



Senate Standing Committees on Economics  
PO Box 6100  
Parliament House  
By email: economics.sen@aph.gov.au

Tuesday December 24, 2024

Dear Chair,

The Digital Industry Group Inc. (DIGI) thanks the Senate Standing Committee on Economics for the opportunity to provide our views on the *Scams Prevention Framework Bill 2024* ("the Framework").

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, HelloFresh, Meta, Microsoft, Pinterest, 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.**

DIGI has engaged extensively with the Government on this issue and on July 26, 2024 launched *The Australian Online Scams Code* (AOSC)<sup>1</sup>. 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 of consultation drafts. Accordingly, as this work demonstrates, **DIGI is supportive of requirements to have 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 marketplaces, and email, which we understand are not intended to be designated initially under the legislation. **The AOSC provides a comprehensive and globally interoperable model that we request the**

---

<sup>1</sup> DIGI, *The Australian Online Scams Code*, [www.digi.org.au/scams](http://www.digi.org.au/scams)



## Committee recommend to the Government draw upon in developing the mandatory sectoral digital industry code.

The AOSC contains 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.

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 the Bill seeks to introduce. Throughout this submission, DIGI advances a range of specific suggestions for how the Bill can effectively achieve these goals, with an emphasis on four overarching themes.

## Overarching concerns

### 1) Duality of obligations under the Framework

We are concerned that the Bill 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. A company could theoretically be in breach of the obligations in the primary legislation while complying with all of the obligations in the subordinate legislation's sectoral code – this is a problem that we hope the Committee can address.

A better solution would be to carefully work through the detail of each sector's obligations through the subsequent codes, given the short timeframe to pass the legislation prior to an election. The interaction between overarching legislation and forthcoming subsequent codes is complex, and could be avoided by retaining strict obligations but placing them in codes rather than legislation. **We therefore recommend that the primary legislation should simply 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.**

DIGI strongly believes that the prescriptive obligations in Division 2 of the primary legislation are currently a) inapt for the three initial sectors and b) 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. The obligations appear to be primarily designed around the banking sector. For example, the obligations around *reporting* scams to the National Anti-Scam Centre will need to look different for multinational companies that are not headquartered in Australia. Some jurisdictions across and within the United States have limitations on the



ability to share personal data with other governments, and especially in instances where there is cross-border transfer of personal data. Companies are still working through the extent to which reporting to the NASC can be done without a conflict of laws; This is not a reflection at all of companies' willingness to work with the NASC, but is a practical and legal reality that needs to be carefully considered. The level of detail provided in the primary legislation around the reporting obligation may create future issues, once code-specific obligations are added in supplementary legislation.

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. In practice, this means the removal of Division 2 (with its obligations considered in the sectoral codes), and the retention of Division 3 authorising the development of these codes.** DIGI's specific suggestions in relation to obligations should be considered by relevant regulators when developing the mandatory codes.

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

Crystal clear obligations for industry, along with clear responsibilities for regulators, mean better outcomes for consumers. DIGI welcomes the addition of section 58BB to the Bill which provides some guidance to industry on the meaning of 'reasonable steps' as to their obligation to prevent scam activity on their platforms. However, we do not consider this adequate; Without clear guidance on 'reasonable steps', companies, consumers and regulators will draw on varying interpretations of such adequate action, potentially leading to penalties being imposed when companies act in good faith within their interpretation of 'reasonable steps' but not within the regulator's interpretation.

DIGI notes that subsection (e) of 58BB states 'reasonable steps' for the purposes of the primary legislation includes whether an entity has complied with the sector-specific code, and highlights this subsection in particular as being helpful to industry. **DIGI further requests the Committee recommend specific 'reasonable steps' be outlined in mandatory sector-specific codes, and be confined to these codes.**

## 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 all potential scams with the regulator. The magnitude of this obligation is enormous. For example, multinational companies may disable millions of accounts, and it is not practical for them to investigate in every instance if that account had any contact with an Australian – under the legislation, this is a sufficient nexus to require a report to the regulator. Given there are high penalties and a low and vague threshold for reporting, one of the few options available to companies will be to report everything to the ACCC, even if an Australian link is not clear, to ensure there is no risk of being found non-compliant with the reporting requirements.

The ACCC is likely to be inundated with millions of low-quality reports about potential scams that might not even eventuate to a serious concern in Australia. 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. The resources used to send these reports from companies, and taxpayer resources to review them at the ACCC, would be better invested in more impactful anti-scam efforts. Reporting requests should be scoped towards clear outcomes, including what meaningful actions will be taken with the information



shared. **DIGI requests that the Committee recommend the reporting requirements under the Bill be removed or vastly narrowed in scope, and that consultation occur on the related technical and operational requirements for receiving reports, before any such requirement is legislated. Any reporting requirements should be included in the sector-specific codes, the timeframe for which would allow this consultation.**

#### 4) Questions regarding consumer redress

DIGI is supportive of an economy-wide approach, and strengthening accountability in the digital industry. **It is important to emphasise 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)<sup>2</sup>. 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.

Initial contact alone is only a small part of the scammers' process. While scammers can employ online forums, their final step always involves theft through financial services, after securing the victim's financial information. 100% of scam cases involve a financial service. Focussing anti-scam interventions on banks – including liability – would be simpler, easier for consumers to understand, and more effective. Given the central role that banks play in the life of every Australian, consumers should be able to trust in the integrity and safety of their accounts. In 2023, bank transfer was the most reported payment method with \$212 million in reported losses, and there have been regulatory and legal decisions that indicate banks are able to take greater steps to protect consumers<sup>3</sup>. We understand the Minister's attention to ensuring that smaller financial institutions like the Broken Hill Credit Union<sup>4</sup> do not have a disproportionate regulatory obligation and liability from the new legislation. However, Australia has one of the most concentrated banking sectors in the world; the risk of smaller financial institutions facing disproportionate obligations is low, and can be managed by regulatory design in the banking-specific codes by applying primary obligations to larger institutions.

