Submission to Senate Standing Committee on Economics

Scams Prevention Framework Bill 2024

Public Version

January 2025

EXECUTIVE SUMMARY

1. Optus welcomes the opportunity to provide a submission to the Senate Standing Committee on Economics on the *Scams Prevention Framework Bill 2024* (the SPF Bill).

2. As the Committee is aware, the telecommunications industry has taken strong actions to protect against scams and fraud impacting telecommunications customers and their accounts, and also has taken significant actions to protect other industries and their customers. Even though telecommunications services are not the end target of most scams, as the information highway that connects all Australians, we are aware of the unique position we play in identifying, disrupting and reporting suspicious scam activity that traverses our networks.

3. Optus is a leader in addressing the threats of scams in the telecommunications industry, including blocking almost 500 million scam calls since December 2020, and more than 235 million scam messages since July 2022. Optus has also introduced a range of scam initiatives such as:

   (a) Optus Call Stop, which blocks outbound calls to known impersonation scam numbers and plays a recorded message to inform customers that the number called has been identified as a scam.

   (b) Optus Scam Wise, which provides our customers information on how to spot scams and stay safe online; including the ability to report suspicious SMS messages and the sharing of trending SMS scams.

   (c) Optus Do Not Originate registry, which protects numbers used by Optus corporate customers from misuse by blocking the number from entering the Optus network.

   (d) Optus SMS Sender ID Registry, which prevents specified SMS Alphanumeric Sender IDs from being spoofed by unauthorised entities.

4. Optus has also partnered with Westpac to develop SafeCall, which allows Westpac customers to receive calls via the app that are Westpac branded, verified by Optus and displays a reason for the call. This program provides customers more certainty in the legitimacy of the call, at a time when bank impersonation scams are among the most common scam types impacting Australian customers.[1]

5. Optus supports the policy intent of the SPF Bill – namely, a coordinated multi-industry approach to tackling scams, which includes banks and digital platforms. The challenge for a single, overarching framework as proposed in the SPF Bill is to establish an effective and workable system of industry codes; developed, approved and enforced by competent regulatory bodies.

6. Optus submits that the SPF Bill is unnecessarily complex due to it addressing many issues of detail and process which would be better dealt with via various industry codes. This has resulted in an unworkable and ineffective Bill that risks not achieving many of the goals which we all support. Optus submits that the legislation can be much simpler and more effective by adopting an approach where the SPF principles guide the drafting of effective and strong mandatory industry codes.

[1] https://www.optus.com.au/about/media-centre/media-releases/2024/07/westpac-and-optus-introduce-australian-first-scam-protection

7. Optus' comments in this submission aim to ensure the SPF Bill focuses on developing a framework that enables powerful mandatory industry codes with effective enforcement mechanisms. This is achieved through the enabling legislation providing clear principles which each industry code must address; and by trusting the regulators empowered to facilitate necessary industry expertise to draft mandatory industry codes that are implementable, enforceable and effective.

8. Optus supports an approach, whereby the SPF Bill contains principles (Division 2) to guide the development of industry codes (Division 3) which can be targeted at the specific issues and deficiencies identified in designated sectors. Optus supports this approach as:

   (a) it ensures the industry codes can be targeted at critical deficiencies in a specific sector to deliver immediate real-world benefits in an efficient and streamlined way;

   (b) it avoids increased complexity from duplicated obligations; and

   (c) it does not prohibit the development of future innovative responses and solutions to disrupt scam activity and can better respond to changes in a highly technical and dynamic industry, such as telecommunications, as scammers constantly evolve their approach.

9. Optus submits that this is achieved by focusing on three key changes:

   (a) Remove civil liability provisions in Division 2 of the SPF Bill so that liability attaches only for non-compliance with SPF codes under Division 3. Alternatively, compliance with SPF codes under Division 3 should be deemed to be a reasonable step under Division 2.

   (b) Re-draft Division 2 so that each principle provides guidance to the development of SPF codes under Division 3. Division 2 should make it mandatory for SPF codes to address each of the principles.

   (c) Ensure that Division 6 delivers simple, fast and effective redress for consumer harm. Division 6 should clarify that IDF, EDF, and regulator actions focus on compensating consumers for any loss incurred as a result of non-compliance with SPF codes under Division 3. Division 6 Subdivision C (damages provisions) should be removed as it should never be required with effective EDF and regulatory actions, and it creates material unintended consequences which works against consumers receiving fast, simple and effective redress.

10. Proposed drafting changes to the SPF Bill are included in Appendix 1 below.

11. To assist the Committee, we do not repeat in this submission the broader policy points raised in our previous submission to Treasury in October 2024. We attach that submission in Appendix 2 below should the Committee wish to review.

KEY ISSUES WITH THE CURRENT BILL

12. While we do not wish to repeat in detail previous comments made to the Treasury by Optus and others reflecting the opportunities for improvements to the SPF Bill, to assist the Committee we provide a brief summary of the main issues below.

Duality of liability across Division 2 and Division 3

13. The central issue with the drafting of the SPF Bill is the duality of liability across Division 2 and Division 3. That is, the requirement to be compliant with the over-arching principles and also be compliant with the specific SPF industry codes.

14. The broad drafting of the proposed framework obligations in Division 2 creates considerable regulatory uncertainty, particularly where there are multiple regulators enforcing the industry-specific regulations under Division 3 and the SPF Principles under Division 2. This issue is magnified by the definition of reasonable steps in s.58BB, which indicates that compliance with industry codes is merely one relevant matter amongst several to be considered rather than deemed to be a reasonable step.

15. This drafting could lead to a scenario of dual liability – where a scam occurs and despite a telecommunications company being compliant with the requirements of the industry code developed under Division 3, another regulator or court may take the view that the company did not take reasonable steps as required by the overarching principles outlined in Division 2. This is particularly likely where other matters such as customer base and size of a company are equal matters to be considered under reasonable steps. The drafting in s.58BB could mean that small telecommunications companies with few customers need only be compliant with industry codes; but the larger telecommunications companies with large customer bases are expected to undertake further, undefined actions which is unknown at the time. It is not clear this is consistent with the intent of the policy.

16. This duality of liability across Division 2 and Division 3, combined with the drafting of reasonable steps under s.58BB, leads to regulatory uncertainty and implementation complexity given the highly technical nature of providing telecommunications services and implementing scam detection, prevention and disruption measures across the whole telecommunications ecosystem. It will likely undermine the intent of the SPF Bill and reduce the effectiveness of the scam framework – a framework which we all support.

17. Optus submits that this can be addressed by removing the civil liability elements in Division 2 and relying on civil liability through industry codes under Division 3. Division 2 should also be amended to make it clear that the principles must be included in industry codes under Division 3.

Protracted consumer redress in Division 6

18. Optus strongly supports the intent of the SPF Bill to provide simple, fast and effective redress for consumer harm. We support the requirement for regulated entities to have dedicated internal dispute resolution processes and be members of an approved external dispute resolution scheme. We note that the telecommunications industry is already subject to both obligations under existing telecommunications laws.

19. Effective internal and external dispute resolution processes combined with a strong and effective regulatory investigation and enforcement powers will ensure that consumer losses as a result of non-compliance with the SPF rules can be addressed swiftly and without cost to impacted consumers.

20. However, Optus is concerned that Division 6 of the SPF Bill does not achieve this objective as it appears that the Bill has listed all possible form of redress rather than propose a process for simple, fast and effective redress for consumer harm.

21. Where a customer suffers harm due to a regulated entity not being compliant with industry codes, the customer can seek redress through:

    (a) Internal dispute processes;

    (b) Independent external dispute resolution scheme;

    (c) Regulator action including:

        (i) Fines;

        (ii) Enforceable undertakings;

        (iii) Public warnings;

        (iv) Remedial directions;

        (v) Adverse publicity orders;

        (vi) Non-punitive Court orders; and

        (vii) Court orders to redress loss of damage.

22. Additionally, after all of the above possible actions are exhausted, there lies under subdivision G the option for action for damages up to 6 years after the scam event. It is not clear what type of loss will not be redressed through the 9 possible actions above and which requires the addition of a private action for damages up to 6 years after the event.

23. Optus does not see that subdivision G adds any benefit that will not be achieved through the other methods of enforcement in Division 6, but we do see that it adds considerable risk and intended consequences. It is foreseeable that actions for damages could be used by corporate class action litigants at a time materially after the scam activity occurred – up to 6 years post the event. The focus of enforcement must be on ensuring a system that delivers simple, fast and effective redress. Allowing corporate class actions litigants to instigate action for damages which could take many years to proceed through the courts, will not deliver this outcome.

24. The Committee may view that a backstop of an action for damages is required to protect consumers where the possible actions undertaken by an independent external resolution body and by the appointed SPF regulator(s) do not provide satisfactory consumer redress. While Optus does not consider such a scenario likely, Optus would prefer that any potential defects in Division 6 of the SPF Bill be addressed through necessary amendments that provide sufficient certainty that the EDR process; and actions by the SPF regulator(s), would prioritise simple, fast and effective redress for consumer harm. Optus submits if this is achieved, there is no need for subdivision G.

PROPOSED AMENDMENTS TO DIVISION 2

25. Optus has proposed several amendments to Division 2 to give effect to the principles above.

26. The intent of the changes listed in the table below is to amend the clauses in Division 2 from a focus on compliance and penalty provisions to being clauses that mandate topics that must be addressed by SPF industry codes in Division 3. For example, we suggest that:

    (a) s.58BD be amended to make clear that SPF codes must require that regulated entities have documented governance policies and procedures to prevent, respond to and report scams. This change will ensure that SPF codes address this issue and contain the detailed compliance obligations.

