaging services

- 4.10. DIGI considers that over the top messaging services are more akin to SMS/MMS, and are better regulated by the ACMA as the sectoral regulator. As detailed in Section F of this submission, we consider that the ACMA is a more well-suited regulator for digital platforms under the Framework, bringing a combination of sectoral and subject-matter expertise.
- 4.11. 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.
- 4.12. Many private messaging services are more private and secure than public communications, in line with users' heightened expectation for privacy in their private communications. Often, these services employ technology like end-to-end encryption in order to keep people safe from harms like compromise of personal information. In order to put those protections in place, the types of measures that are appropriate for combatting scams will differ for private messaging services, compared to those services with public communication. Providers of private messaging services do not have the same level of visibility over content, data and context when compared to public services. Crucially, this level of visibility (whether by government or the service provider) is in line with consumer expectation for a private messaging service.
- 4.13. DIGI is concerned that the obligations set out in the principles-based obligations in the Framework may not all be readily applicable to messaging services in areas such as content removal. Clarification in the legislation and/or sectoral codes should be provided to clearly indicate that the following measures would not be 'reasonable steps':
 - 4.13.1. implement or build a systemic weakness, or a systemic vulnerability, into a form of encrypted service or other information security measure;
 - 4.13.2. render methods of encryption less effective;
 - 4.13.3. build a new decryption capability in relation to encrypted services;
 - 4.13.4. undertake monitoring of private communications.
- 4.14. On the latter point, 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 Australians¹¹.

Matters considered before designation

- 4.15. s58AE indicates that the Minister may consider a range of factors before designating sectors, including 'scam activity in the sector' and 'the effectiveness of existing industry initiatives to address scams in the sector'.
- 4.16. We expect that these assessments will be made from data provided from the ACCC via its *Targeting Scams* reports, which are premised on consumer reports through its Scamwatch 'report a scam' portal¹². If that is the case, DIGI is extremely concerned that assessments about scam activity in the digital industry are not premised on disaggregated data collection, a matter that we have raised publicly¹³ and raised with the National Anti Scam Centre (NASC) and other relevant Government departments.
- 4.17. Public commentary on scams originating from 'social media' continue to be premised on ACCC data collected from consumer reports about 'online forums', which include social media sites, some online trading sites, professional forums, and online dating sites. Scams whereby the contact method was an 'online forum' represented 5.8% of contacts among 2023 reports, of which 'social media' remains a quantifiably unknown subset. Furthermore, there are separate categories for 'mobile apps' and 'internet', which would further confuse any data collected by this means.
- 4.18. If the Government seeks to properly evaluate the effectiveness of the Framework, and associated activities on regulated entities, it must improve data collection about the digital industry. The ACCC is urged to make modifications to the options presented to consumers reporting a scam to rectify the ongoing opacity around the data collection on the digital industry in relation to scams, which is serving other industries that seek to over-index on its role as a scam vector in the ecosystem.

5. The definition of a scam

- 5.1. 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.

¹¹Resolve Strategic (2022), *Consolidated Industry Codes of Practice for Online 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 ACCC, *Report a scam*, <https://www.scamwatch.gov.au/report-a-scam>

¹³ Bose, Sunita (2/8/24), *Blame game won't protect Australians from scams*, <https://www.innovationaus.com/blame-game-wont-protect-australians-from-scams/>

- 5.2. DIGI is concerned that the current definition, as set out below, does not provide this clarity, and is therefore overbroad and difficult to operationalise:

58AG Meaning of scam

(1) A scam is a direct or indirect attempt to engage an SPF consumer of a regulated service that:

(a) involves deception (see subsection (2)); and

(b) would, if successful, cause loss or harm including obtaining personal information of, or a benefit (such as a financial benefit) from, the SPF consumer or the SPF consumer's associates.

- 5.3. We consider the Commonwealth Fraud Control Policy (CFCP)¹⁴ 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'.

- 5.4. 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.

- 5.5. However, we recognise that the intention may be to include scams where consumers do not engage. To that end, in DIGI's AOSC, a scam is defined as:

an invitation, request, notice or offer by a person with the purpose of deceiving another person in order to obtain a financial benefit or cause a financial loss¹⁵.

DIGI recommends refining the definition of a scam in line with this definition.

- 5.6. It is also worth acknowledging that definitions of scams in sectoral codes may vary, depending on the role of the sector in a typical scam lifecycle. For example, in the Communications Alliance's *Reducing Scam Calls and Scam SMS 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).¹⁶ 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. The latter scenario would be a more responsive, flexible, and efficient method for dealing with a dynamic threat environment that is subject to change.

¹⁴Attorney General's Department (2017), *Commonwealth Fraud Control Framework*, <https://www.ag.gov.au/sites/default/files/2020-03/CommonwealthFraudControlFramework2017.PDF>

¹⁵ DIGI, *The Australian Online Scams Code*, www.digi.org.au/scams

¹⁶ 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

'Obtaining personal information'

- 5.7. DIGI notes that the Exposure Draft's definition of a scam includes the obtainment of personal information. We assume that proposed definition's inclusion of 'personal information' refers to the Privacy Act, where personal information is defined as:

*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.'*¹⁷

- 5.8. We are concerned that the inclusion of personal information, irrespective of whether a financial benefit has occurred, dramatically expands the scope of the Framework beyond the Government's intention.
- 5.9. 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. In the Summary of Reforms, the intention is stated to not include data breaches, however our interpretation is that these are caught in scope. 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.
- 5.10. Including personal information significantly 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.
- 5.11. 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. 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.
- 5.12. DIGI recommends the removal of 'personal information' from the definition of a scam, and a greater focus on the obtainment of financial benefit.
- 5.13. Alternatively, at a minimum, the second 'or' in 58AGb should be replaced with 'and' so as to read: 'would, if successful, cause loss or harm including obtaining personal information and a benefit (such as a financial benefit)... '.

¹⁷OAIC (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%20personal,a%20material%20form%20or%20not.>

'Indirect attempt'

- 5.14. DIGI questions the inclusion of 'indirect attempt' in the definition of a scam. We also note that 'indirect attempt' was not advanced in the Treasury's Consultation Paper, and seek to better understand its inclusion by way of examples of what this is considered to mean, as such examples do not appear in the Explanatory Memorandum.
- 5.15. We consider that this inclusion further broadens and confuses the definition of a scam, and propose its removal, in order to ensure precision and implementability by industry participants.