DIGI notes that the model introduced in the Bill is in contrast to the mandatory reimbursement model by banks implemented in the United Kingdom. While it appears that there has been intense and ongoing consultation since 2022 with the Australian Banking Association on the Framework<sup>5</sup>, 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, redress under the Framework could take years 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. **DIGI asks the Committee to recommend to the Government that this external dispute resolution model advanced in the Bill not be rushed into law, especially considering it is a novel legislative model without international precedent, and be reconsidered at a later stage as potential secondary legislation.** We are concerned

<sup>2</sup> April 2024, ACCC, *Targeting Scams 2023*,

<https://www.accc.gov.au/system/files/targeting-scams-report-activity-2023.pdf>

<sup>3</sup> See, for example, AFCA's recent decision involving HSBC

<sup>4</sup> Assistant Treasurer Stephen Jones, Address to National Press Club, Q&A,

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

<sup>5</sup> Documents released under the Freedom of Information Act,

<https://treasury.gov.au/sites/default/files/2024-09/foi-3675.pdf>



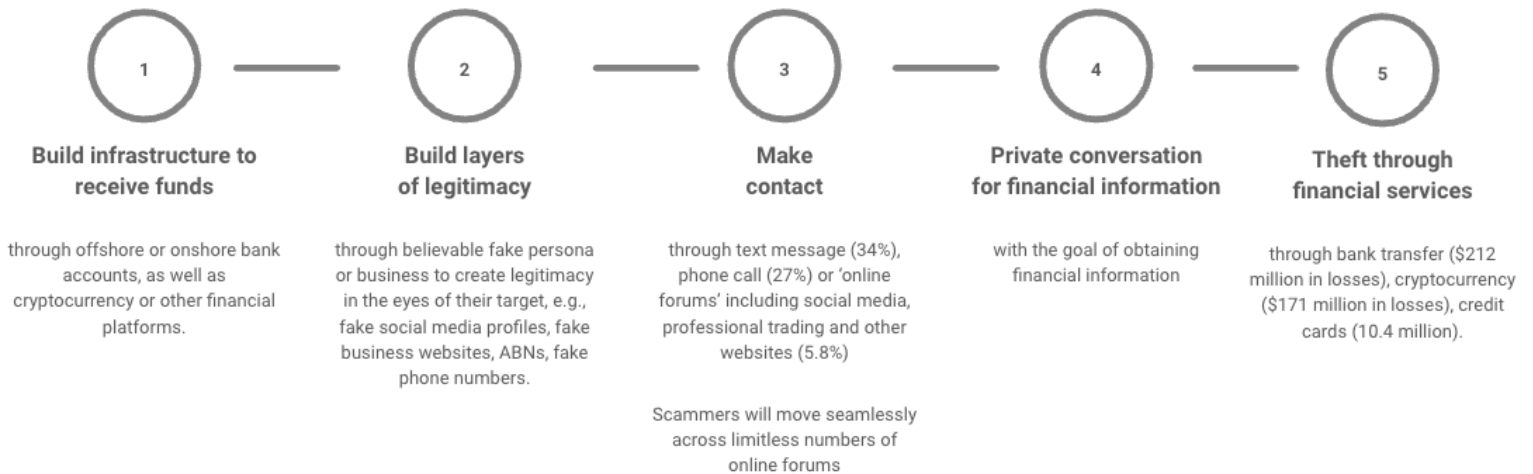
that the Government is proposing to legislate mechanisms for consumers to be directly compensated by platforms for scam related losses without providing any necessary detail about the boundaries and circumstances in which consumer compensation would be considered appropriate, and how it might be shared across different regulated and non-regulated entities.

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 collaboration as we work with you toward the shared goal of making Australia a harder target for scammers.

Best regards,

Sunita Bose  
Managing Director, DIGI

Image 1: A typical scam 'attack chain'





## Table of contents

<b>Overarching concerns</b>	<b>2</b>
1) Duality of obligations under the Framework	2
2) 'Reasonable steps' should be determined in mandatory codes	3
3) Excessive and impractical reporting requirements	3
4) Questions regarding consumer redress	4
Image 1: A typical scam 'attack chain'	5
<b>A. Missing elements in the legislation</b>	<b>8</b>
1. Empowering the NASC to provide consumers and companies with real-time information	8
2. Global leadership to pursue scammers	9
3. Empowering the ACCC to remove non-investment scams	9
Summary of Requested Recommendations in Section A	10
<b>B. Division 1: Scope</b>	<b>10</b>
4. Scope of services	10
Social Media Services	10
Functionalities within services	12
Messaging services	12
Matters considered before designation	13
5. The definition of a scam	14
'Obtaining personal information'	15
'Indirect attempt'	16
'Engage an SPF consumer'	16
The impact of overcorrection	17
6. Definition of an 'SPF consumer'	17
7. Actionable scam intelligence	18
Internal thresholds of suspicion	18
Consistent application of terminology	18
8. Extraterritorial application	19
Summary of Requested Recommendations in Section B	19
<b>C. Division 2: Overarching principles</b>	<b>20</b>
9. Overarching considerations	20
Avoiding a dual-set of obligations	21
Role of sectoral codes in determining reasonable steps	21
10. SPF Principle 1: Governance	22
Obligations triggered after a single report	22
Annual certification	22
Arming scammers with unprecedented information	23
Record keeping	23
11. SPF Principle 2: Prevention	23



12. SPF Principle 3: Detect	24
'As it happens'	24
Consumer profiling	24
Reasonable steps	24
13. SPF Principle 4: Report	25
High volumes of reports	25
'Authorised third party data gateways'	26
14. SPF Principle 5: Disrupt	27
Reporting concerns	27
Warnings	27
Need for regulatory takedown powers	27
Safe harbour scheme	27
15. SPF Principle 6: Respond	28
Internal dispute resolution	28
External dispute resolution	28
Summary of Requested Recommendations in Section C	28
<b>D. Division 3: Sector-specific codes</b>	<b>30</b>
16. Sector specific codes are central to driving uplifts	30
Summary of requested recommendations in Section D	30
<b>E. Division 4: EDR for the SPF</b>	<b>31</b>
17. External dispute resolution (Division 2 & Division 4 combined)	31
Summary of Requested Recommendations in Section 3	32
<b>F. Division 5: Regulating the SPF</b>	<b>33</b>
18. The role of the ACMA for the digital platforms sector	33
Summary of requested recommendations in Section F	34
<b>G. Division 6: Enforcing the SPF</b>	<b>34</b>
19. Enforceable undertakings	34
20. Penalty regime	34
21. Remedial Directions	35
Summary of Requested Recommendations in Section G	36
<b>H. Appendix</b>	<b>36</b>
Item 1 Table of Recommended Changes	36