27. Related to these drafting changes, Optus also suggests that several clauses be deleted as they contain detail which would be better contained in SPF codes rather than overarching enabling legislation. For example, s.58BF and s.58BG are not required under this structure as they contain detailed record keeping and reporting which would be better dealt with in industry codes. To be clear, Optus agrees that there should be record keeping and reporting obligations, but again, these obligations are not best located in enabling legislation.

28. In addition to these comments, Optus also wishes to highlight our suggestion to amend s.58BZA, to remove the 28-day limit to the safe harbour provisions. This limitation was added after industry consultation and we have yet to provide comment on this issue.

29. Optus supports safe harbour provisions for taking action when advised of actionable scam intelligence. But it is not clear that an explicit time limit will add any benefits. Optus submits that the starting point should be that where a regulated entity is required to take action when provided with actionable scam intelligence under these provisions, that entity should be protected from liability for that action.

30. Importantly, s.58BZA(2)(e) requires that a regulated entity promptly reverses an action once it is identified that the activity is not a scam. Optus strongly submits that this clause is sufficient. In telecommunications, this provision is sufficient to ensure incorrect blocking of legitimate traffic is addressed. We also note that reflects current practices of Optus.

31. The inclusion of a 28-day hard limit also means that a telco could be liable even where it has not been advised that its scam disruption activity has impacted legitimate traffic. Optus reiterates that the focus of this provisions should be that regulated entities take quick corrective measures when advised of legitimate traffic being impacted by disruption actions.

32. We note that a time limit may be relevant for other industries, such as banking, where action may include barring access to a person's funds, which can have material impacts on that person. However, this level of detail would be best placed within the industry code for that industry.

PROPOSED AMENDMENTS TO DIVISION 6

33. Optus suggests changes in Division 6 to reflect the removal of civil penalty provisions from Division 2. We also submit that subdivision G of Division 6 be deleted – as outlined above. That is, remove s.58FZC through to s.58ZK.

CONSEQUENTIAL AMENDMENTS

34. Optus submits that consequential amendments may be required to the *Telecommunications (Interception And Access) Act 1979* (the TIA Act) to give full effect to the SPF Bill in the telecommunications industry. The TIA Act prohibits network operators from intercepting traffic carried over that network unless allowed for by the TIA Act, which typically requires warrants by law enforcement agencies.

35. It is foreseeable that the SPF Bill and associated industry codes may impose obligations on telecommunications companies to conduct interrogation of traffic over their networks to identify or respond to scams. While we do not yet know the details nor whether this issue is likely (this would be decided under industry codes), there is a potential issue if requirements under the SPF Bill require actions that would otherwise raise issues under the TIA Act. Optus believes it would be prudent to address any potential area of conflict by making clear in the TIA Act that actions conducted pursuant to Part IVF of the *Competition and Consumer Act 2010* do not breach obligations under the TIA Act.

Appendix 1: Recommended amendments to the *Scams Prevention Framework Bill 2024*

DIVISION 2 Overarching principles of the Scams Prevention Framework		
Section	**Proposed Changes**	**Reason**
58BB	**58BB Meaning of *reasonable steps*** (1) Matters relevant to whether a regulated entity has taken ***reasonable steps*** for the purposes of a provision of this Division include: (a) the size of the regulated entity; and (b) the kind of regulated services concerned; and (c) the consumer base of those services; and (d) the kinds of scam risks those services face; and ~~(e) whether the regulated entity has complied with any relevant SPF code obligations relating to that provision~~ (2) A regulated entity has taken *reasonable steps* if it has complied with any relevant SPF code obligations relating to that provision.	Note that this change may not be required if Division 2 is reworked to reflect that principles guide the development of the SPF Code; and that regulated entities must comply with SPF Codes.
58BD	**58BD Documenting and implementing governance policies and procedures~~— civil penalty provision~~** (1) The SPF Code ~~Each regulated entity~~ for a regulated sector must require that Regulated Entities ~~contravenes this subsection if the entity fails to do one or more of~~ ~~the following~~:	Suggested amendments to give effect to make this clause outline that SPF Codes contain this type of obligations, and to

	(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 effectiveness of those governance policies and procedures; ~~and~~ ~~(ii)comply with any requirements for those metrics and targets that are prescribed by the SPF rules~~. ~~(2)Subsection (1) is a civil penalty provision.~~ ~~Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).~~	transfer civil liability to the associated industry code.
58BE	**58BE Annual certification about SPF governance policies, procedures, metrics and targets~~ civil penalty provision~~** (1) The SPF Code ~~A regulated entity~~ for a regulated sector must require that Regulated Entities ~~contravenes this subsection if~~: (a) A ~~no~~ senior officer of the entity certify ~~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 complies with the SPF Code ~~this Subdivision; or~~ ~~(b) no senior officer of the entity certifies in writing, within 7 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.~~ ~~(2) Subsection (1) is a civil penalty provision~~	Suggested amendments to give effect to make this clause outline that SPF Codes contain this type of obligations, and to transfer civil liability to the associated industry code.

58BF	**~~58BF Record keeping of compliance with SPF provisions—civil penalty provision~~** ~~(1) A regulated entity for a regulated sector contravenes this subsection if the entity fails to keep records of information of a material nature relating to each of the following activities for at least 6 years after that activity happens:~~ ~~(a)the initial documenting, and each revision of the documenting, of the entity's SPF governance policies, procedures, metrics and targets for the sector;~~ ~~(b)the initial implementation, and each reimplementation, of those SPF governance policies, procedures, metrics and targets;~~ ~~(c)each consideration (including certification) by one of the entity's senior officers of those SPF governance policies, procedures, metrics and targets, including in relation to their documenting, implementation and review;~~ ~~(d)any other activities that are prescribed by the SPF rules.~~ ~~(2)Subsection (1) is a civil penalty provision.~~ ~~Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).~~	This level of detail is better contained in the SPF Code. Noting that different industries have different record keeping obligations under their relevant sector-specific regulations. It is important to maintain consistency across record keeping obligations to minimise risks around cyber and privacy.
58BG	**~~58BG Reporting about compliance with this Subdivision—civil penalty provision~~** ~~(1)A regulated entity for a regulated sector contravenes this subsection if:~~ ~~(a)the SPF general regulator, or the SPF sector regulator for the sector, gives the entity a written request for a copy of:~~ ~~(i)the entity's SPF governance policies, procedures, metrics and targets for the sector; or~~ ~~(ii)specified kinds of other records required by this Subdivision to be kept for the sector by the entity; and~~ ~~(b)the entity fails to comply with the request within:~~ ~~(i)10 business days after the day the entity is given the request; or~~ ~~(ii)such longer period as is allowed by the SPF regulator.~~ ~~(2)Subsection (1) is a civil penalty provision.~~ ~~Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties)~~	This level of detail is better contained in the SPF Code.

58BH	~~**58BH Sector-specific details can be set out in SPF codes**~~ ~~For the purposes of (but without limiting) subsection 58CC(1), the SPF code for a regulated sector may include sector-specific provisions describing:~~ ~~(a)the matters that a regulated entity for the sector must include in the entity's governance policies and procedures for the purposes of this Subdivision; or~~ ~~(b)the factors that a regulated entity for the sector must have regard to when developing the entity's governance policies and procedures for the purposes of this Subdivision~~.	This provision is not required under the proposed structure where Division 2 outlines the principles that must be addressed in SPF Codes.
58BJ	**58BJ Taking reasonable steps to prevent scams from being committed~~—civil penalty provision~~** (1) The SPF Code for a regulated sector must require that Regulated Entities ~~A regulated entity contravenes this subsection if the entity fails to~~ take reasonable steps to prevent another person from committing a scam relating to, connected with, or using a regulated service of the entity. Note: Sections 58GA to 58GC extend the meaning of ***person*** for partnerships, unincorporated associations and trusts. ~~(2) Subsection (1) is a civil penalty provision.~~ ~~Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).~~	Suggested amendments to give effect to make this clause outline that SPF Codes contain this type of obligations, and to transfer civil liability to the associated industry code.
58BK	**58BK Further detail about certain concepts** ~~(1) Taking reasonable steps for the purposes of subsection 58BJ(1) requires more than merely acting on actionable scam intelligence in the form of information provided to the regulated entity by another person.~~	Details are better contained in SPF Codes rather than primary enabling legislation. Removing obligation to report information about scams to consumers as this would require telcos to provide massive amounts

	~~*Further sector-specific details can be set out in SPF codes*~~ (~~2~~1) For the purposes of (but without limiting) subsection 58CC(1), the SPF code for a regulated sector may include sector-specific provisions: ~~(a) describing what are reasonable steps for the purposes of this Subdivision (see also section 58BB); or~~ (b) requiring each regulated entity for the sector to: (i) identify its SPF consumers who are at risk of being targeted by a scam; or (ii) identify its SPF consumers who have a higher risk of being targeted by a scam.~~; or~~ ~~(c) requiring each regulated entity for the sector to provide information about such scams to an SPF consumer described in subparagraph (b)(i) or (ii).~~	of information (noting that Optus blocks around 1m scam SMSs and 1m scam calls a month). Information about public reporting should be outlined in the reporting principles, with details contained in SPF Codes not primary enabling legislation.
58BM	**58BM Taking reasonable steps to detect scams~~ — civil penalty provision~~** (1) The SPF Code for a regulated sector must require that Regulated Entities ~~A regulated entity contravenes this subsection if the entity fails to~~ take reasonable steps to detect a scam relating to, connected with, or using a regulated service of the entity. ~~(2) Subsection (1) is a civil penalty provision.~~ ~~Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).~~ ~~(3) Without limiting subsection (1), 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:~~ ~~(a) detect such a scam as it happens; or~~ ~~(b) detect such a scam after it happens.~~ ~~Note:For further details about the meaning of reasonable steps, see sections 58BB and 58BP.~~	Suggested amendments to give effect to make this clause outline that SPF Codes contain this type of obligations, and to transfer civil liability to the associated industry code. Suggest deletion as this level of detail is best outlined in SPF Codes rather than in enabling primary legislation.