'Engage an SPF consumer'

- 5.16. King Wood Mallesons published legal analysis of the Framework notes that the reference to 'engage an SPF consumer' in the definition of a scam appears to have the effect that each communication to a consumer may be considered a separate scam, even if various communications are associated with the one scammer¹⁸. This should be clarified in updates to the definition.

The impact of overcorrection

- 5.17. The broad definition of a scam makes it extremely difficult for the digital industry to operationalise, without considerable overcorrection. Taken together with the penalty regime, where penalties are up to the greater of \$50 million or 30 percent of global revenue, this will see services err on the side of content removal, at the expense of potentially harming legitimate businesses activity. This would likely have an outsized impact on small enterprises and businesses due to the key role digital services often play in small business marketing and daily operations. While the proposed safe harbour offers a level of protection for regulated entities, it does not address the underlying issue of potential impact on legitimate business activity or offer protections for small businesses that will be impacted.
- 5.18. 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, we expect that the Framework will result in a substantial increase in platforms over-correcting to avoid the risk of significant penalties. 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.
- 5.19. Further refinement of the definition of a scam, and throughout the Framework, must be applied to protect legitimate small and other businesses that are inadvertently impacted by regulated entities' scam activities.

¹⁸King Wood Mallesons, *Unpacking the scams prevention framework: what you need to know*, <https://www.kwm.com/au/en/insights/latest-thinking/unpacking-the-scams-prevention-framework.html>

6. Definition of an 'SPF consumer'

- 6.1. DIGI has concerns that the definition of an 'SPF consumer' applies to Australian citizens and residents anywhere in the world, as well as non-Australians in Australia. In practice, this may mean that entities must apply the Australian principles to Australians anywhere in the world as well as non-Australian consumers who are merely travelling or passing through Australia. Under the current definition, entities that do not actively track their consumers' locations might need to do so in order to determine if they were in Australia at the time of the scam.
- 6.2. The definition of an 'SPF consumer' in s58AH(1) should be modified to:
 - 6.2.1. require that an 'SPF consumer' be geographically in Australia; and
 - 6.2.2. exclude a natural person who 'is in Australia' to ensure that the Framework focuses on persons ordinarily resident in Australia, permanent residents of Australia and Australian citizens, and Australian small businesses, rather than persons who are merely visiting or travelling through Australia.

7. Actionable scam intelligence

Internal thresholds of suspicion

- 7.1. DIGI is concerned that the definition of 'actionable scam intelligence' does not set a high enough threshold for action under the Framework in response to such intelligence.
- 7.2. Specifically, the drafting of the legislation may mean that an entity has 'actionable scam intelligence' if it has a single consumer report about an alleged scam. This is specifically acknowledged in the note accompanying the definition which states the relevance of 'information (including complaints) provided by SPF consumers'. This is further complicated by the objective test whereby, rather than a requirement to have formed a view that content is a scam, the test is whether it is reasonable in the circumstances for the regulated entity to form a suspicion that content is a scam.
- 7.3. While user reports are an important source of information to digital platforms in relation to possible scams, they are not consistently accurate.
- 7.4. In fact, reporting tools are commonly abused. As an example, bad actors in the USA weaponised copyright law to harm competitors by submitting thousands of bogus takedown reports on Google Search, which resulted in over 100,000 business websites being removed.¹⁹
- 7.5. If obligations to act on scam reports are retained, they must be limited to scams that meet internal thresholds of suspicion, as opposed to all scam reports made by consumers. Under the DSA, for example, notices provided by consumers to a hosting service will lead to an obligation to act to remove or disable access to content only 'where they allow a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination'.²⁰ We recommend

¹⁹ Google Keyword (blog), *Taking legal action to protect users of AI and small businesses*, <https://blog.google/outreach-initiatives/public-policy/taking-legal-action-to-protect-users-of-ai-and-small-businesses/>

²⁰ Art.16(3), *Digital Services Act*, <https://www.eu-digital-services-act.com/>

comparable thresholds. Additionally, it should be made clear that a regulated business will not be exposed to penalties or consumer claims (or other liability) if it does not act on an individual report.

Consistent application of terminology

- 7.6. The concept of 'actionable scam intelligence' is only referenced in the Exposure Draft in a limited number of instances compared to references to 'scams', which has the broad definition previously discussed.
- 7.7. With the addition of 'internal thresholds for suspicion' as outlined above, the concept of 'actionable scam intelligence' should be called out extensively throughout the principles in Division 2 as the threshold point at which an entity has obligations to act.

8. Extraterritorial application

- 8.1. It is unclear how the Framework is intended to apply outside Australia. Section 58AJ provides that the provisions 'apply to acts, omissions, matters and things outside Australia'. As King Wood Mallesons notes in their analysis of the Framework, the standard Competition and Consumer Act extraterritoriality provisions that limit the operation of the extended jurisdiction to bodies corporate incorporated in or carrying on business in Australia are not being amended to apply to the SPF provisions²¹.
- 8.2. DIGI's members operate globally. Digital platforms respect the laws in which they operate by providing slightly different services or content in each jurisdiction. We are concerned that the Framework and particularly the definition of SPF consumer might require regulated entities to alter the services they provide anywhere in the world. We recommend that the Framework be amended to more specifically set out the intended extraterritorial operation.

Summary of recommendations in Section B

- D. Given the diversity of services encompassed in 'social media services', a risk-based approach may be advanced in the sectoral codes through a framework that allows entities to assess their risk profile.
- E. The designation instrument for the digital industry requires extensive and meaningful consultation with the digital industry to enable a risk-based approach, and the varied functionalities offered within a service.
- F. As detailed in Section F of this submission, we consider that the ACMA is a more well-suited regulator for digital platforms in general, bringing both sectoral and subject-matter expertise to

²¹ King Wood Mallesons, *Unpacking the scams prevention framework: what you need to know*, <https://www.kwm.com/au/en/insights/latest-thinking/unpacking-the-scams-prevention-framework.html>

the Framework. DIGI considers in particular that over the top messaging services are more akin to SMS/MMS, and are better regulated by the ACMA as the sectoral regulator.