## 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 scammers<sup>6</sup>. Yet the NASC is not mentioned in the Framework, and the Bill's Explanatory Memorandum makes it clear the NASC's role is primarily in the 'status quo', rather than under the reforms the Bill proposes. The Bill instead proposes the ACCC as the overarching regulator of the Framework, with the Australian Securities and Investments Commission (ASIC) and the Australian Communications and Media Authority (ACMA) assisting in regulating the banking and telecommunications industries respectively. The ACCC would also regulate digital platforms' code responsibilities. **DIGI requests the Committee recommends to the Government that the role of the NASC under this new Framework is clearly outlined, so both consumers and regulated companies can understand its role.** DIGI also recommends the NASC be at the centre of an ecosystem approach, providing timely information to companies and consumers to intercept scammers' efforts.
- 1.3. **DIGI requests that the Committee 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.** 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'<sup>7</sup>. 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 ASIC on the publicly available Moneysmart website.<sup>8</sup>

### 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.

---

<sup>6</sup> 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>

<sup>7</sup> 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>

<sup>8</sup> ASIC 2024, 'Investor alert list', <https://moneysmart.gov.au/check-and-report-scams/investor-alert-list>





- 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 Bill proposes a 'multi-regulator model' where multiple regulators, including the ACCC, ASIC and ACMA, 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 in regulation for:
  - 3.2.1. less mainstream services without such policies, such as the professional trading sites that are counted in the NASC's data about 'social media services';
  - 3.2.2. cases where companies do not have enough information to verifiably conclude that content is a scam – in such cases, third party verification from an authoritative source, such as a regulator, could provide information needed to conclusively remove associated content or accounts.
- 3.3. Today, ASIC only has takedown powers in relation to investment scam websites – and removes up to 20 scam websites a day.<sup>9</sup> The Government has acknowledged the key role the ASIC takedown scheme has played in reducing scam losses on an annual basis.<sup>10</sup> 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.

---

<sup>9</sup> 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>

<sup>10</sup> ACCC 2024, *Targeting Scams 2023 - Observations on declining losses*, p.7  
<https://www.accc.gov.au/system/files/targeting-scams-report-activity-2023.pdf>



- 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 Requested Recommendations in introduction and Section A

### Overarching introductory recommendations:

- A. The AOSC provides a comprehensive and globally interoperable model that we request the Committee recommend to the Government draw upon in developing the mandatory sectoral digital industry code.
- B. The primary legislation should simply 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.
- C. The Framework should not itself contain obligations, other than the obligation for entities to comply with the codes. In practice, this means the removal of Division 2 (with its obligations considered in the sectoral codes), and the retention of Division 3 authorising the development of these codes.
- D. 'Reasonable steps' be outlined in mandatory sector-specific codes, and be confined to these codes.
- E. Reporting requirements under the Bill be removed or vastly narrowed in scope, and that consultation occur on the related technical and operational requirements for receiving reports, before any such requirement is legislated. Any reporting requirements should be included in the sector-specific codes, the timeframe for which would allow this consultation.
- F. The external dispute resolution model advanced in the Bill not be rushed into law, especially considering it is a novel legislative model without international precedent, and be reconsidered at a later stage as potential secondary legislation.

### Section A recommendations:

- G. The role of the NASC under this new Framework should be clarified, so both consumers and regulated companies can understand its role.
- H. Any actionable reports shared with the NASC, through the Framework or the NASC's existing operations, should 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.



- I. 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.
- J. 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

#### Social Media Services

- 4.1. We note that the Bill indicates 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 shown below:

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

- 4.2. 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.
- 4.3. 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;<sup>11</sup> 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. **As such, DIGI requests that the Committee recommends the application of any designation be limited by size of user base or risk profile**, similarly to how the level of obligation placed on platforms under the *Online Safety Act's* codes and standards is determined.
- 4.4. 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.
- 4.5. 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.

#### Functionalities within services

- 4.6. It is currently unclear whether certain functionalities of a digital service are caught under the Framework and not others, and how the designation might apply in such cases. For example, we understand that marketplaces are not intended to be designated in the first tranche of regulated entities under the Framework. As such, this makes it unclear whether a social media service with marketplace functionality could or would be designated. As another example, it is unclear whether a messaging service embedded

---

<sup>11</sup> See example: Beyond Blue, *Online forums*: <https://forums.beyondblue.org.au/>



within an excluded service, such as a marketplace, would be included in the designation of 'messaging services'.

- 4.7. 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 matters relating to the designation instrument must be brought forward ahead of the passage of the Framework to ensure its design does not have unintended consequences.**

#### Messaging services

- 4.8. DIGI considers that over the top messaging services are more akin to SMS/MMS, and are better regulated by 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.**
- 4.9. 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.
- 4.10. 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.
- 4.11. 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' for messaging services:**
  - 4.11.1. implement or build a systemic weakness, or a systemic vulnerability, into a form of encrypted service or other information security measure;
  - 4.11.2. render methods of encryption less effective;
  - 4.11.3. build a new decryption capability in relation to encrypted services;
  - 4.11.4. undertake monitoring of private communications.
- 4.12. 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 Australians<sup>12</sup>.

#### Matters considered before designation

- 4.13. Section 58AE indicates that the Minister must 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'.
- 4.14. 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' portal<sup>13</sup>. 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 publicly<sup>14</sup> and raised with the National Anti Scam Centre (NASC) and other relevant Government departments.
- 4.15. 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.
- 4.16. **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.** This particularly important as the the ACCC has acknowledged in Senate Estimates inaccuracies and anomalies with the data collection in its quarterly reports<sup>15</sup>. 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.