58BN	**58BN Investigating actionable scam intelligence~~— civil penalty provision~~** (1) The SPF Code for a regulated sector must require that Regulated Entities take reasonable steps to investigate whether or not the activity is a scam if the entity: (a)has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity; ~~and~~ ~~(b)fails to during the 28-day period starting on the day that the intelligence becomes actionable scam intelligence for the entity.~~ ~~(2) Subsection (1) is a civil penalty provision.~~ ~~Note:This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).~~	Suggested amendments to give effect to make this clause outline that SPF Codes contain this type of obligations, and to transfer civil liability to the associated industry code.
58BO	~~**58BO Identifying impacted SPF consumers — civil penalty provision**~~ ~~(1) A regulated entity contravenes this subsection if the entity:~~ ~~(a)has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity; and~~ ~~(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.~~ ~~(2) Subsection (1) is a civil penalty provision.~~ ~~Note:This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).~~	The details of this provision is best left for SPF Codes. There will be different impacts for different industries. For instance, in the telecommunications industry this clause would requires all telcos to contact all customers who ever received a scam SMS or call. Given the millions of potential contacts per month, this could entrail many customers receiving many additional contacts by a range of different telco companies. Should this obligation be retained, it should be limited to scams related directly to the regulated service of an entity. Ie, a bank should contact customers subject to a bank-related scam. Telcos to contact their

		customers if the scam relates to their telco service.
58BP	~~**58BP Sector-specific details can be set out in SPF codes**~~ ~~For the purposes of (but without limiting) subsection 58CC(1), the SPF code for a regulated sector may include sector-specific provisions describing:~~ ~~(a)what are reasonable steps (see also section 58BB); or~~ ~~(b)what is a reasonable time;~~ ~~for the purposes of this Subdivision.~~	Clause is not required under proposed structure.
58BR	**58BR Reporting actionable scam intelligence to SPF regulators~~ civil penalty provision~~** (1) This section applies if a regulated entity has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity. ~~*Civil penalty provision*~~ (2) The SPF Code for a regulated sector must require that Regulated Entities ~~The entity contravenes this subsection if the entity fails to~~ give a report about the actionable scam intelligence: (a) to the SPF general regulator within the period, and in the manner and form, prescribed by the SPF rules; and (b) that contains the kinds of information prescribed by the SPF rules. Note: This subsection only applies to the entity when the SPF rules prescribe matters for paragraphs (a) and (b) that apply to the entity. ~~(3) Subsection (2) is a civil penalty provision.~~	Suggested amendments to give effect to make this clause outline that SPF Codes contain this type of obligations, and to transfer civil liability to the associated industry code. Defence provision not required in new structure, where the details are contained in the SPF Rules.

	~~Note: This means subsection (2) is a civil penalty provision of an SPF principle for the purposes of section 58FJ (about civil penalties).~~ ~~*Defence*~~ ~~(4) Subsection (2) does not apply to the entity if circumstances of a kind prescribed by the SPF rules apply to the entity.~~ ~~Note: A defendant bears an evidential burden in relation to the matter in this subsection (see section 96 of the Regulatory Powers Act).~~ *Matters relevant to reports* (5) For the purposes of (but without limiting) subsection (2), the SPF rules may prescribe: (a) that the report may be given via access to a specified data gateway, portal or website; and (b) that the report include the sources or evidence that the entity has for that intelligence (see section 58AI); and (c) different matters for different kinds of regulated entities. Note: For more about the data gateways, portals or websites referred to in paragraph (a), see section 58BT. (6) The report may be required to include SPF personal information.	
~~**58BS**~~	~~**58BS Reporting scams to SPF regulators—civil penalty provisions**~~ ~~(1) This section applies if an SPF regulator gives a written request to a regulated entity for the entity to give the SPF regulator a report about a scam relating to, connected with, or using a regulated service of the entity.~~ ~~*Civil penalty provision*~~ ~~(2) The entity contravenes this subsection if the entity fails to give a report about the scam:~~ ~~(a) to the SPF regulator within the period, and in the manner and form, set out in the request; and~~ ~~(b) that contains the kinds of information set out in the request.~~	Suggested amendments to give effect to make this clause outline that SPF Codes contain this type of obligations, and to transfer civil liability to the associated industry code. Agree with the intent of the clause, namely that regulated entities must respond to written requests for information. Also note that the ACMA and the ACCC both have

	~~(3) Subsection (2) is a civil penalty provision.~~ ~~Note: This means subsection (2) is a civil penalty provision of an SPF principle for the purposes of section 58FJ (about civil penalties).~~ ~~(4) For the purposes of (but without limiting) subsection (2), the SPF regulator's request may:~~ ~~(a) provide that the report may be given via access to a specified data gateway, portal or website; and~~ ~~(b) ask that the report set out:~~ ~~(i) what loss or harm may have resulted from the scam, what disruptive actions the entity has taken and whether any of those actions have been reversed; and~~ ~~(ii) what steps the entity is taking to disrupt similar scams, and to prevent loss or harm resulting from similar scams.~~ ~~Note: For more about the data gateways, portals or websites referred to in paragraph (a), see section 58BT.~~ ~~(5) The request may ask for the report to include SPF personal information. If so, the request must require the entity to de-identify the information unless the SPF regulator reasonably believes that doing so would not achieve the object of this Part.~~ ~~(6) If:~~ ~~(a) a regulated entity gives a scam report to an SPF regulator under this section; and~~ ~~(b) another SPF regulator later requests a scam report under this section from the regulated entity about the same matters;~~	mandatory information gathering powers under the Telco Act and CCA which covers this issue. Given the already existing legislative powers to mandatory compel provision of information, consideration of whether additional powers is needed should be considered under the code development process.
58BX	**58BX Taking reasonable steps to disrupt activities that are the subjects of actionable scam intelligence~~ civil penalty provision~~** (1) The SPF Code for a regulated sector must require that if a Regulated Entity ~~A regulated entity contravenes this subsection if the entity~~ ~~(a)~~ has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity; ~~and~~	Suggested amendments to give effect to make this clause outline that SPF Codes contain this type of obligations, and to transfer civil liability to the associated industry code.

	(~~a~~b) it must ~~fails to~~ take reasonable steps within a reasonable time to: (i) disrupt the activity; or (ii) prevent loss or harm (including further loss or harm) arising from the activity. ~~(2) Subsection (1) is a civil penalty provision.~~ ~~Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).~~ (~~2~~3) For the purposes of subsection (1), the steps taken should be proportionate to the actionable scam intelligence that the entity has. Note 1: For example, if a bank has received a substantial number of similar reports of suspicious activities, it may be appropriate to pause or delay authorised push payments while the bank investigates these suspicious activities. Note 2: For further details about the meaning of reasonable steps, see sections 58BB and 58BZ.	
58BY	**58BY Reporting about the outcomes of investigations of activities that are the subjects of actionable scam intelligence~~ — civil penalty provision~~** (1) This section applies if a regulated entity has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity. ~~*Civil penalty provision*~~ (2) The SPF Code for a regulated sector must require that a Regulated Entity ~~The entity contravenes this subsection if the entity fails to~~ give a report about the actionable scam intelligence: (a) to the SPF general regulator: (i) before the end of the period prescribed by the SPF rules that starts at the end of the period referred to in paragraph 58BZA(2)(d) for that intelligence; and (ii) in the manner and form prescribed by the SPF rules; and (b) that contains the kinds of information prescribed by the SPF rules. Note:This subsection only applies to the entity when the SPF rules prescribe matters for paragraphs (a) and (b) that apply to the entity.	Suggested amendments to give effect to make this clause outline that SPF Codes contain this type of obligations, and to transfer civil liability to the associated industry code.

	~~(3) Subsection (2) is a civil penalty provision.~~ ~~Note: This means subsection (2) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).~~ (~~3~~4) For the purposes of (but without limiting) subsection (2), the SPF rules may prescribe: (a) that the report may be given via access to a specified data gateway, portal or website; and (b) that the report set out whether the entity reasonably believes that the activity that is the subject of the intelligence is a scam; and (c) different matters for different kinds of regulated entities. Note: For more about the data gateways, portals or websites referred to in paragraph (a), see section 58BT. (~~4~~5) The report may be required to include SPF personal information. (~~5~~6) A duty of confidence owed under an agreement or arrangement is of no effect to the extent that it is contrary to this section.	
	~~**58BZ Sector-specific details can be set out in SPF codes**~~ ~~For the purposes of (but without limiting) subsection 58CC(1), the SPF code for a regulated sector may include sector-specific provisions:~~ ~~(a) describing what are reasonable steps (see also section 58BB), or what is a reasonable time, for the purposes of this Subdivision; or~~ ~~(b) requiring each regulated entity for the sector to provide its SPF consumers with information about activities that are the subjects of the entity's actionable scam intelligence.~~	Not required under the new structure, where the details of the obligations including defining reasonable steps and reasonable time.
58BZA	**58BZA Safe harbour for taking actions to disrupt an activity while investigating whether the activity is a scam** (1) This section applies if a regulated entity has actionable scam intelligence about an activity relating to, connected with, or using a regulated service of the entity.	Optus supports safe harbour provisions for taking action when advised of actionable scam intelligence.