- G. Clarification in the legislation should be provided to clearly indicate that obligations on messaging services do not require service providers to implement or build a systemic weakness, or a systemic vulnerability, into a form of encrypted service or other information security measure; render methods of encryption less effective; build a new decryption capability in relation to encrypted services; or undertake monitoring of private communications.
- H. The ACCC is urged to make modifications to the options presented to consumers reporting a scam to rectify the ongoing opacity around the data collection relating to the digital industry, which is serving other industries that seek to over-index on its role as a scam vector in the ecosystem.
- I. The proposed definition of a 'scam' is overly broad and should be clarified to ensure the legislation can be effectively operationalised by businesses by:
 - a. More closely aligning the definition of a scam with the Commonwealth Fraud Control Policy (CFCP) definition of 'fraud'.
 - b. Should the intention be to include scams where consumers do not engage, aligning the definition more closely with the definition of a scam advanced in the Australian Online Scams Code (AOSC).
 - c. Removing 'personal information' from the definition of a scam, and a greater focus on the obtainment of financial benefit.
 - d. Alternatively, at a minimum, the second 'or' in 58AGb should be replaced with 'and' so as to read: 'would, if successful, cause loss or harm including obtaining personal information and a benefit (such as a financial benefit)...'.
- J. The reference to 'engage an SPF consumer' in the definition of a scam appears to have the effect that each communication to a consumer may be considered a separate scam, even if various communications are associated with the one scammer. This should be clarified in updates to the definition.
- K. The definition of an 'SPF consumer' in s58AH(1) should be modified to:
 - a. require that an 'SPF consumer' be geographically in Australia (see related recommendation below on the intended extraterritorial operation of the Framework); and
 - b. exclude a natural person who 'is in Australia' to ensure that the Framework focuses on persons ordinarily resident in Australia, permanent residents of Australia and Australian citizens, and Australian small businesses, rather than persons who are merely visiting or travelling through Australia.
- L. The definition of 'actionable scam intelligence' should be modified to set a higher threshold for action under the Framework in response to such intelligence. If obligations to act on scam

reports are retained, they must be limited to scams that meet internal thresholds of suspicion, as opposed to all scam reports made by consumers.

- M. With the addition of 'internal thresholds for suspicion' as outlined above, the concept of 'actionable scam intelligence' should be called out extensively throughout the principles in Division 2 as the threshold point at which an entity has obligations to act.
- N. We recommend that the Framework be amended to more specifically set out the intended extraterritorial operation.

C. Division 2: Overarching principles

9. Overarching considerations

Avoiding a dual-set of obligations

- 9.1. The overarching principles of the Framework are civil penalty provisions. DIGI understands that the sectoral codes, to be established as subordinate legislation, will also be civil penalty provisions. This creates a complex, dual framework that complicates regulated entities' understanding of their compliance obligations. DIGI believes that sector-specific obligations will be sufficient in creating clarity and lifting the bar on anti-scam efforts 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, that need to be drafted to apply to highly disparate sectors.
- 9.2. The principles-based obligations under the Framework are wide-ranging, and arranged in a structure that mirrors the banking sector's voluntary code *The Scams Safe Accord* ('Disrupt', 'Detect', 'Respond') with the addition of 'prevent' and 'report'. As noted, there is a risk that such a prescriptive framework in the overarching legislation will limit the ability of the Government to bring in other sectors it intends to have legislated under the Framework in future, which the Consultation Paper indicates are intended to be superannuation funds, digital currency exchanges, other payment providers, and transaction-based digital platforms like online marketplaces.
- 9.3. The Explanatory memorandum states that the '*designation mechanism supports a responsive and adaptable approach for the SPF as scams shift and evolve over time. A legislative instrument can be made quickly to bring vulnerable sectors into the SPF and consequently require regulated entities in the regulated sectors to uplift their anti-scam practices.*' The nature of the overarching principles constrain the Government's intention to bring in vulnerable sectors; Division 2 is already an inapplicable model for the three existing sectors, and would not readily apply to future sectors.
- 9.4. We understand from earlier consultations in relation to the Consultation Paper that the 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. DIGI considers that these same four

objectives could be met through more refined amendments to CCA to empower relevant regulators to:

- 9.4.1. enable the designation of applicable sectors;
- 9.4.2. direct a company to adopt an existing industry code, or for it to develop an equivalent;
- 9.4.3. empower the relevant regulator with code and standard-making powers, or oversight powers over industry-led codes;
- 9.4.4. empower the relevant regulator with information gathering powers in relation to scams. For example, the operation of the Basic Online Safety Expectations (BOSE) under the Online Safety Act may provide a useful model to explore.

We therefore recommend that the Framework focus on amendments to the CCA in these areas. We are confident that these objectives can be met without establishing a secondary set of obligations, and a secondary regulator, and a secondary penalty regime.

Role of sectoral codes in determining reasonable steps

- 9.5. The Framework contains a set of unclear obligations with penalties that hinge on varying interpretations – by companies, consumers, regulators, an EDR Scheme, and Courts – of the concept of 'reasonable steps'. Currently, a company can be in breach of the overarching legislation while complying with all of the obligations in its mandatory sectoral code. 'Reasonable steps' must be outlined in mandatory sector-specific codes; this will also ensure obligations are well-suited to the industries to which they apply.
- 9.6. The Framework contains several obligations that require regulated entities to take 'reasonable steps'. It would be extremely burdensome for regulated businesses if their compliance with the obligations was open to challenge by individuals, or organisations beyond the responsible regulator. For example, regulated services could be exposed to potentially a huge number of claims about whether they complied with obligations to have appropriate strategies for preventing, detecting, reporting, disrupting and responding to scams. Such disputes would likely also require the disclosure of commercially sensitive information about platforms' internal strategies and systems in discovery processes. It would be extremely concerning, and counterproductive to industry's efforts to combat scams, if this type of detailed information was made public.
- 9.7. If the Government intends for individuals to be able to bring claims for compensation for scams losses, the scope of the obligations on regulated entities must first be clarified within the sectoral codes. This is why we consider that the model for consumer claims is best addressed through the code development process. The sectoral codes provide the opportunity for necessary details and consideration of the obligations in respect of which such claims should be capable of being brought, taking into account issues such as burden on businesses, impact on courts and ombuds schemes, proportionality, and the sensitivity of confidential information about how businesses combat scams. The consideration of these factors cannot be rushed into law soon after a three week consultation period in pre-election haste, and must be done through the mandatory sectoral code development processes.