---

<sup>12</sup>Resolve 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

<sup>13</sup> ACCC, *Report a scam*, <https://www.scamwatch.gov.au/report-a-scam>

<sup>14</sup> Bose, Sunita (2/8/24), *Blame game won't protect Australians from scams*,

<https://www.innovationaus.com/blame-game-wont-protect-australians-from-scams/>

<sup>15</sup> *Senate Economics Legislation Committee - Estimates. Thursday, 21 November 2024, Canberra, ACCC testimony on page 23.*



## 5. The definition of a scam

- 5.1. A precise and appropriate definition for what is, and is not, a 'scam' is the foundation for clarity for platforms to determine the action they need to take in relation to scam activity.
- 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:

*A scam is a direct or indirect attempt (whether or not successful) to engage an SPF consumer of a regulated service where it would be reasonable to conclude that the attempt:*

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

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

- 5.3. DIGI notes that the definition has been expanded from the Exposure Draft by adding "whether or not successful", and narrowed the definition as the meaning of an SPF consumer in section 58AH is now a person who ordinarily resides in Australia.
- 5.4. DIGI considers the definition proposed by the Bill as lacking clarity. We consider the Commonwealth Fraud Control Policy (CFCP)<sup>16</sup> 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'.*

- 5.5. 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 Bill does include this scenario.
- 5.6. 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 loss<sup>17</sup>.*

**DIGI requests the Committee recommends refining the definition of a scam to be consistent with the AOSC definition.**

- 5.7. 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

---

<sup>16</sup>Attorney General's Department (2017), *Commonwealth Fraud Control Framework*, <https://www.ag.gov.au/sites/default/files/2020-03/CommonwealthFraudControlFramework2017.PDF>

<sup>17</sup> DIGI, *The Australian Online Scams Code*, [www.digi.org.au/scams](http://www.digi.org.au/scams)



SMS are often characterised by a high volume of messages to a large number of B-Parties (i.e. potential victims/recipients).<sup>18</sup> 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.

### 'Obtaining personal information'

- 5.8. DIGI notes that the Bill'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 1988*, where personal information is defined 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.'*<sup>19</sup>

- 5.9. 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.
- 5.10. 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.
- 5.11. 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.
- 5.12. 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

<sup>18</sup> Communications Alliance Ltd, *Industry Code C661:2022 Reducing Scam Calls And Scam SMSs*, [https://www.commsalliance.com.au/\\_data/assets/pdf\\_file/0015/72150/C661\\_2022.pdf](https://www.commsalliance.com.au/_data/assets/pdf_file/0015/72150/C661_2022.pdf)

<sup>19</sup> OAIC (2017), *What is personal information?*, <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/what-is-personal-information#:~:text=The%20Privacy%20Act%20defines%20personal,a%20material%20form%20or%20not.>





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.

- 5.13. **DIGI requests the Committee recommends the removal of 'personal information' from the definition of a scam, and a greater focus on the obtainment of financial benefit.**
- 5.14. **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)...'**
- 5.15. DIGI notes in section 58AG(4) the Bill now includes the ability for the scam rules to exclude scam attempts from this definition.

#### 'Indirect attempt'

- 5.16. DIGI questions the inclusion of 'indirect attempt' in the definition of a scam. We consider that this inclusion further broadens and confuses the definition of a scam. **We propose the removal of 'indirect attempt' from the definition of a scam, in order to ensure precision and implementability by industry participants.**

#### 'Engage an SPF consumer'

- 5.17. 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 scammer<sup>20</sup>. DIGI welcomes that the addition of subsection (3) to the Bill in section 58AG now includes that 'the attempt may be a single act or a course of conduct', clarifying each individual communication would not be considered a separate scam.

#### The impact of overcorrection

- 5.18. The broad definition of a scam makes it extremely difficult for the digital industry to operationalise, without considerable overcorrection. Considering the penalty regime, where penalties are up to the greater of \$50 million or 30 percent of global revenue, services will 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 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.
- 5.19. 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

---

<sup>20</sup>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>



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 and Boxing Day sales), 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.

- 5.20. 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.

## 6. Definition of an 'SPF consumer'

- 6.1. DIGI welcomes that the definition of an 'SPF consumer' included in the Bill has been narrowed from the Exposure Draft's definition through residency requirements. These changes were in line with DIGI's recommendations to Consultation on the Exposure Draft.
- 6.2. DIGI was previously concerned that the Exposure Draft's definition of an 'SPF consumer' applied to Australian citizens and residents anywhere in the world, as well as non-Australians in Australia meaning entities would need to actively track consumer location in order to comply with the Framework. DIGI is pleased to see these concerns mitigated by the inclusion of residency requirements, which are more easily determined by platforms without the need for location monitoring, respecting consumer privacy and cybersecurity concerns.

## 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.<sup>21</sup>

---

<sup>21</sup> 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/>



- 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'.<sup>22</sup> We request the Committee recommend 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 Bill 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 provisions<sup>23</sup>.
- 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 might require regulated entities to alter the services they provide anywhere in the world. **We request the Committee recommend that the Framework be amended to more specifically set out the intended extraterritorial operation.**

## Summary of Requested Recommendations in Section B

- K. 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.
- L. 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

<sup>22</sup> Art.16(3), *Digital Services Act*, <https://www.eu-digital-services-act.com/>

<sup>23</sup> 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>



functionalities offered within a service. Consideration of matters relating to the designation instrument must be brought forward ahead of the passage of the Framework to ensure consistency.

- M. As detailed in Section F of this submission, we consider that ACMA is a more well-suited regulator for digital platforms in general, bringing both sectoral and subject-matter expertise to 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.
- N. 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.
- O. 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.
- P. 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)...'.
  - e. Removing 'indirect attempt' in order to ensure precision and implementability by industry participants.
- Q. The definition of 'actionable scam intelligence' should be modified to set a higher threshold for action under the Framework in response to such intelligence.
- R. 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.
- S. 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.