	(2) The regulated entity is not liable in a civil action or civil proceeding for taking action to disrupt the activity if the action: (a) is taken in good faith; and (b) is taken in compliance with the SPF provisions; and (c) is reasonably proportionate to the activity, and to information that would reasonably be expected to be available to the entity about the activity; ~~and~~ ~~(d) is taken during the period:~~ ~~(i) starting on the day that the intelligence becomes actionable scam intelligence for the entity; and~~ ~~(ii) ending when the entity reasonably believes that the activity is or is not a scam, or after 28 days, whichever is the earlier; and~~ (e) is promptly reversed if: (i) the entity identifies that the activity is not a scam; and (ii) it is reasonably practicable to reverse the action. Note: Assume the regulated entity temporarily blocks an SPF consumer's website while investigating whether an activity relating to the website is a scam. This subsection protects the regulated entity from civil actions brought by the consumer when the regulated entity is acting appropriately. (3) For the purposes of paragraph (2)(c), matters relevant to whether the action is reasonably proportionate to the activity include: (a) the potential loss or damage to SPF consumers, or to persons carrying on the activity, if the action is not taken; and (b) the potential loss or damage to SPF consumers, or to persons carrying on the activity, if the action is taken and the activity is not a scam.	Not clear why there is a time limit imposed for this action. Where a regulated entity is required to take action when provided with actionable scam intelligence under these provisions, that entity should be protected from liability for that action. In telecommunications, there is a risk that legitimate traffic is impacted when increasing the level of blocking and protections. However, there is no need for a time limit of protections. Optus notes that there remains an explicit obligation to promptly reverse actions when advised that blocking has impacted non scam traffic. This provision is sufficient to ensure incorrect blocking of legitimate traffic is addressed. We also note that reflects current practices of Optus. The inclusion of a 28 day hard limit also means that a telco could be liable even where it has not been advised that its scam disruption activity has impacted legitimate traffic. Optus reiterates that the focus of this provisions should be that regulated entities take quick corrective measures when advised of legitimate traffic that is being impacted by disruption actions.

		Time limit may be relevant for other industries such as banking where action may include barring access to a person's funds – which can have material impacts on that person. However, in the context of telecommunications blocking does not have such impact. Providing that a telco promptly reverses a block, the impact is minimal.
58BZC	**58BZC Enabling SPF consumers to easily report activities that are or may be scams~~— civil penalty provision~~** (1) The SPF Code for a regulated sector must require that a Regulated Entity ~~A regulated entity contravenes this subsection if the entity does not~~ has an accessible mechanism for a person to report to the entity an activity that: (a) is or may be a scam; and (b) relates to, is connected with, or uses a regulated service of the entity; and (c) impacts the person at a time when the person is an SPF consumer of the service. Note: The reporting mechanism will need to extend to scams impacting the person at a time when the regulated service is only purportedly being provided to the person (see subsection 58AH(1) (about the meaning of SPF consumer)). ~~(2) Subsection (1) is a civil penalty provision.~~ ~~Note: This means subsection (1) is a civil penalty provision of an SPF principle for the purposes of section 58FJ (about civil penalties~~).	Reflects new structure where the principles mandate what is to be dealt with in the SPF Code, while leaving the detail for the SPF Code to determine relevant to each regulated industry

58BZD	**58BZD Having an accessible and transparent internal dispute resolution mechanism~~ – civil penalty provision~~** (1) The SPF Code for a regulated sector must require that a Regulated Entity ~~A regulated entity contravenes this subsection if the entity does not~~ has an accessible and transparent internal dispute resolution mechanism to deal with a person's complaint about: (a) an activity that: (i) is or may be a scam; and (ii) relates to, is connected with, or uses a regulated service of the entity; and (iii) impacts the person at a time when the person is an SPF consumer of the service; or (b) the entity's conduct relating to an activity of a kind described in paragraph (a). ~~(2) Subsection (1) is a civil penalty provision.~~ ~~Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).~~	Reflects new structure where the principles mandate what is to be dealt with in the SPF Code, while leaving the detail for the SPF Code to determine relevant to each regulated industry
58BZE	**~~58BZE Having regard to processes and guidelines when undertaking internal dispute resolution – civil penalty provision~~** ~~(1) A regulated entity contravenes this subsection if the entity:~~ ~~(a) is undertaking internal dispute resolution in dealing with a person's complaint of a kind described in paragraph 58BZD(1)(a) or (b); and~~ ~~(b) in doing so, the entity fails to have regard to:~~ ~~(i) any process prescribed by the SPF rules for undertaking internal dispute resolution; or~~ ~~(ii) any guidelines prescribed by the SPF rules for apportioning any liability arising from the complaint.~~	Provision not required given new structure where the principles mandate what is to be dealt with in the SPF Code, while leaving the detail for the SPF Code to determine relevant to each regulated industry

	~~(2) Subsection (1) is a civil penalty provision.~~ ~~Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).~~	
58BZF	**58BZF Publishing information about reporting and dispute resolution mechanisms~~— civil penalty provision~~** (1) The SPF Code for a regulated sector must require that a Regulated Entity ~~A regulated entity for a regulated sector contravenes this subsection if the entity fails to make~~ provides publicly accessible information about the rights of SPF consumers of the entity's regulated services for the sector under: (a) the reporting mechanism required by subsection 58BZC(1); or (b) the internal dispute resolution mechanism required by subsection 58BZD(1); or (c) if the entity is a member of an SPF EDR scheme for the sector—the SPF EDR scheme. ~~(2) Subsection (1) is a civil penalty provision.~~ ~~Note: This means subsection (1) is a ***civil penalty provision of an SPF principle*** for the purposes of section 58FJ (about civil penalties).~~	Reflects new structure where the principles mandate what is to be dealt with in the SPF Code, while leaving the detail for the SPF Code to determine relevant to each regulated industry
58BZG	**58BZG SPF external dispute resolution schemes~~— civil penalty provisions~~** ~~*Regulated entity must not provide a regulated service if the entity is not a member of an SPF EDR scheme*~~ (1) The SPF Code for a regulated sector must require that a Regulated Entity which provides a regulated service for the sector that has one or more SPF consumers is a member of an SPF EDR scheme for the sector ~~A regulated entity for a regulated sector contravenes this subsection if the entity~~:	Reflects new structure where the principles mandate what is to be dealt with in the SPF Code, while leaving the detail for the SPF Code to determine relevant to each regulated industry

	~~(a) provides a regulated service for the sector that has one or more SPF consumers; and~~ ~~(b) is not a member of an SPF EDR scheme for the sector.~~ ~~*Regulated entity that is a member of an SPF EDR scheme must give reasonable assistance to, and cooperate with, the scheme operator*~~ (~~2) A regulated entity for a regulated sector contravenes this subsection if the entity:~~ ~~(a) is a member of an SPF EDR scheme for the sector; and~~ ~~(b) fails to give reasonable assistance to, or cooperate with, the operator of the scheme.~~ ~~*Regulated entity that is a member of an SPF EDR scheme must comply with related obligations in an SPF code*~~ ~~(3) A regulated entity for a regulated sector contravenes this subsection if the entity:~~ ~~(a) is a member of an SPF EDR scheme for the sector; and~~ ~~(b) fails to comply with an obligation in the SPF code for the sector that relates to the scheme.~~ ~~*Civil penalty provisions*~~ ~~(4) Subsections (1), (2) and (3) are civil penalty provisions.~~ ~~Note: This means these subsections are ***civil penalty provisions of an SPF principle*** for the purposes of section 58FJ (about civil penalties).~~	Clause (3) contains detail that is best contained in the APF Code.
58BZH	**~~58BZH Sector-specific details can be set out in SPF codes~~** ~~For the purposes of (but without limiting) subsection 58CC(1), the SPF code for a regulated sector may include sector-specific provisions setting out:~~	Reflects new structure where the principles mandate what is to be dealt with in the SPF Code, while leaving the detail for the SPF

	~~(a) conditions that must be met for a reporting mechanism required by subsection 58BZC(1); or~~ ~~(b) conditions (such as standards and requirements) that must be met for an internal dispute resolution mechanism required by subsection 58BZD(1); or~~ ~~(c) obligations that must be met in relation to an SPF EDR scheme for the sector by a regulated entity for the sector that is a member of the scheme.~~	Code to determine relevant to each regulated industry Clause not required under proposed new structure.
Division 6 – Enforcing the Scams Prevention Framework		
Section	**Changes**	**Reason**
58FJ	**58FJ Civil penalty provisions** *Enforcing civil penalty provisions* (1) Each of the following is enforceable under Part 4 of the Regulatory Powers Act: ~~(a) a civil penalty provision of an SPF principle;~~ (~~a~~b) a civil penalty provision of an SPF code. Note: Part 4 of the Regulatory Powers Act allows a civil penalty provision to be enforced by obtaining an order for a person to pay a pecuniary penalty for the contravention of the provision.	Reflects proposed new structure and that there no longer exists any civil penalty provisions in Division 2.
58FK	**58FK Maximum penalty ~~for tier 1~~ contraventions** (1) Despite subsection 82(5) of the Regulatory Powers Act, the pecuniary penalty payable by a person: (a) under an SPF civil penalty order; and	Update the maximum penalty sections to reflect that liability occurs only with SPF Code provisions. This simplifies the proposed two tier system which has

	(b) a civil penalty provision of an SPF code ~~for a contravention of a civil penalty provision of an SPF principle in any of Subdivisions C, D, F or G of Division 2 of this Part;~~ must not be more than the maximum penalty amount worked out under this section for such a contravention by the person. *Maximum amount of civil penalty for bodies corporate* (2) For the purposes of subsection (1), the maximum penalty amount for such a contravention by a body corporate is the greater of the following: (a) 159,745 penalty units; (b) if the relevant court (see subsection 58FJ(3)) can determine the total value of the benefit that: (i) the body corporate; and (ii) any body corporate related to the body corporate; have obtained directly or indirectly and that is reasonably attributable to the contravention—3 times that total value; (c) if that court cannot determine that total value—30% of the adjusted turnover of the body corporate during the breach turnover period for the contravention. *Maximum amount of civil penalty for other persons* (3) For the purposes of subsection (1), the maximum penalty amount for such a contravention by a person other than a body corporate is 7,990 penalty units.	different maximum penalties for contraventions against Division 2 and Division 3 obligations. Optus proposes that the maximum penalty apply to SPF Codes.