10. SPF Principle 1: Governance

Obligations triggered after a single report

- 10.1. Does the appearance of a single scam on an entity's service, prior to its removal under associated policies, constitute a failure to 'implement policies'? This is a critically important question that must be answered in response to this consultation. Currently, under s58BC, it would appear that any regulated entity may be in contravention of this civil penalty provision, prior to any anti-scam action taken. The liability of regulated services at the point at which a scam surfaces, prior to action, must be clarified. For example, it is unclear whether each time a consumer reports a message as spam if that must be reported.

Annual certification

- 10.2. Under s58BE, a regulated entity contravenes the provision if a senior officer does not certify in writing, within seven days of the financial year, that an entity's SPF governance policies, procedures, metrics and targets comply with all of the principles. Given the vastly open-ended nature of the provisions – and the ambiguous position regulated entities face if a single scam or a single consumer report appears – this sort of certification places the officer in an untenable position, and should be removed. If this requirement is to be retained, the Government should specify that there is an express exclusion of individual liability of the senior officer.
- 10.3. Any requirements around financial years need to recognise that non-Australian companies do not operate to the Australian July 1-June 30 financial year, and should be tied to the entity's financial year.

Arming scammers with unprecedented information

- 10.4. s58BF requires regulated entities to make publicly accessible the measures they have in place to protect consumers from scams; this should be amended to indicate that a regulated entity meets their obligations by publicly stating that there are enforced policy restrictions on scams. As currently drafted, the requirement to detail measures across the wide range of services caught by the definitions of the digital industry sectors intended to be designated will arm scammers with an unprecedented amount of information that they can use to circumvent these measures. It is important to emphasise that consumers are also unlikely to read these reports – they will instead be read by scammers.

Record keeping

- 10.5. s58BG's record-keeping requirements, to retain records for six years, may not be proportionate to the wide range of regulated entities, especially taken together with the requirement in s58BH to produce such records to the regulator within five days. There also needs to be flexibility and proportionality about the form that these reports take, for example, if an entity's volume of 'actionable scam intelligence' is low, then record-keeping needs to be adjusted proportionately. Entities also need to understand the criteria for why

a regulator may demand these reports.

11. SPF Principle 2: Prevention

- 11.1. Knowledge of a scam is usually 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, the standard of 'prevention' is not attainable in all cases. 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 industry codes. While many scams will be prevented through the deployment of technology and verification measures, scams must appear in the first place for them to be reported. Again, we consider that the 'reasonable steps' required under this provision, and others, should be determined through the details of the sectoral codes.
- 11.2. For the digital industry, it is unclear how the prevention principle in 58BJ applies outside of advertiser verification measures. As not all social media services or messaging services offer advertising, in DIGI's AOSC, we have created specific provisions for services that offer paid advertising that serve the goal of prevention.
- 11.3. The Government might consider a 'safe harbour' for the Prevent mechanism, where a company has been required to make changes to their processes in order to comply with other Australian or other regulation.

Mandating consumer profiling

- 11.4. Under s58BK, a regulated entity contravenes the provision if it fails to take reasonable steps to identify the classes of consumers who have a higher risk of being targeted by a scam, and provide warnings to them. This provision is mandating consumer profiling; it is unclear on what basis an entity would make determinations of consumers more vulnerable to scams, and if this requires the appending of generalised demographic information about scam susceptibility in the wider community; a prospect that raises a number of questions in relation to the Privacy Act, and proposed privacy act reforms in relation to inferred data, and possible restrictions on the act of 'data appending'. Further, the privacy implications are heightened as these could involve processing sensitive categories of personal information. Adhering to good principles of data minimisation may preclude entities from such profiling, and meeting this obligation. Furthermore, this requirement may not be proportional to the wide range of digital industry entities in scope of the regulation.
- 11.5. Additionally, the proposal to warn users raises feasibility questions. There are logistical barriers in relation to the appropriate placement of such warnings on digital services, and whether warnings are required in relation to the myriad of different scams that may be in community circulation at any given time – this will result in 'warning fatigue' where consumer attention to these notices is limited.

12. SPF Principle 3: Detect

'As it happens'

- 12.1. DIGI is concerned about the standard set in s58BN where a regulated entity fails to take reasonable steps to detect a scam if they fail to detect a scam 'as it happens'. It is wholly unclear to DIGI how an entity detects a scam as it happens. The technical capacity for this has not been determined for the digital industry, as any 'detection' of scams as a contact method usually requires at least one dissemination of the message; it will always be in the 'after it happens' category that is included in the Exposure Draft. 'As it happens' should be removed from s58BN.
- 12.2. We question the proportionality of some of the detection and disruption measures for services where the incidence of scams is low. Building effective detection technology is a heavy technological lift and the cost to implement effective proactive detection of scams may be prohibitive for small and mid-sized services.

Consumer profiling

- 12.3. DIGI is also concerned about the requirement in this provision to identify consumers who have been 'impacted by a scam', and the provision in s58BO to 'to identify each SPF consumer of that service who is or could be impacted by the suspected scam'. In the context of the digital industry, it is unclear whether 'impact' relates to exposure, engagement or financial loss; this is even further complicated by the addition of 'could be impacted'. More broadly, the focus on identifying consumers, rather than scam content, is misplaced and leads to more data collection about consumers.

Reasonable steps

- 12.4. The standard in 58BO 'fails to take reasonable steps within a reasonable time' is inherently subjective, and is likely to lead to disagreements between individuals and companies around what they consider that they are undertaking reasonable steps. This underscores the importance of cross-referencing the sectoral codes as the clear description of what 'reasonable steps' entails. While we acknowledge that s58BP indicates that sector-specific details can be set out in SPF codes, entities can still be in breach of overarching principles while meeting the obligations set out in sectoral codes.