- T. We request the Committee recommend that the Framework be amended to more specifically set out the intended extraterritorial operation.

## C. Division 2: Overarching principles

### 9. Overarching considerations

- 9.1. **Fundamentally, DIGI is supportive of Division 3 of the Bill in affording the development of sector-specific codes. In line with this, we strongly urge the removal of Division 2 at this stage, with its proposed obligations reconsidered in the context of the codes to be later developed under the powers afforded in Division 3.**
- 9.2. In this section of the submission, DIGI substantiates why the proposed obligations in Division 2 are not fit for purpose, nor readily applicable to a wide range of sectors. **We offer suggested refinements to Division 2's obligations, with our strong preference that such obligations and stakeholder feedback be further explored and in the sectoral codes.**

#### Avoiding a dual-set of obligations

- 9.3. 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.
- 9.4. 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 to the Treasury Consultation on the Exposure Draft indicates are intended to be superannuation funds, digital currency exchanges, other payment providers, and transaction-based digital platforms like online marketplaces.
- 9.5. DIGI submits that 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.
- 9.6. We understand from earlier consultations 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:

- 9.6.1. enable the designation of applicable sectors;
- 9.6.2. direct a company to adopt an existing industry code, or for it to develop an equivalent;
- 9.6.3. empower the relevant regulator with code and standard-making powers, or oversight powers over industry-led codes;
- 9.6.4. 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 request the Committee 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

- 9.7. 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'. DIGI welcomes that the Bill does provide additional guidance on this issue, and section 58BB has been added from the Exposure Draft to give guidance as to what 'reasonable steps' imposes on platforms. However, DIGI does not believe the addition of these five factors provides enough guidance to industry on what action is satisfactory to not be in breach of the primary legislation or any subordinate codes.
- 9.8. Currently, a company could theoretically 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. DIGI is concerned that a lack of clarity around what constitutes 'reasonable steps', combined with the ability for individuals to claim compensation for scam losses from industry, will lead to confusion about how best industry is to manage scam risks and when individuals have a meritorious claim.
- 9.9. 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. Currently, under section 58BD, 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. DIGI notes changes to the timelines regarding annual certification have been actioned, shifting the timeline from seven days after the beginning of the financial year to the anniversary of becoming a regulated entity. DIGI welcomes this change, as it reflects how the meaning of 'financial year' is different throughout the world, recognising that most digital platforms are based overseas. **We suggest further simplification should occur to ensure this corresponds to the entity's financial year, which will be more institutionally memorable than the anniversary of its designation.**
- 10.3. DIGI is still concerned this section places the senior officer in an untenable position, considering the ambiguous position regulated entities face if a single scam or a single consumer report appears. **DIGI maintains this section should be removed, but if it is to be retained, the Government should specify that there is an express exclusion of individual liability of the senior officer.**

### Arming scammers with unprecedented information

- 10.4. DIGI welcomes that the Government has addressed our concern on Section 58BF of the Exposure Draft, by removing the obligation to publish information about protecting SPF Consumers. This section required regulated entities to make publicly accessible the measures they have in place to protect consumers from scams, which DIGI believes would be used by scammers, rather than consumers, in order to craft more complex and believable scams.

### Record keeping

- 10.5. Section 58BF'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 section 58BG to produce such records to the regulator within ten 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 section 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 Committee might consider recommending 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.**
- 11.4. DIGI welcomes that the Government has addressed industry concerns over identifying classes of consumers at higher risk of being targeted by scams, by removing section 58BK of the Exposure Draft. This change reflects DIGI's concerns over how it would profile consumers whilst respecting privacy and abiding by principles of data minimisation.

## 12. SPF Principle 3: Detect

### 'As it happens'

- 12.1. DIGI is concerned about the standard set in section 58BM 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 would detect 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. **DIGI strongly requests the Committee recommends 'as it happens' be removed from section 58BM.**
- 12.2. We also 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 section 58BO to 'identify the persons who were SPF consumers of that service 2 at the time when the persons were or may have been impacted by the activity'. 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 'may have been 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 section 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 section 58BP 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 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 detract 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(5) to the potential disclosure to the SPF regulator of personal information.
- 13.6. **DIGI requests that the Committee recommend the reporting requirements under the Bill be removed or vastly narrowed in scope, and that consultation occur on the related technical and operational requirements for receiving reports, before any such requirement is legislated. Any reporting requirements should be included in the sector-specific codes, the timeframe for which would allow this consultation.**

#### 'Authorised third party data gateways'

- 13.7. The Bill indicates that "the SPF rules may prescribe a scheme for authorising third parties to operate data gateways, portals or websites that give access to reports under this Division". **This should not be mandated in legislation before the operational details for receiving reports is released to industry, and work is undertaken to ensure that it is practical.**
- 13.8. We question whether any third party data gateway or portal, as contemplated in the Bill, could operate effectively to receive millions of reports from all regulated entities, let alone provide actionable information to regulated entities. Put frankly, this prospect is a fantasy, and we instead urge emphasis on ensuring the NASC is communicating to regulated entities in a non-automated way to ensure that scams are promptly actioned.
- 13.9. The effective operation of such a portal may require the development of 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.
- 13.10. 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.

- 13.11. 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.
- 13.12. For example, such consultation would enable service providers to reconcile their competing obligations under the Privacy Act, with the requirements in s58BS(5) 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 Subdivision E and Subdivision F.

### Warnings

- 14.3. DIGI welcomes that the Government has removed the obligation on industry to warn consumers with respect to a specific scam once they receive actionable scam intelligence, as in section 58BX of the Exposure Draft. DIGI believes this section would have placed a large burden on industry considering the uncertainty around whether 'actionable scam intelligence' could refer to a single report of a scam, and if industry were to comply, would have meant consumers were inundated with warnings so that such warnings would essentially become meaningless.