58FL	~~**58FL Maximum penalty for tier 2 contraventions**~~ ~~(1) Despite subsection 82(5) of the Regulatory Powers Act, the pecuniary penalty payable by a person:~~ ~~(a) under an SPF civil penalty order; and~~ ~~(b) for a contravention of:~~ ~~(i) a civil penalty provision of an SPF principle in Subdivision B or E of Division 2 of this Part; or~~ ~~(ii) a civil penalty provision of an SPF code;~~ ~~must not be more than the maximum penalty amount worked out under this section for such a contravention by the person.~~ ~~*Maximum amount of civil penalty for bodies corporate*~~ ~~(2) For the purposes of subsection (1), the maximum penalty amount for such a contravention by a body corporate is the greater of the following:~~ ~~(a) 31,950 penalty units;~~ ~~(b) if the relevant court (see subsection 58FJ(3)) can determine the total value of the benefit that:~~ ~~(i) the body corporate; and~~ ~~(ii) any body corporate related to the body corporate;~~ ~~have obtained directly or indirectly and that is reasonably attributable to the contravention 3 times that total value;~~ ~~(c) if that court cannot determine that total value 10% of the adjusted turnover of the body corporate during the breach turnover period for the contravention.~~	Update the maximum penalty sections to reflect that liability occurs only with SPF Code provisions. This simplifies the proposed two tier system which has different maximum penalties for contraventions against Division 2 and Division 3 obligations. SPF Code maximum penalty has been moved into 59FK.

	~~*Maximum amount of civil penalty for other persons*~~ ~~(3) For the purposes of subsection (1), the maximum penalty amount for such a contravention by a person other than a body corporate is 1,600 penalty units.~~	
58FN	**58FN Purpose and effect of this Subdivision** (1) The purpose of this Subdivision is to provide for the issue of an infringement notice to a person for an alleged contravention of: ~~(a) a civil penalty provision of an SPF principle in Subdivision B or E of Division 2 of this Part; or~~ (b) a civil penalty provision of an SPF code; as an alternative to proceedings for an SPF civil penalty order.	Proposed change reflects that there are no civil penalty provisions in Division 2.
58FO	**58FO Issuing an SPF infringement notice** ~~*Notices for contraventions of certain SPF principles*~~ ~~(1) If an inspector of the SPF general regulator reasonably believes that a person has contravened a civil penalty provision of an SPF principle in Subdivision B or E of Division 2 of this Part, the inspector may issue a notice (an SPF infringement notice) to the person.~~	Proposed change reflects that there are no civil penalty provisions in Division 2.

58FV	**58FV Enforceable undertakings** ~~*Accepting an undertaking*~~ ~~(1) The SPF general regulator may accept a written undertaking given by a person for the purposes of this section in connection with compliance with a provision of the SPF principles.~~	Proposed change reflects that there are no civil penalty provisions in Division 2.
58FW	**58FW Granting injunctions** (1) The Court may, on application, grant an injunction in such terms as the Court considers appropriate if the Court is satisfied that a person has engaged, or is proposing to engage, in conduct that constitutes or would constitute: (a) a contravention of a civil penalty provision of an SPF code: (~~i) a civil penalty provision of an SPF principle; or~~ ~~(ii) a civil penalty provision of an SPF code; or~~ (b) attempting to contravene such a provision; or (c) aiding, abetting, counselling or procuring a person to contravene such a provision; or (d) inducing, or attempting to induce, whether by threats, promises or otherwise, a person to contravene such a provision; or (e) being in any way, directly or indirectly, knowingly concerned in, or party to, the contravention by a person of such a provision; or (f) conspiring with others to contravene such a provision	Proposed change reflects that there are no civil penalty provisions in Division 2.

58FZC	~~**58FZC Actions for damages—general rule**~~ ~~(1) A person (the victim) who suffers loss or damage by conduct of another person that was done in contravention of:~~ ~~(a) a civil penalty provision of an SPF principle; or~~ ~~(b) a civil penalty provision of an SPF code;~~ ~~may recover the amount of the loss or damage by action against that other person.~~ ~~(2) An SPF regulator may make a claim under subsection (1) on behalf of the victim if the SPF regulator has the victim's written consent to do so.~~ ~~(3) A claim under subsection (1) may be made at any time within 6 years after the day the cause of action that relates to the conduct accrued.~~ ~~(4) However, this section applies subject to sections 58FZD to 58FZK (about proportionate liability for concurrent wrongdoers).~~ ~~Note: See subsection 58FZF(1) in particular.~~	Optus proposes removing the general rules for civil actions for damages. This power sites in addition to the range of all other enforcement activities, including IDR, EDR, and regulator and court action. Optus' priority is to ensure that customers who suffer damages and loss due to non-compliance with SPF Codes receive simple, effective and timely compensation and resolution. It is not clear how the addition of a general action for damages – in addition of all the other potential avenues for redress – adds to this principle. Consumers should not have to take court action themselves to receive compensation. The dispute resolution processes, with the back up of regulator action (which prioritises compensation for loss), should be sufficient to ensure all losses are recovered. Optus submits that if these processes are not sufficient, legislative provisions should be presented that address the shortcomings of dispute resolution and regulator action.
58FZD	~~**58FZD Meaning of *concurrent wrongdoers***~~ ~~(1) In this Subdivision, a concurrent wrongdoer, in relation to a claim under subsection 58FZC(1), is a person who is one of 2 or more persons:~~	See above, Optus proposes this sub-division be removed.

	~~(a) who each contravened a civil penalty provision of an SPF principle or a civil penalty provision of an SPF code (whether or not the same civil penalty provision); and~~ ~~(b) whose contraventions caused, independently of each other or jointly, the loss or damage that is the subject of the claim.~~ ~~(2) For the purposes of this Subdivision, a person can be a concurrent wrongdoer if the person is insolvent, is being wound up or has ceased to exist or died.~~	
58FZE	**~~58FZE Certain concurrent wrongdoers not to have benefit of apportionment~~** ~~(1) Nothing in this Subdivision operates to exclude the liability of a concurrent wrongdoer (an excluded concurrent wrongdoer) in proceedings involving a claim under subsection 58FZC(1) to recover an amount of loss or damage if:~~ ~~(a)the concurrent wrongdoer intended to cause the loss or damage; or~~ ~~(b)the concurrent wrongdoer fraudulently caused the loss or damage.~~ ~~(2) The liability of an excluded concurrent wrongdoer is to be determined in accordance with the legal rules (if any) that (apart from sections 58FZD to 58FZK) are relevant.~~ ~~(3) The liability of any other concurrent wrongdoer who is not an excluded concurrent wrongdoer is to be determined in accordance with the other provisions of this Subdivision.~~	See above, Optus proposes this sub-division be removed.
58FZF	**~~58FZF Proportionate liability for claims involving concurrent wrongdoers~~** ~~(1) In any proceedings involving a claim under subsection 58FZC(1) to recover an amount of loss or damage:~~	See above, Optus proposes this sub-division be removed.

	~~(a)the liability of a defendant who is a concurrent wrongdoer in relation to the claim is limited to an amount reflecting that proportion of the loss or damage that the court considers just having regard to the extent of the defendant's responsibility for the loss or damage; and~~ ~~(b)the court may give judgment against the defendant for not more than that amount.~~ ~~(2) If the proceedings also involve another claim that is not a claim under subsection 58FZC(1), liability for the other claim is to be determined in accordance with the legal rules, if any, that (apart from this Subdivision) are relevant.~~ ~~(3) In apportioning responsibility between defendants in the proceedings:~~ ~~(a)the court is to exclude that proportion of the loss or damage in relation to which the victim is contributorily negligent under any relevant law; and~~ ~~(b)the court may have regard to the comparative responsibility of any concurrent wrongdoer who is not a party to the proceedings.~~ ~~(4) This section applies in proceedings whether or not all concurrent wrongdoers are parties to the proceedings.~~ ~~(5) A reference in this Subdivision to a defendant in proceedings includes any person joined as a defendant or other party in the proceedings (except as a plaintiff) whether joined under this Subdivision, under rules of court or otherwise.~~	
58FZG	**~~58FZG Defendant to notify plaintiff of concurrent wrongdoer of whom defendant aware~~** ~~(1) If:~~ ~~(a)a defendant in proceedings involving a claim under subsection 58FZC(1) has reasonable grounds to believe that a particular person (the other person) may be a concurrent wrongdoer in relation to the claim; and~~	See above, Optus proposes this sub-division be removed.