13. SPF Principle 4: Report

High volumes of reports

- 13.1. DIGI is concerned that this principle establishes extremely onerous reporting requirements across a wide range of digital services, without a pathway for how the reporting will benefit Australian consumers. Under the Framework, entities face penalties of at least \$10 million if they do not share information about *potential* scams with the

regulator, which will inundate the ACCC with millions of reports about scams. It is unclear what the ACCC will do with all of that information, how they will receive it, and how they will use it to inform consumers about potential scams. Specifically, we are concerned about the inclusion of 'potential' in relation to this requirement when it is described in the Explanatory Memorandum.

- 13.2. DIGI is concerned that an entity may have 'actionable scam intelligence' if it has a single consumer report about a scam. This is specifically acknowledged in the note accompanying the definition which states the relevance of 'information (including complaints) provided by SPF consumers'. Taken with the requirement in 58BR, where a regulated entity contravenes the subsection if it fails to provide the regulator with a report of 'actionable scam intelligence', this implies that regulated entities may have to provide every consumer report of a scam to the regulator. This will see millions, if not billions, of reports being made to the ACCC from the digital industry alone, let alone other regulated entities. Digital platform services are managing content complaints at an extremely large scale, and cannot reasonably share information about all scam reports, unless there is a clearly articulated threshold of the type of report the regulator requires in order to take action.
- 13.3. It is also important to underscore that the resources required for reporting take away resources from the teams who are focused on rapidly disrupting scams; incessant documentation and information sharing will slow those teams down, and will divert resources from where they are most needed, particularly during rapid response moments.
- 13.4. Furthermore, it is also unclear whether these reports need to be shared continuously with the regulator, or whether they can be batched around time periods. s585X3 and 58BZ2(d), relating to the 'disrupt' set of obligations, indicates that reports of actionable scam intelligence should be provided to the regulator 24 hours after the closure of the 28-day safe harbour period. It is unclear whether the reports required under the 'report' set of obligations must align with the timetable in s585X3, and whether 'report' requirements are intended to be broader in scope.
- 13.5. Reporting obligations may involve the disclosure of personal information of non-Australians, and may therefore enter into conflict with international privacy laws applicable to regulated entities that will restrict reporting. The obligation to report actionable scam intelligence to the regulator may come in tension, or even in direct conflict, with provisions of the U.S. Stored Communications Act, which limits platforms' ability to disclose user data with foreign regulators. Most concerning in this context is the reference in s58BS(3) to the potential disclosure to the SPF regulator of personal information.
- 13.6. Should such any reporting be retained in the primary legislation, the Government must work with industry to understand constraints and determine feasible technical and operational details of industry's expected reporting arrangements, before this requirement is legislated.
- 13.7. This work with industry must also include operational details for the receiving mechanism from the ACCC to receive these reports. The details must go beyond ambiguous preferences for industry to develop a 'consistent taxonomy' around scams reporting. The development of a consistent taxonomy to automate the arrangement of

millions of scams reports across the ACCC, and all regulated sectors – particularly those that are global in nature, operating in multiple languages – is wishful thinking.

- 13.8. Appropriate and effective reporting requirements should be developed after more extensive consultation with regulated entities through the mandatory code development processes, and can be reflected in subordinate legislation relating to the mandatory codes.
- 13.9. Should any reporting requirements be retained in the primary legislation, they must be scaled back considerably for practicality. Additionally, the notifiable instrument noted in s58BS that determines the kinds and the form of the reports must undergo extensive industry consultation.
- 13.10. For example, such consultation would enable service providers to reconcile their competing obligations under the Privacy Act, with the requirements in s58BS3 that suggest reports could include the personal information of people who engage with and report scams, as well as those who perpetrate them.

14. SPF Principle 5: Disrupt

Reporting concerns

- 14.1. In relation to 'disrupt', we reiterate the concerns articulated above in relation to the 'report' section of reporting obligations. Taken together, this is an extreme volume of industry reporting.
- 14.2. It also illustrates the duplicative nature of the structure of the Division 2 of the Framework. There are reporting requirements to the regulator under 'report' and reporting requirements under s58BX2b.

Warnings

- 14.3. It appears that this section creates an additional obligation to warn potentially all users of a regulated entity about a possible scam. Under s58BX, a regulated entity contravenes the subsection if the entity 'fails to take reasonable steps within a reasonable time to disclose to SPF consumers of the regulated service sufficient information to enable those consumers to act in relation to the suspected scam'. It is unclear to DIGI how this obligation differs from the obligation under s58BK, which provides that a regulated entity contravenes the provision if they fail to take reasonable steps to identify the classes of consumers who have a higher risk of being targeted by a scam, and provide warnings to them. s58BX then implies that warnings must be provided to *all users* as opposed to classes of users determined to be at higher risk; both requirements are extremely problematic.
- 14.4. It is also unclear why these two similar obligations appear in different sections, which speaks to limitations in the structure of Division 2.
- 14.5. As noted previously, proposals to warn users about all scams in the digital industry raise feasibility questions. There are logistical barriers in relation to the appropriate placement

of such warnings on digital services, and whether warnings are required in relation to the myriad of different scams that may be in community circulation at any given time – this will result in ‘warning fatigue’ where consumer attention to these notices becomes limited.

Need for regulatory takedown powers

- 14.6. In addition, we underscore the need for the ‘disrupt’ efforts to be bolstered through regulatory powers to issue takedown requests, which would support industry in making accurate determinations as to what constitutes a scam, without undue impact on legitimate business activity. As detailed in Section A3 of this submission, DIGI urges the Government to provide the ACCC with wider powers to issue takedown requests of known scams on relevant services. 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 is 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. eSafety takedown requests therefore provide a useful complement to platforms’ own work, because they can bring additional real-life context. 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.