### Need for regulatory takedown powers

- 14.4. 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 A 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

- 14.5. As noted, while the proposed safe harbour in section 58BZA 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. It is unclear how the regulated entity would be able to effectively reverse any erroneous decisions.
- 14.6. DIGI welcomes the addition of s 58BZA(3) which adds a test of reasonable proportionality to any mechanisms platforms take to the safe harbour protections.
- 14.7. 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 section 58BZD that requires regulated entities to have an accessible mechanism for consumers to report scams relating to their service. However, the expansion of the action required to be in response to activity that “may be scams” instead of merely ‘scams’ introduces further ambiguity in how an entity should respond. As stated above, there is potential for consumers to report perfectly legitimate activity and the platform to respond by overcorrection because of the expansion of this definition.
- 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 Requested Recommendations in Section C

- U. **Fundamentally, DIGI is supportive of Division 3 of the Bill in affording the development of sector-specific codes. In line with this, we strongly urge the removal of Division 2 at this stage, with its proposed obligations reconsidered in the context of the codes to be later developed under the powers afforded in Division 3.** 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.
- V. '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.
- W. We offer the following suggested refinements to Division 2's obligations, with our strong preference that these recommendations be further explored and in the sectoral codes.
- a. The Committee might consider recommending 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.
  - b. The liability of regulated entities at the point at which a scam surfaces, prior to action, must be clarified.
  - c. 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 section 58BE places the senior officer in an untenable position, and should be removed.
  - d. Regarding annual certification, further simplification should occur to ensure alignment with the entity's financial year, which will be more institutionally memorable than the anniversary of its designation.
  - e. If this requirement under section 58BE 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.
  - f. Section 58BF'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 section 58BG to produce such records to the regulator within ten 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 standard set in s58BM 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'.
- i. 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.
- j. 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.
- k. The prescription of a scheme for authorising third parties to operate data gateways, portals or websites that give access to reports should not be mandated in legislation before the operational details for receiving reports is released to industry.
- l. The notifiable instrument noted in s58BS that determines the kinds and the form of the reports must undergo extensive industry consultation.
- m. While a safe harbour is welcome, it must be coupled with more targeted definitions and refined obligations to mitigate error before it occurs.
- n. We suggest that section 58BZD be further explored in subordinate legislation for sectoral codes.

## 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. DIGI has led the development of the AOSC and attempted to work with Government on formulating this proactive response to scam activity on digital platforms in Australia.
- 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 AOSC'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 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 request the Committee recommend the Government draw upon in developing the mandatory sectoral digital industry code.** DIGI stands ready to contribute our extensive expertise to this effort.
- 16.4. As mentioned, DIGI is supportive of Division 3, and we consider that Division 2 should be removed at this stage, with its proposed obligations reconsidered in the context of the codes to be later developed under the powers afforded in Division 3.

## Summary of requested recommendations in Section D

- X. 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 different to 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, 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 sector<sup>24</sup> 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.*

*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 stage<sup>25</sup>.*

- 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

---

<sup>24</sup> Documents released under the Freedom of Information Act, <https://treasury.gov.au/sites/default/files/2024-09/foi-3675.pdf>

<sup>25</sup> As above, p. 76.





appears to be Ministerial feedback<sup>26</sup>.

- 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 Requested Recommendations in Section 3

- Y. 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.
- Z. Alternatively, if the Government wishes to focus on scam prevention, that should be the sole focus of the Framework.
- AA. Should the Government insist on including an EDR scheme in the 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:

*'...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*

---

<sup>26</sup> As above, p. 123.



*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 2023 Consultation Paper. 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 requested recommendations in Section F

BB. 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 section 58FV(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 requests that the Committee 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.

## 21. Remedial Directions

- 21.1. DIGI submits that the remedial direction power given to the SPF general regulator, being the ACCC, in section 58FZM is too broad. Due to the drafting of the provision, the regulator could rely on the power to require regulated entities to take measures that are disproportionate, unreasonable, unrelated to the purposes and objectives of the SPF, and that may be burdensome and or disruptive to the entity's business. **DIGI requests the Committee recommend that this remedial directions power should be removed from the Bill.**



- 21.2. DIGI shares the view the Law Council of Australia advanced in their submission to the Treasury Consultation on the SPF Exposure Draft.<sup>27</sup> The Law Council raised concerns that such a power may encourage the regulator to take a ‘two-step’ approach to enforcement action, whereby they issue remedial directions prior to commencing civil penalty proceedings<sup>28</sup>.
- 21.3. The ACCC, as the SPF regulator, would still have ample power to engage with regulated entities on proposed changes without the remedial directions power, and changes could be voluntarily agreed or through enforceable undertakings; failing cooperation, the ACCC could seek court orders (as is the case currently).
- 21.4. If the Committee is not of the opinion the remedial directions power should be removed, DIGI submits that as an alternative, it is amended to include safeguards to limit the scope of the regulator’s power to make remedial directions under the SPF to only where it is reasonable and proportionate. DIGI would also request the Committee recommend a formal investigation be required to establish a breach of the SPF principle before a remedial direction could be issued.
- 21.5. We recommend that wording along the following lines be added into 58FZM:
- (2) Before issuing a direction, the SPF Regulator is required to conduct an investigation of the suspected breach of an SPF principle or code obligation and to be satisfied (i) on a balance of probabilities that a breach has occurred; and  
(ii) that any countervailing benefits to the conduct in question do not outweigh the harm caused by the breach.*
- Before making a finding, the SPF Regulator must:  
(i) consider any representations that the regulated company makes in relation to the investigation; and;  
(ii) provide a grace period to permit compliance steps before any enforcement action.*

## Summary of Requested Recommendations in Section G

- CC. DIGI requests the Committee recommend that this remedial directions power should be removed from the Bill.
- DD. Section 58FV(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’.
- EE. DIGI requests the Committee recommend 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.

<sup>27</sup> Law Council of Australia, Submission No 50 to *Treasury Consultation on Scams Prevention Framework Exposure Draft* (17 October 2024), p. 21.

<sup>28</sup> Law Council of Australia, Submission, p. 76



FF. 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.