	~~(b)the defendant fails to give the plaintiff, as soon as practicable, written notice of the information that the defendant has about:~~ ~~(i)the identity of the other person; and~~ ~~(ii)the circumstances that may make the other person a concurrent wrongdoer in relation to the claim; and~~ ~~(c)the plaintiff unnecessarily incurs costs in the proceedings because the plaintiff was not aware that the other person may be a concurrent wrongdoer in relation to the claim;~~ ~~the court hearing the proceedings may order that the defendant pay all or any of those costs of the plaintiff.~~ ~~Note:The plaintiff is the victim or an SPF regulator (see subsections 58FZC(1) and (2)).~~ ~~(2) The court may order that the costs to be paid by the defendant be assessed on an indemnity basis or otherwise.~~	
58FZH	**~~58FZH Contribution not recoverable from defendant~~** ~~A defendant against whom judgment is given under this Subdivision as a concurrent wrongdoer in relation to a claim under subsection 58FZC(1):~~ ~~(a) cannot be required to contribute to any damages or contribution recovered from another concurrent wrongdoer in respect of the claim (whether or not the damages or contribution are recovered in the same proceedings in which judgment is given against the defendant); and~~ ~~(b) cannot be required to indemnify any such wrongdoer.~~	See above, Optus proposes this sub-division be removed.

58FZI	~~**58FZI Subsequent actions**~~ ~~(1) For a claim under subsection 58FZC(1), nothing in this Subdivision or any other law prevents a plaintiff (or a victim) who has previously recovered judgment against a concurrent wrongdoer for an apportionable part of any loss or damage from bringing another action against any other concurrent wrongdoer for that loss or damage.~~ ~~(2) However, in any proceedings in respect of any such action, an amount of damages cannot be recovered by or for the victim that, having regard to any damages previously recovered by or for the victim in respect of the loss or damage, would result in the victim receiving compensation for loss or damage that is greater than the loss or damage actually sustained by the victim.~~	See above, Optus proposes this sub-division be removed.
58FZI	~~**58FZJ Joining non-party concurrent wrongdoer in the action**~~ ~~(1) The court may give leave for any one or more persons to be joined as defendants in proceedings involving a claim under subsection 58FZC(1).~~ ~~(2) The court is not to give leave for the joinder of any person who was a party to any previously concluded proceedings in respect of the claim.~~	See above, Optus proposes this sub-division be removed.
58FZK	~~**58FZK Application of this Subdivision**~~ ~~Nothing in this Subdivision:~~ ~~(a) prevents a person being held vicariously liable for a proportion of a claim under subsection 58FZC(1) for which another person is liable; or~~ ~~(b) prevents a person from being held severally liable with another person for that proportion of a claim under subsection 58FZC(1) for which the other person is liable; or~~	See above, Optus proposes this sub-division be removed.

	~~(c) affects the operation of any other provision of this Act or of any other Act to the extent that the provision imposes several liability on any person in respect of what would otherwise be a claim under subsection 58FZC(1).~~	
Part 2 — Other amendments		
	Telecommunications (Interception And Access) Act 1979 **At the end of subsection 7(2)(bc)** Insert: (bd) an act or thing done in compliance with Part IVF of the *Competition and Consumer Act 2010*	Optus notes that minor changes may be required to the TIA Act to make clear that actions required under the Part IVF do not breach section 7 of the TIA Act. Optus notes that the TIA Act could otherwise prevent telecommunications networks from taking the necessary actions to analyse traffic patterns and/or content to identify scam traffic, as required under the SPF Codes.

Appendix 2: Optus submission to Treasury consultation on Scams Prevention Framework in October 2024

Submission in response to The Treasury consultation

Treasury Laws Amendment Bill 2024: Scams Prevention Framework

Public Version

October 2024

EXECUTIVE SUMMARY

36. Optus welcome the opportunity to provide comments on the Treasury Laws Amendment Bill 2024: Scams Prevention Framework (SPF). Optus also supports the Communications Alliance and Australian Mobile Telecommunications Association submissions on the proposed SPF.

37. The SPF introduces a multi-sectorial framework (initially relating to banks, digital platforms and the telecommunications sector) aimed at ensuring businesses adopt scam prevention actions to address the risk to Australian consumers from fraudulent scam activity.

38. Optus supports these efforts and supports the Government's desire to adopt a coordinated, whole of ecosystem approach to preventing and disrupting scam activity. Scams operate across multiple different sectors and scammers change their approach to exploit different vulnerabilities in different sectors.

39. While it may not be possible to completely eradicate scams, Optus agrees that some sectors require immediate uplift and others need more consistent uplift to reduce the effectiveness of scams and make Australia an unattractive target for scammers.

40. The telecommunications industry has led the way in implementing measures to detect and prevent scam activity, including an enforceable industry code, which has significantly reduced the number of scam calls and SMS reaching Australian consumers. The industry also has in place a range of industry-specific direct regulation that already addresses the majority of the obligations proposed in the SPF.

41. Telecommunications companies have also developed a range of technical solutions that would assist other companies in identifying if their customer was at high risk of fraudulent transactions, particularly where companies rely on SMS as a security protocol, despite never being designed as a security tool. However, take-up of these by other companies has been slow or inconsistent in sectors.

42. Because of this, Optus supports a flexible framework approach, whereby the SPF contains principles to guide the development of subordinate regulation which can be targeted at the specific issues and deficiencies identified in designated sectors. Optus supports this approach as:

    (a) it ensures the subordinate regulation can be targeted at critical deficiencies in a specific sector to deliver immediate real-world benefits in an efficient and streamlined way;

    (b) it avoids increased complexity from duplicated obligations; and

    (c) does not prohibit the development of future innovative responses and solutions to disrupt scam activity and can better respond to changes in a highly technical and dynamic industry such as telecommunications as scammers constantly evolve their approach.

43. A flexible framework would also streamline and minimise complexity in relation to:

    (a) enforcement of sector-specific obligations, where there is a sector-specific regulator in addition to the general SPF regulator; and

(b) dispute resolution, liability and compensation arrangements, particularly where a sector-already has an existing sector-specific external dispute resolution (EDR) scheme.

44. As currently drafted, the proposed framework contains broadly drafted obligations some of which could be impractical to implement; and could have unintended consequences such as inadvertently assisting scammers and negative impacts on consumers, for example, overloading them with scam notifications. Such outcomes would undermine the overarching aims of the SPF.

45. Optus also supports a holistic policy approach to addressing scams in each sector, particularly where there are additional actions that Government or regulators could take that would have immediate, real-world benefits in addressing scams.

46. As such, Optus supports the timely finalisation of a mandatory SMS Sender ID Registry (following the legislation that has been passed by the Government) as this can immediately provide confidence to recipients as to the legitimacy of an SMS. In addition, Optus also considers work needs to be urgently progressed on clarifying the rights of use of numbers.

47. Finalising and implementing both of these projects should be a priority in tackling scams, prior to designating the telecommunications sector under the SPF as these would have a direct impact on disrupting scam activity and complement existing activities of the telecommunications industry.

48. There has been significant work already done by the telecommunications sector to protect telecommunications services, its consumers and more broadly prevent and disrupt scam activity. Where appropriate this is governed by existing regulations. Industry also actively participates in collaborative government-led initiatives, such as the National Anti-Scam Centre (NASC).

49. Optus urges Treasury to implement a flexible framework that:

(a) Contains guiding principles to support targeted obligations in subordinate regulation to address gaps or identified issues, rather than containing broad, general overarching obligations in the primary legislation, given the different roles and existing regulation of key sectors;

(b) Minimises complexity by avoiding duplication of obligations in the primary legislation with existing industry regulations or external dispute resolution schemes;

(c) Does not discourage or slow innovative technical solutions to scam activity, particularly where this may require collaboration across sectors;

(d) Enables obligations in subordinate regulation to commence at the time designating a sector occurs to address concerns about slow or inconsistent action in a sector; and

(e) Complements other policy initiatives or work that may better address issues related to scams, such as, the SMS Sender ID Registry or work on clarifying the rights of use of numbers in the telecommunications sector.

50. Optus also recommends that care is needed in designating any liability to compensate customers for financial or other loss. The use of SMS, for example, as a security tool to authenticate financial transactions should not make telecommunications providers liable

for loss because this service was never designed as a security tool and financial institutions can and should invest in more robust solutions.

51. Optus believes such an approach will still be able to achieve timely success in uplifting standards where needed without adversely impacting sectors that already have significant sector-specific capabilities and regulation in place, to ensure Australia is an unattractive target for scammers.

PROTECTIONS ARE INCONSISTENT ACROSS SECTORS

52. Optus welcomes the Government's recognition that a whole of eco-system approach is needed in relation to scams and that some sectors require immediate uplift and others require a more consistent approach in an effort to tackle scams.

53. In considering how best to legislate a scams prevention framework, it is important to remember that some sectors are considerably more advanced in terms of efforts and regulation at addressing scams. In addition, there are very different scam issues prevalent in each sector, scams evolve and change their approach and interact with sectors in different ways. While there is a common overarching policy intent, the role each sector has to play and how this is achieved in each sector may need to be addressed differently.