Safe harbour scheme

- 14.7. As noted, while the proposed safe harbour offers a level of protection for regulated entities, it does not offer protections for small businesses that will be impacted. It is insufficient in addressing the risks to legitimate business activity created by overcorrection by entities in earnest efforts to comply with the standards in the Framework.
- 14.8. The explanatory memorandum states that ‘Once the regulated entity concludes that the website has not been used for scam activities, the regulated entity must reverse its actions promptly to minimise disruption to the business’. It is unclear how the regulated entity would be able to effectively reverse any erroneous decisions.
- 14.9. This is also a limited safe harbour in Australia that does not cover claims against regulated entities in other jurisdictions. While a safe harbour is welcome, it must be coupled with more targeted definitions and refined obligations to mitigate error before it occurs; this will allow for diligent anti-scam action driven by legitimate suspicion rather than overcorrection driven by fear of penalties.

15. SPF Principle 6: Respond

Internal dispute resolution

- 15.1. DIGI is supportive of s58BZB that requires regulated entities to have an accessible mechanism for consumers to report scams relating to their service.

- 15.2. Along with other obligations in Division, we suggest that this provision be further explored in subordinate legislation for sectoral codes; this would serve to enable the reconciliation of this effort with the Government's broader intent and parallel workstreams in the area of internal dispute resolution.

External dispute resolution

- 15.3. DIGI's concerns about the Framework's External Dispute Resolution are detailed in Section E of submission, relating to Division 4.

Summary of recommendations in Section C

- O. Rather than setting out an additional set of provisions with penalties, DIGI considers that the Government's objectives can be met through more refined amendments to CCA to empower relevant regulators to:
- a. Enable the designation of applicable sectors;
 - b. direct a company to adopt an existing industry code, or for it to develop an equivalent;
 - c. empower the relevant regulator with code and standard-making powers, or oversight powers over industry-led codes;
 - d. empower the relevant regulator with information gathering powers in relation to scams.
- P. 'Reasonable steps' therefore must be outlined in mandatory sector-specific codes; which will also ensure obligations are well-suited to the industries to which they apply.
- Q. Following our preference for all obligations to be set out in the mandatory codes, DIGI urges the following refinements to obligations, regardless of whether they sit in the codes or the primary legislation:
- a. The liability of regulated entities at the point at which a scam surfaces, prior to action, must be clarified.
 - b. Given the vastly open-ended nature of the provisions – and the ambiguous position regulated entities face if a single scam or a single consumer report appears – the certification requirement under s58BE places the senior officer in an untenable position, and should be removed.
 - c. If this requirement under s58BE for certification by a senior officer is retained, the Government should specify that there is an express exclusion of individual liability of the senior officer.
 - d. Any requirements around financial years need to recognise that non-Australian companies do not operate to the Australian July 1-June 30 financial year, and should be tied to the entity's financial year.
 - e. s58BF requires regulated entities to make publicly accessible the measures they have in place to protect consumers from scams; this should be amended to indicate that a regulated entity meets their obligations by publicly stating that there are enforced

policy restrictions on scams to avoid a counter-productive situation where bad actors are able to leverage published information to circumvent anti-scam measures.

- f. s58BG's record-keeping requirements, to retain records for six years, may not be proportionate to the wide range of regulated entities, especially taken together with the requirement in s58BH to produce such records to the regulator within five days, and should be reconsidered.
- g. There also needs to be flexibility and proportionality about the form that any reports take, for example, if an entity's volume of 'actionable scam intelligence' is low, then record-keeping needs to be adjusted proportionately. Entities also need to understand the criteria for why a regulator may demand reports.
- h. The Government might consider a 'safe harbour' for the Prevent mechanism, where a company has been required to make changes to their process to comply with other regulation.
- i. The requirement under s58BK to identify the classes of consumers who have a higher risk of being targeted by a scam, and provide warning to them, should be removed for both privacy and practicality reasons.
- j. The standard set in s58BN where a regulated entity fails to take reasonable steps to detect a scam if they fail to detect a scam 'as it happens' should be removed to recognise that any 'detection' of scams as a contact method usually requires at least one dissemination of the message, so will always be 'after it happens'.
- k. The provision in s58BO to 'to identify each SPF consumer of that service who is or could be impacted by the suspected scam' should be removed for privacy and practicality reasons.
- l. The provision in s58BX to disclose to SPF consumers of the regulated service sufficient information to enable those consumers to act in relation to the suspected scam' should be removed for privacy and practicality reasons.
- m. Should any reporting be retained in the primary legislation, the Government must work with industry to understand constraints and determine feasible technical and operational details of industry's expected reporting arrangements, before this requirement is legislated. If that cannot occur in the Government's timeline, the reporting requirements should be removed.
- n. The notifiable instrument noted in s58BS that determines the kinds and the form of the reports must undergo extensive industry consultation.
- o. While a safe harbour is welcome, it must be coupled with more targeted definitions and refined obligations to mitigate error before it occurs.
- p. We suggest that s58BZC be further explored in subordinate legislation for sectoral codes; this would serve to enable the reconciliation of this effort with the Government's broader intent, by way of its February 2024 request to the digital industry, for work in the area of internal dispute resolution.

D. Division 3: Sector-specific codes

16. Sector specific codes are central to driving uplifts

- 16.1. As noted previously, DIGI is supportive of sector-specific codes in creating greater accountability for relevant industries to uplift their anti-scam activities.
- 16.2. In the development of its voluntary code, DIGI has sought to create alignment, and avoid duplicative consultation processes, with forthcoming mandatory codes. The code's scope reflects the Government's Federal Budget announcement to include social media services, paid search engine advertising and direct messaging. DIGI also considered it important to include further categories and additional services, such as social media services with peer-to-peer marketplaces, and email.
- 16.3. DIGI wrote to the Government on February 22, 2024, to advise that we were commencing work to develop a scams code of practice for the digital industry, now known as the AOSC. That letter indicated that we sought a co-development approach involving the digital industry and Government, seeking close and ongoing consultation with relevant offices, departments and portfolio agencies.
- 16.4. DIGI sought to obtain input from the relevant Minister's Offices, and Departments, via a series of workshops, meetings and correspondence between February and July 2024. A draft of the code was provided for feedback on June 21, 2024, after which no specific edits nor measures were requested. At no time did the Government advise the code did not meet community expectations. In the absence of formal feedback, DIGI finalised the code and instructed industry representatives to consider its adoption. DIGI wrote to the Government July 16, 2024 with the final version of the code, and launched it publicly on July 26, 2024.
- 16.5. On July 26, 2024, DIGI was surprised to read the Assistant Treasurer's public comments that the code 'falls short of what is needed and what is expected by the Australian community'²². Further, on August 26, 2024, the Assistant Treasurer described the code as a 'document full of weasel words that impose no obligations, really doesn't provide any uplift for consumers, for consumer safety'²³. Concerns that the code did not meet community expectations were not provided directly to DIGI during the ample opportunities we provided for feedback before the code's finalisation. As such, the