GG. The remedial directions power given to the SPF regulator should be removed, and if not removed, narrowed in scope so that it may only be used when it is reasonable and proportionate. The power should also have constraints placed upon it, including that an investigation is conducted into the suspected SPF Principle breach prior to issuing a remedial direction.

## H. Appendix

### Item 1 Table of Recommended Changes

Outlined below is a table of some of the recommendations advanced in this submission where specific changes are proposed to the bill. **Note that it is not comprehensive of all of the recommendations advanced in the submission.**

Recommendation	Section of DIGI's Submission	Proposed Section of the Bill	Current Section	Proposed Change
A	A1	N/A	Currently not within the Bill.	That the role of the National Anti-Scam Centre in the SPF be made clear considering the investment the Government has made to it.
B	A2	NA	Currently not within the Bill.	That the Government indicate how it intends to use information gathered under the Framework to share with foreign governments and prosecute organised crime networks running scams from outside Australia.
C	A3	N/A	Currently not within the Bill.	That the Government legislate to give the ACCC the power to issue takedown requests to relevant services of known non-investment scams, with appropriate safeguards on the ACCC's powers, including appeal



				mechanisms.
D	B4	58AC(2)(c)(ii)		That within the sectoral codes, obligations on a social media service be dependent on a platform's self-assessed risk profile.
E	B4	58AC(2)(c)(ii)		That the Government consider how a platform may have some functionalities the SPF does not apply to, and some that the SPF does apply to, and clarify how a platform should act in such circumstances.
F/G	B4	58AC(2)(c)		That Government consider that the SPF Principles and obligations may not be applicable to messaging services, and that ACMA is a more suitable regulator.
H	B4	58AE		That the Government improve data collection about the digital industry so that it may make accurate assessments before designation.
I a and b	B5	58AG	<p><i>A scam is a direct or indirect attempt (whether or not successful) to engage an SPF consumer of a regulated service where it would be reasonable to conclude that the attempt:</i></p> <p><i>(a) involves deception (see subsection (2)); and</i></p> <p><i>(b) would, if successful, cause loss or harm including obtaining SPF personal information of, or a financial or other benefit from, the SPF consumer or the SPF consumer's associates.</i></p>	<p>The definition of a scam be changed to:</p> <p><i>'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 loss'</i></p> <p>Furthermore, the definition of a scam should sit within sector-specific codes and not the overarching legislation.</p>
I c and d	B5	58AG	<i>A scam is a direct or indirect attempt (whether or not successful)</i>	The definition of a scam should be changed to remove



			<p><i>to engage an SPF consumer of a regulated service where it would be reasonable to conclude that the attempt:</i></p> <p><i>(a) involves deception (see subsection (2)); and</i></p> <p><i>(b) would, if successful, cause loss or harm including obtaining SPF personal information of, or a financial or other benefit from, the SPF consumer or the SPF consumer's associates.</i></p>	<p>'personal information' so it reads:</p> <p><i>A scam is a direct or indirect attempt (whether or not successful) to engage an SPF consumer of a regulated service where it would be reasonable to conclude that the attempt:</i></p> <p><i>(a) involves deception (see subsection (2)); and</i></p> <p><i>(b) would, if successful, cause loss or harm including obtaining a financial or other benefit from the SPF consumer or the SPF consumer's associates.</i></p> <p>OR should be changed to</p> <p><i>A scam is a direct or indirect attempt (whether or not successful) to engage an SPF consumer of a regulated service where it would be reasonable to conclude that the attempt:</i></p> <p><i>(a) involves deception (see subsection (2)); and</i></p> <p><i>(b) would, if successful, cause loss or harm including obtaining SPF personal information of, <b>and</b> a financial or other benefit from, the SPF consumer or the SPF consumer's associates.</i></p>
I	B5	58AG	<p><i>A scam is a direct or indirect attempt (whether or not successful) to engage an SPF consumer of a regulated service where it would be reasonable to conclude that the</i></p>	<p>'Indirect attempt' should be removed so the definition reads:</p> <p><i>A scam is a direct attempt</i></p>



			attempt:	(whether or not successful) to engage an SPF consumer of a regulated service where it would be reasonable to conclude that the attempt:
I	B5	58AG	<p>A scam is a direct or indirect attempt (whether or not successful) to engage an SPF consumer of a regulated service where it would be reasonable to conclude that the attempt:</p> <p>(a) involves deception (see subsection (2)); and</p> <p>(b) would, if successful, cause loss or harm including obtaining SPF personal information of, or a financial or other benefit from, the SPF consumer or the SPF consumer's associates.</p>	That the definition of a scam be further re-worked to ensure that over-correction is not necessary to operationalise the SPF.
J	B7	58AI	<p>A regulated entity identifies or has actionable scam intelligence if (and when) there are reasonable grounds for the entity to suspect that a communication, transaction or other activity relating to, connected with, or using a regulated service of the entity is a scam.</p>	<p>That the definition be amended to include the clarification that 'actionable scam intelligence' does not mean merely a singular consumer report about an alleged scam:</p> <p><i>A regulated entity identifies or has actionable scam intelligence if (and when) there are reasonable grounds for the entity to suspect that a communication, transaction or other activity relating to, connected with, or using a regulated service of the entity is a scam. There is not reasonable grounds if there have only been consumer reports about an alleged scam, and there is nothing else present to raise the entity's suspicions.</i></p>





K	B7	58AI	Throughout the Bill.	That the concept of 'actionable scam intelligence'; be used throughout the Bill instead of scam as the threshold point at which any entity has an obligation to act.
L	B8	58AJ	<i>The SPF provisions extend to acts, omissions, matters and things outside Australia.</i>	That extra-territorial application be amended to ensure that a regulated entity would not need to alter the services they provide anywhere in the world:  <i>The SPF provisions extend to acts, omissions, matters and things outside Australia, but do not require a regulated entity to change how its platform operates outside Australia.</i>
M	C9	Division 2	<i>Throughout the Bill</i>	That the SPF should not implement a dual-set of obligations in the primary legislation and the sector-specific codes
O a	C10	58BD	<i>A regulated entity for a regulated sector contravenes this subsection if the entity fails to do one or more of the following: (a) document governance policies and procedures about: (i) preventing, detecting and disrupting scams; and (ii) responding to scams; and (iii) reports relating to scams;  relating to, connected with, or using the entity's regulated services for the sector; (b) implement those governance policies and procedures; (c) develop and implement performance metrics and targets that: (i) are for measuring the</i>	That this section be clarified to state a regulated entity would not be in contravention prior to any anti-scam action taken, and that an entity's obligation at the point a scam surfaces is clarified.