Telecommunications has strong regulatory obligations for addressing scams

54. Scams can affect the telecommunications industry in two ways:

    (a) telecommunications services can be used by scammers in an attempt to contact customers as part of a scam; or

    (b) telecommunications services themselves can be a target for scammers because SMS continues to be used by a range of companies (such as banks or other service providers) as a security protocol for accounts (e.g. one time codes) even though SMS was never designed nor intended to be used in this way.

55. As Treasury would be aware, the telecommunications industry has numerous existing regulations that address issues around telecommunications account security, customer identification, and scam protection, including:

    (a) the *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022* (MFA Determination) which requires multi-factor customer authentication for certain high-risk transactions and prevents scammers from taking over telecommunications accounts;

    (b) the *Telecommunications (Industry Standard for Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020* requires industry to conduct stronger identity checks to stop mobile porting fraud; and

    (c) the *Reducing scam calls and scam SMS Code* (Reducing Scams Code) which aims to identify and stop scam calls and SMS based on certain characteristics.

56. These regulations have been particularly successful in increasing telecommunications account security and reducing the number of scall calls and texts reaching consumers.

57. Telecommunication providers, including Optus, have a range of built-in protections on our networks that are automatic, such as SMS and Scam Call Firewalls, and these have blocked huge quantities of scams from reaching our customers.

58. Across the telecommunications industry, 2.1 billion scam calls have been blocked since 2020 and over 668 million scam SMS have been blocked since the Reducing Scams Code was updated to include SMS in 2022.[2] While it may not be possible to completely

[2] https://www.acma.gov.au/publications/2024-08/report/action-scams-spam-and-telemarketing-april-june-2024

stop all scam traffic, through these measures, which have been in place for many years, Australia is a more difficult place to send successful scam communications traffic.

59. Further the industry already has well-established internal dispute resolution regulation and an external dispute resolution scheme in place, with:

    (a) the *Telecommunications (Consumer Complaints Handling) Industry Standard 2018* (Complaints Handling Standard), which sets out obligations for dealing with customer complaints; and

    (b) the Telecommunications Industry Ombudsman scheme, which Carriage Service Providers (CSPs) are required to join.

60. The industry also participates and works collaboratively across Government-led initiatives such as:

    (a) the National Anti-Scam Centre (NASC);

    (b) the Australian Financial Crimes Exchange (AFCX) including the Anti-Scam Intelligence Loop, and

    (c) the Security & Fraud Alliance Forum, an initiative of the telecommunications sector that brings together all major carriers, banks, crypto currency providers, large Australian brands and organisations, State, Territory and Federal police agencies, the Australian Financial Crimes Exchange (AFCX), ID Care and law enforcement agencies, to exchange information in a highly operational context and cooperative environment.

Telecommunications has measures that can assist other industries

61. Scammers continue to change their approach and exploit deficiencies in scam protections across the broader Australian ecosystem. Scammers adopt different communication channels, such as social media, messaging sites/apps and dating sites/apps, as well as false advertisements on social media sites and digital platforms and different approaches, from large scale mass scam texts or calls to targeted relationship building once initial contact is made.

62. Ultimately scammers are after financial reward which can be achieved in different ways, for example, convincing a consumer to willingly transfer money; impersonating a legitimate recipient of a money transfer and providing false details; or by account takeover whereby the scammer has enough security information to take over the consumer's bank account and transfer the money out of the consumer's bank account themselves. The overwhelming purpose of scammers trying to access or takeover telecommunications services is to use those services as a stepping stone to accessing consumers' bank accounts.

63. Optus and the broader telecommunications industry have a range of capabilities that are available to other industries, such as banks, to address impersonation scams and account takeover scams.

64. Protections against sender impersonation scams include:

    (a) **Do Not Originate List**: For specified number ranges, where Optus is the originating network for legitimate calls, Optus blocks the numbers from entering the Optus network. We also ask other participating telcos to not allow their own directly connected customers to originate calls using the specified

numbers, and to block them from being received onto their network from anywhere other than Optus.

For protected originating customers of other networks, Optus only allows calls to enter the Optus network from the network that calls are authorised to originate those calls. It is then up to that originating telco to ensure that no one else on their network can originate calls using those numbers, or to use their network to transit such calls.

For all cases (even where there aren't any DNO arrangements) Optus has our network configured to not allow our directly connected customers to Spoof their CLI (Calling Line Identification).

(b) **SMS Sender ID Protection:** Also known as "Trusted Sources", which has evolved into ACMA's SMS Sender ID Registry trial; this service allows participants to prevent their Alphanumeric Sender IDs ("alpha tags") from being spoofed by unauthorised entities. The participating telcos (Telstra, Optus, TPG Telecom, & Pivotel) set their SMS Firewalls to only allow the specified alpha tags to arrive on their network where they come from the trusted source network. This primarily prevents Scam SMS from arriving in the same message thread as legitimate messages from the bank or other protected organisation. There are protection types available that offer higher levels of protection, such as applying restrictions to any SMS Sender ID that contains the protected word or words in a Sender ID.

This scheme has been available since 2021, and after all this time, take-up is disappointingly low..

(c) **Optus Call Stop & Optus Text Stop**:. Participating financial institutions provide details of Scam SMS that feature a Scam Callback number that impersonates the reporting entity. The Scam SMS will usually contain a claim that a financial transaction took place on the person's bank account, and to immediately call a supplied number. At times, the Scam SMS may appear in the same message thread as legitimate messages of the impersonated entity (which further highlights the importance of SMS Sender ID protection).

There are currently 2 separate instances of Call Stop in operation. The first instance, with the AFCX, focuses on bank impersonation scams, with validated scam data supplied by the banks, and directly led to the creation of the AFCX Anti-Scam Intelligence Loop ("the loop"). The second instance uses validated data supplied by NASC and focusses on investment scams.

Once Optus receives the validated scam data, Optus then diverts any calls made to the Scam Callback number, to a recorded voice announcement (RVA) warning that "The number you have called has been reported as being used for scam activities. For more information, please visit optus.com.au/CallStop." This immediately disrupts the scam for customers on the Optus network.

Optus then submits details of the Scam Callback number to the traceback process in the Reducing Scam Calls and Scam SMs Industry Code, and the offending service will be disconnected. This ensures that customers of other network will also benefit from Optus' actions, although without the education piece of the warning message.

65. Protections against telecommunications account take-overs include:

(a) **SIM Swap Notifications are available to companies who use SMS for security**: While the telecommunications industry has implemented multi-factor authentication capabilities for 'high risk customer transactions' transactions' (including SIM swaps) as required by the MFA Determination to protect telecommunications accounts from fraudulent takeovers it is difficult to prevent all fraudulent SIM swaps, especially where a scammer has sufficient stolen ID. information to be able to impersonate a customer.

The telecommunications industry created a data service through Jersey Telecom's 'JT Monitor SIM Swap Services', which can provide real-time information to banks on SIM swaps that have taken place. The key reason that scammers conduct a fraudulent SIM swap is in order to gain access to a victim's bank accounts by receiving and acting on one-time-codes received by SMS. This service can be used by companies, such as banks to raise red flags on any transactions that are requested subsequent to a SIM swap.

Again, disappointingly this capability has not been taken up . The telecommunications industry has these tools available and we consider this a proactive measure that can provide an additional safeguard to financial institutions that rely on SMS as an authentication tool.

(b) **Number Porting Notifications**: While Pre-Port Verification (PPV) has significantly reduced instances of fraudulent porting, some scammers will find a way, such as through socially engineering their victim. To further protect Australians, the telecommunications industry provides real-time porting information (for all number types) as both a data feed service and a lookup service. This would enable companies, such as banks, to consider any recent porting activity in their risk profile for any financial transactions.

66. While some companies have done good work in implementing measures to disrupt scam activity, we note that ASIC has recently released a report (Report 790) showing the inconsistent take up by the banking industry of these protections.[3]

67. Report 790 examined the scam prevention, detection and response activities of 15 banks outside of the four major banks. ASIC found that there is a lack of protection by banks against brand misuse across all their telecommunication channels. Only one of the reviewed banks had fully implemented controls to minimise misuse of its telephone numbers and SMS alpha tags to prevent impersonation scams.

68. There also appears to be inconsistent use of the DNO List and Sender ID service, with ASIC findings that:

(a) One bank had implemented both DNO List protection and SMS Sender ID protection;

(b) Seven banks had partially implemented the protections;

(c) Seven banks had not implemented either of the protections; and

(d) Seven banks had plans to implement or improve their protection status.

[3] ASIC, Report 790: Anti-scam practices of banks outside the four major banks, 20 August 2024. Available at: https://download.asic.gov.au/media/eiahqnwn/rep790-published-20-august-2024.pdf

69. This reflects Optus' observations and experience that there has been modest take up of these protection services.

70. Regarding protection against impersonation scams, we note again that only 5 banks have implemented SMS Sender ID protections since the scheme has been available since 2021. More broadly there are varying degrees of adoption of this across other key businesses and organisations, such as, essential services providers, large retailers, delivery services and government organisations. Optus considers that SMS Sender ID protections is a measure that all companies should have in place to provide confidence to consumers of the legitimacy of SMS.

71. It is clear there has been an inconsistent approach to uplifting protections in key sectors such as banking and digital platforms. While the telecommunications industry is already regulated to address issues identified in other sectors (such as, account protection or blocking scam contacts) a one size fits all approach across all sectors risks creating an unnecessarily complex regulatory landscape. Optus considers the framework should be flexible enough to support regulation appropriately tailored to the issues and characteristics of each sector.