²²InnovationAus (26/7/24), *Platforms' scam code 'falls short' of \$2.7b problem*, <https://www.innovationaus.com/platforms-scam-code-falls-short-of-2-7b-problem/>

²³ The Daily Telegraph (26/8/24) *How Australians are being conned of almost \$3bn a year through scams*, <https://www.dailytelegraph.com.au/truecrimeaustralia/how-australians-are-being-conned-of-almost-3bn-a-year-throu-gh-scams/news-story/136c47ba506cc4a20f74bfa0bc4456e4>; see also The Australian (26/8/24), *Albanese government concern over tech sector response to scams and fraud*, <https://www.theaustralian.com.au/business/technology/albanese-government-concerned-over-tech-sectors-weak-res-ponse-to-scams-and-fraud/news-story/41d201dcf714e0152bba42e0ff6ff89c>

expectations for such a code remain unclear to DIGI, particularly when the AOSC contains specific measures that the Assistant Treasurer have been publicly stated to be needed²⁴.

- 16.6. DIGI has always worked to advance the Government's eventual intention to introduce mandatory scams codes, we are unclear about the measure by which it was determined that the digital industry's voluntary code did not meet expectations, and that the banking sector's voluntary scams code should be welcomed through a media release²⁵ and event²⁶.
- 16.7. Nonetheless, DIGI will continue to work constructively and collaboratively across Government and with the digital industry to make Australia a harder target for scammers. The AOSC provides an implementable and globally interoperable model that we recommend the Government draw upon in developing the mandatory sectoral digital industry code, and DIGI stands ready to contribute our extensive expertise to this effort.

Summary of recommendations in Section D

- R. The Government should work with DIGI in the development of the mandatory digital industry sectoral code, and draw upon the model provided in the Australian Online Scams Code.

E. Division 4: EDR for the SPF

17. External dispute resolution (Division 2 & Division 4 combined)
 - 17.1. DIGI, along with many other stakeholders, has serious questions about the Framework's proposed External Dispute Resolution (EDR) scheme. In this section of the submission, we also detail concerns relating to the broader EDR scheme reflected in Division 2.
 - 17.2. Anti-scam interventions within the banking industry are likely to be of greatest benefit to consumers. It is evident that the Government has developed a bespoke model that resists the model that has been implemented in the United Kingdom, where a mandatory reimbursement model for banks has been introduced for consumers. Any novel model,

²⁴ In the National Press Club Address on July 31, 2024, it was stated that forthcoming mandatory codes for digital platforms will include actions to verify advertisers and take down scam pages; these measures are included in the AOSC. Signatories to the code are committing to detect and block suspected scams, provide a simple and quick route for users to report them, and quick action to take down verified scam content and scammers. There are also commitments related to the verification or authentication of new advertisers, additional confirmations with respect to financial services advertisers, and the screening of advertisements for suspicious or changing content. See Address to National Press Club (31/7/24), Fighting scammers, fighting for Australians,

<https://ministers.treasury.gov.au/ministers/stephen-jones-2022/speeches/address-national-press-club-canberra>

²⁵ The Hon Stephen Jones MP (24/11/23), Government welcomes Scam Safe Accord,

<https://ministers.treasury.gov.au/ministers/stephen-jones-2022/media-releases/government-welcomes-scam-safe-a-cord>

²⁶ Australian Banking Association (24/11/23), Press conference: Scam-Safe Accord launch,

<https://www.ausbanking.org.au/press-conference-scam-safe-accord-launch/>

without international precedent, takes time to get right; it cannot be rushed into law soon after a three week consultation period. The EDR scheme contemplated provides a perfunctory attempt to provide consumer redress, in a manner that will not be timely nor efficient for consumers wishing to avail of it.

- 17.3. Under the proposed Australian scheme, there could be a protracted examination through an external dispute resolution body of different companies' relative roles in the scammers' attack, in order to determine possible redress. Unlike the UK scheme, that could take years for any form of reimbursement for people who have lost their life savings because of the sheer number of different services scammers exploit in their complex attack chain. DIGI has included its conceptualisation of the scam attack chain in Image 1, above.
- 17.4. We are concerned that the Government is proposing to legislate mechanisms for consumers to be directly compensated by platforms for scam related losses without providing any necessary detail about the boundaries and circumstances in which consumer compensation would be considered appropriate, and how it might be shared across different regulated and non-regulated entities.
- 17.5. It is also an uncomfortable fit to mandate that digital platforms and telecommunications providers join the Australian Financial Complaints Authority, which is the banks' EDR scheme. DIGI considers this a reflection of the extensive consultation that has occurred with banking sector²⁷ on the design of the framework that has not occurred to the same extent with other sectors.
- 17.6. AFCA would lack familiarity and experience with the new sectors it would need to regulate. Furthermore, we understand that AFCA generally considers disputes involving a single service provider.
- 17.7. The Explanatory Memorandum acknowledges that scams involve more than one regulated sector and more than one regulated entity. It is also entirely unclear how the EDR scheme would apportion liability across the different sectors, given the sheer complexity of scam attack chains, as illustrated in Image 1. To our knowledge, such an EDR scheme is without precedent.
- 17.8. Further, we query whether any EDR scheme – as opposed to a Court – has the necessary resources and expertise across the regulated sectors to make the determinations contemplated in the legislation, particularly if large numbers of claims are brought forward.
- 17.9. We understand that Treasury recommended to the Minister that their preference was 'a mechanism to determine redress and reimbursement of funds for breaches by a bank', the rationale for which was expressed as:

An external dispute resolution (EDR) mechanism (such as through AFCA) to determine redress and reimbursement of funds to a consumer where a bank has breached its obligations under the sector-specific code.