			<p><i>effectiveness of those governance policies and procedures; and</i></p> <p><i>(ii) comply with any requirements for those metrics and targets that are prescribed by the SPF rules.</i></p>	
O b and c	C10	58BE	<p><i>A regulated entity for a regulated sector contravenes this subsection if:</i></p> <p><i>(a) no senior officer of the entity certifies in writing, within 12 months of the day the entity becomes a regulated entity for the sector, whether the entity's SPF governance policies, procedures, metrics and targets for the sector comply with this Subdivision; or</i></p> <p><i>(b) no senior officer of the entity certifies in writing, within 7 30 days after each 12-month anniversary of the day the entity becomes a regulated entity for the sector, whether the entity's SPF governance policies, procedures, metrics and targets for the sector comply with this Subdivision.</i></p>	<p>That the clause be removed OR be amended to include: <i>The senior officer is excluded from liability under this section and other legislation with respect to their duties under this Division.</i></p>
O d and e	C10	58BF and 58BG	<p><i>A regulated entity for a regulated sector contravenes this subsection if:</i></p> <p><i>(a) the SPF general regulator, or the SPF sector regulator for the sector, gives the entity a written request for a copy of:</i></p> <p><i>(i) the entity's SPF governance policies, procedures, metrics and targets for the sector; or</i></p> <p><i>(ii) specified kinds of other records required by this Subdivision to be kept for the sector by the entity; and</i></p> <p><i>(b) the entity fails to comply with the request within:</i></p> <p><i>(i) 10 business days after the day the entity is given the request; or</i></p> <p><i>(ii) such longer period as is allowed by the SPF regulator.</i></p>	<p>That the Government allows flexibility and proportionality about the form these reports take, by adding:</p> <p><i>(c) These reports are not to be in any prescribed form, and entities have flexibility and proportionality with how they meet reporting obligations under this section, unless specifically stated in the sector-specific code.</i></p>



O f	C12	58BM	<i>the regulated entity fails to take reasonable steps to detect a scam relating to, connected with, or using a regulated service of the entity if the entity fails to take reasonable steps to:</i> <i>(a) detect such a scam as it happens; or</i> <i>(b) detect such a scam after it happens</i>	'As it happens' be removed from the section, so it reads:  <i>the regulated entity fails to take reasonable steps to detect a scam relating to, connected with, or using a regulated service of the entity if the entity fails to take reasonable steps to detect such a scam after it happens</i>
O g	C12	58BO	<i>A regulated entity contravenes this subsection if the entity:</i> <i>(a) has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity; and</i> <i>(b) fails to take reasonable steps within a reasonable time to identify the persons who were SPF consumers of that service at the time when the persons were or may have been impacted by the activity.</i>	That this section be removed.
P	D16	Division 3		Government should work with DIGI to develop the mandatory digital industry scams sectoral code and draw upon the model provided in the Australian Online Scams Code.
Q, R, S	E17	Divisions 2 & 4		The EDR and reimbursement scheme should occur through banks, following the UK model, in line with Treasury's original recommendation, OR prevention should be the sole focus of the SPF OR EDR should be included at a later time after extensive industry and consumer consultation.
T	F18	Division 5		ACMA should be the regulator tasked with regulating digital platforms



				for the purposes of scam activity.
U	G19	58FV(5)(c)	<i>any order that the Court considers appropriate directing the person to compensate any other person who has suffered loss or damage as a result of the breach</i>	Narrowing this provision down to: <i>any user who has suffered actual loss or damage as a direct result of a regulated entity's breach"</i>
V	G20	Division 6		The dual penalty regime be removed in favour of a penalty regime enforced by the relevant sectoral regulator, in relation to the sectoral codes.
W	G20			If penalties are retained in the Framework, because of the potential for overcorrection to avoid penalties, a proportional or tiered penalty framework should be implemented instead where fines are levelled for serious or systematic breaches.
X	G21	58FZM	<i>If the SPF general regulator reasonably suspects that a regulated entity: (a) is failing to comply with an SPF principle; or (b) will fail to comply with an SPF principle; the SPF general regulator may, by written notice given to the entity, direct the entity to take specified action to comply with that SPF principle.</i>	This section should be removed OR be amended to state:  <i>If the SPF general regulator reasonably suspects that a regulated entity: (a) is failing to comply with an SPF principle; or (b) will fail to comply with an SPF principle; the SPF general regulator may, by written notice given to the entity, direct the entity to take specified action to comply with that SPF principle. The specified action must be reasonable and proportionate to the scam activity and the entity's size.</i>
X	G21	58FZM	<i>If the SPF general regulator</i>	The following section added



			<p><i>reasonably suspects that a regulated entity:</i></p> <p><i>(a) is failing to comply with an SPF principle; or</i></p> <p><i>(b) will fail to comply with an SPF principle;</i></p> <p><i>the SPF general regulator may, by written notice given to the entity, direct the entity to take specified action to comply with that SPF principle.</i></p>	<p>into 58FZM:</p> <p><i>(2) Before issuing a direction, the SPF Regulator is required to conduct an investigation of the suspected breach of an SPF principle or code obligation and to be satisfied</i></p> <p><i>(i) on a balance of probabilities that a breach has occurred; and</i></p> <p><i>(ii) that any countervailing benefits to the conduct in question do not outweigh the harm caused by the breach.</i></p> <p><i>Before making a finding, the SPF Regulator must:</i></p> <p><i>(i) consider any representations that the regulated company makes in relation to the investigation; and;</i></p> <p><i>(ii) provide a grace period to permit compliance steps before any enforcement action.</i></p>
--	--	--	--	---