²⁷ Documents released under the Freedom of Information Act,
<https://treasury.gov.au/sites/default/files/2024-09/foi-3675.pdf>

Developing and implementing a multi-sector EDR scheme would be complex and time consuming, and would be a future consideration.

Clear obligations on businesses and strong penalties in the Framework will provide incentives for businesses to reduce scam losses, and the need for a multi-sector EDR scheme would be considered at a later stage²⁸.

- 17.10. DIGI agrees with the above assessment from Treasury. If the Government wishes to provide consumers with timely redress and reimbursements, then we support the original recommendation made to the Government by Treasury to focus on banks. If the Government alternatively wishes to focus on scam prevention, that should be the sole focus of the Framework. The concept of a mechanism to allow for direct compensation by digital platforms is globally unprecedented. Should the Government insist on including a multi-sector EDR scheme Framework, it should be addressed at a later stage. We are unclear as to why the Government departed from this recommendation based on what appears to be Ministerial feedback²⁹.
- 17.11. We are concerned that the Government is proposing to legislate mechanisms for consumers to be directly compensated by digital platforms for scam related losses without providing any necessary detail about the boundaries and circumstances in which consumer compensation would be considered appropriate, and how it might be shared across different regulated and non-regulated entities.

Summary of recommendations in Section 3

- S. If the Government wishes to provide consumers with timely redress and reimbursements, then the UK bank reimbursement model should be followed, in line with Treasury's original recommendation.
- T. Alternatively, if the Government wishes to focus on scam prevention, that should be the sole focus of the Framework.
- U. Should the Government insist on including an EDR scheme Framework, it should be addressed at a later stage after extensive industry and consumer consultation to determine details.

F. Division 5: Regulating the SPF

18. The role of the ACMA for the digital platforms sector

- 18.1. The Scams – *Mandatory Industry Codes Consultation Paper*, released in November 2023 (the Consultation Paper) indicated that the ACMA would be the regulator for the digital platforms sector, stating that:

²⁸ As above, p. 76.

²⁹ As above, p. 123.

'...the Government would establish powers in the relevant legislation, such as ACMA's administered legislation (e.g. Broadcasting Services Act 1992 (BSA) or Telecommunications Act), for the ACMA to establish and enforce codes and standards for digital communications platforms regarding scams. The Minister for Communications would then direct the ACMA to develop a new industry standard applying to digital communications platforms, consistent with the obligations under the CCA.

The ACMA would consult with industry to ensure that obligations are fit-for-purpose and able to be implemented by different types and sizes of businesses in the sector, as well as have a meaningful impact on reducing scam activity across the sector. 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.'

- 18.2. It is unclear why there has been a shift to make the ACCC the regulator for digital platforms, since the release of the Consultation Paper. No rationale for this shift is provided in the Explanatory Memorandum nor the Summary of Reforms. We consider that the ACMA has a combination subject matter and sectoral expertise, through its oversight of the telecommunications industry's scams code and its work with digital platforms in areas such as misinformation.
- 18.3. While we have concerns about effective co-operation under a multi-regulator model, this means that the digital platforms sector is the only sector that does not have this model.
- 18.4. Rather than the ACCC enforcing a mirrored set of obligations to the sectoral regulators, we consider that a more valuable role for the ACCC would be to empower it with power to issue takedown requests concerning scams cross-sectorally, as noted.

Summary of recommendations in Section F

- V. The ACMA should be the sectoral regulator for the digital platforms scams code, consistent with the previous position expressed in the Consultation Paper, and reflecting that they are the only regulator with a combination of sectoral and subject matter expertise.

G. Division 6: Enforcing the SPF

19. Enforceable undertakings

- 19.1. The provision for court orders to compensate 'any other person who has suffered loss or damage' as a result of a regulated entity's breach of a written undertaking to the regulator in s58FS(5)(c) seems to impose strict liability on regulated entities for any loss incurred by any person (including non-parties to the undertaking) as a result of the entity's breach

of such an undertaking. This appears excessive and unfairly punitive, especially since it appears to fully transfer liability from the scammer to the platform, as if the platform is complicit in the scam. DIGI suggests narrowing this provision down to "any user who has suffered actual loss or damage as a direct result of a regulated entity's breach".

20. Penalty regime

- 20.1. DIGI understands that breaches of the principles-based obligations in the primary law relating to preventing, detecting, disrupting and responding to scams attract penalties for entities that are the greater of \$50 million, three times the value of the benefit obtained, or 30 percent of the turnover during the period in breach. Breaches of the principle-based obligations in the primary law relating to reporting and governance and any breaches of the sector codes, attract penalties that are the greater of \$10 million, three times the value of the benefit obtained, or 10 percent of turnover during the period in breach.
- 20.2. It is unclear how the breach turnover period for the contravention will be calculated, and whether it refers to local or global turnover.
- 20.3. In light of the definitional ambiguities outlined throughout this submission, and the cross-sectoral and cross-platform nature of scams, DIGI considers the proposed penalties to be extremely high.
- 20.4. 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.
- 20.5. While the Government previously indicated its intent in the Consultation Paper that 'Government and regulators will work through the necessary arrangements to avoid two regulators taking simultaneous action against a breach under the Framework', it is unclear if that intent is retained in the Framework. DIGI recommends that the dual penalty regime be removed in favour of a penalty regime enforced by the relevant sectoral regulator, in relation to the sectoral codes.
- 20.6. 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 B), 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. As noted, 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.
- 20.7. Taking into account the impact of overcorrection on legitimate business activity, we encourage a proportional or tiered penalty framework where fines are levelled for serious breaches or systemic failures.

Summary of recommendations in Section G

- W. s58FS(5)(c) should be narrowed to 'any user who has suffered actual loss or damage as a direct result of a regulated entity's breach'.
- X. DIGI recommends that the dual penalty regime be removed in favour of a penalty regime enforced by the relevant sectoral regulator, in relation to the sectoral codes.
- Y. If penalties are retained in the Framework, taking into account the impact of overcorrection on legitimate business activity, we encourage a proportional or tiered penalty framework where fines are levelled for serious breaches or systemic failures.