A MORE FLEXIBLE FRAMEWORK IS NEEDED

72. Key elements of the SPF include:

    (a) 6 principles containing broad overarching obligations that would apply to a sector as soon as that sector is designated;

    (b) An external dispute resolution (EDR);

    (c) civil causes of action; and

    (d) Provision for an SPF regulator and an industry-specific regulator.

73. Optus acknowledges the desire to immediately uplift actions in a relevant sector in a timely fashion (i.e. as soon as that sector is designated), but, has some concerns with the approach in the proposed framework. These concerns include:

    (a) The principles in the overarching framework contain broad obligations that can duplicate already existing industry-specific regulations in some sectors which increases the complexity of implementation and enforcement;

    (b) Some of the obligations are potentially impractical to implement; and

    (c) Some obligations could have unintended negative consequences on industry and consumers.

The framework should avoid duplicating existing obligations

74. As noted, the telecommunications sector already has a range of industry-specific regulations in place designed to prevent and disrupt scam activity and provide protections to consumers. This includes:

    (a) The Reducing Scams Code, which aims to identify and stop calls and SMS that are scam calls / SMS based on certain characteristics;

    (b) The MFA Determination, which requires multi-factor customer authentication for certain high-risk transactions;

    (c) The Telecommunications (Industry Standard for Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020 requires industry to conduct stronger identity checks to stop mobile porting fraud; and

    (d) The *Telecommunications (Consumer Complaints Handling) Industry Standard 2018* (Complaints Handling Standard), which sets out obligations for dealing with customer complaints.

75. The broad obligations in the proposed principles of the framework concern requirements regarding governance, prevention, detection, reporting, disruption and response (including internal dispute resolution) which largely duplicate the existing industry-specific obligations but in a broader way.

76. If the telecommunications sector is designated (as apparently intended by the Government) it would immediately become subject to these broad obligations which will create significant complexity in operation between these regimes particularly where there are multiple regulators.

77. For example, the Reducing Scams Code focuses on operational requirements to identify and block scam SMS and calls and is enforced by the ACMA. However, the proposed principles require companies to take reasonable steps to detect scams related to certain services (s. 58BN), to prevent scams from being committed (s. 58BK) and to disrupt scams and prevent loss or harm.

78. Similarly, proposed s. 58BZC requires an entity to have an internal dispute resolution mechanism for consumers to complain about scams. Yet, the telecommunications industry is already subject to the Complaints Handling Standard, enforced by the ACMA, which is prescriptive in its requirements regarding handling of customer complaints.

79. The broad drafting of these proposed framework obligations creates considerable regulatory uncertainty, particularly where there are multiple regulators enforcing the industry-specific regulations and the SPF.

80. It could conceivably lead to a scenario where a scam occurs and despite a telecommunications company being compliant with the requirements of the industry code or industry-specific regulation, another regulator may take the view that the company did not take reasonable steps as required by the overarching obligations in the SPF.

81. This leads to regulatory uncertainty and implementation complexity given the highly technical nature of providing telecommunications services and implementing scam detection, prevention and disruption measures.

82. In addition, liability and compensation arrangements need to be carefully considered. The SPF proposes that there be an external dispute resolution (EDR) scheme as well as civil rights of action.

83. Optus does not consider that telecommunications companies should be broadly liable or share the liability for financial or other loss, particularly where a telecommunications company has complied with its industry-specific obligations.

84. The use of SMS, for example, as a security tool to authenticate financial transactions, should not make telecommunications providers liable for loss because this service was never designed as a security tool and financial institutions can and should invest in more robust solutions.

85. Optus considers that liability should be limited to circumstances where a telecommunications company has failed to comply with its industry-specific obligations and the customer has suffered loss with that telecommunications company (for example, if a scammer has gained control of the customer's telecommunications account and obtained devices).

86. In addition, the SPF contemplates an additional external dispute resolution scheme. However, the telecommunications industry already has an external dispute resolution scheme, the Telecommunications Industry Ombudsman. Optus believers the SPF framework should be flexible such that if a sector already has an established EDR scheme (like telecommunications does with the TIO scheme) it should not also be subject to an additional EDR scheme.

87. Multiple EDR schemes applying to a sector, particularly where there are duplicative obligations, would also be complex, create confusion and raise industry costs. One EDR scheme for the telecommunications sector would ensure there is less confusion for telecommunications companies and consumers.

88. Optus considers that there should also be a safe harbour provision that where a telecommunications company complies with an industry code or industry-specific regulation the company will not be subject to enforcement action under the SPF Framework, via civil action nor via an EDR scheme.

Some obligations may be impractical to implement or have unintended consequences

89. There are further concerns about the practical implementation of some of the principles.

90. Proposed Principle 2 related to the prevention of scams requires a regulated entity to take reasonable steps to identify the classes of consumers of that entity's service who have a higher risk of being targeted by a scam relating to the service and provide warnings about such a scam to each consumer (s. 58BK(2)).

91. Given that companies regularly use SMS as a security protocol (as previously noted despite SMS not being designed nor intended to be used in this way) all users of telecommunications services are at risk of being targeted by scammers for account takeover to be used to gain access to other accounts (such as bank accounts) or in perpetrating other criminal activity.

92. Further, given the proposed broad definitions of 'scam' and 'actionable scam intelligence' it is conceivable that *every* SMS or call blocked in accordance with the Reducing Scams Code would be considered actionable scam intelligence.

93. This means telecommunications companies would need to send an alert/notification to users every time a scam call or SMS was blocked. In the April – June 2024 quarter telecommunications companies blocked in excess of **291.4+ million** scam SMS and calls (this would be on average more than 3.1 million contacts blocked **each day**).[4]

94. This is likely to lead to notification fatigue for consumers from the telecommunications industry alone, let alone in conjunction with notifications from any other sector.

95. We agree that consumer awareness and education is an important element of combatting scams and reducing their success, but the proposed notification obligations in the framework which would apply as soon as a sector is designated may not be the best approach.

96. In addition, proposed s. 58BF requires an entity publish information about the measures the entity has in place to protect its consumers. Such a requirement should be considered against the harm that could be caused if scammers have easy access to a company's changing protective measures, particularly where new innovative solutions are implemented. In that case, it is not clear any benefit would be outweighed by the potential harm.

97. Again, Optus considers a better approach would be for the framework to include the principles as guidance for any subordinate regulation with the capacity for some or all of that subordinate regulation to come into effect for a relevant sector as soon as that sector is designated, as achieving the same timely outcome in a more appropriately targeted way.

There are advantages to a more flexible framework

98. Keeping in mind the desire for there to be a whole of eco-system approach to tackling scams and the need for there to be a timely uplift in some sectors, Optus believes this

[4] https://www.acma.gov.au/publications/2024-08/report/action-scams-spam-and-telemarketing-april-june-2024

can be achieved while avoiding the issues that result from having broad, duplicative obligations in the primary legislation.

99. This could be achieved by making minor adjustments to the construction of the framework so that it is more flexible in its operation.

100. Specifically, the concerns noted above could be addressed by removing the obligations set out in proposed Principles 1-6 and instead have these as matters that must be addressed by subordinate regulation (e.g. a Ministerial Instrument, SPF Rules and/or Industry Code).

101. This would allow the subordinate regulation to address these overarching principles in a way that is targeted towards the key concerns in each sector, which ensures regulation is appropriately targeted and consistent with good regulatory practice. This would remove the complexity associated with having broad obligations duplicating existing Code requirements and allow Code obligations to be crafted appropriately in relation to other industry-specific regulations already in place and technical and/or operational considerations of that industry.

102. The framework could also provide the flexibility for subordinate regulation to implement obligations in a sector immediately upon designation (i.e. designation and obligations in subordinate regulation could be considered and come into effect concurrently). This would still support the timely uplifting of a sector's activity in relation to scams.

103. Ensuring the obligations are in subordinate regulation such as an industry code could also assist where there would otherwise be one regulator enforcing the obligations in the framework and an industry-specific regulator enforcing obligations in an industry code.

104. Further, given the highly technical and dynamic nature of the telecommunications industry, Optus believes an industry code is more advantageous than having obligations in primary legislation as an industry code can be more easily adapted over time in response to technical changes in the industry and the evolving nature of scam methods.

105. More broadly, such flexibility would allow the Government and regulators to pursue multiple solutions where the SPF complements other policy initiatives that are also likely to have a real impact on preventing scams. The evolving nature of scams means solutions will always need to adapt and a particular scam-related issue may need to be tackled by multiple industries and/or in multiple ways.

106. In particular, Optus encourages the timely implementation of a mandatory SMS Sender ID Registry, following the passage of the relevant legislation, as well as the clarification over the right of use of numbers.

107. While large numbers of scam messages are blocked by telecommunications companies, scammers are still able to evade these efforts. Therefore, multiple solutions are needed to prevent scam activity.

108. A mandatory SMS Sender ID Registry applying broadly across the Australian ecosystem would increase confidence amongst consumers as to the legitimacy of SMS and reduce the likelihood of consumers being duped by fraudulent messages, consistent with the policy objective of the SPF.

109. The SMS Sender ID Registry is already in train and implementing it is likely to have an immediate impact in delivering real world benefits to consumers in protecting them from scam activity.

110. In addition, Optus requests that urgent work be done by the ACMA to clarify the rights of use of numbers. Such work would assist in circumstances where numbers are spoofed to appear as though a scammer is calling from a trusted institution. Optus recommends that addressing issues related to the rights of use of numbers would assist in preventing such scam calls and further protect Australians from scams and again, is something that could be undertaken to deliver additional timely protections to Australian consumers.

Consumer education will continue to be important

111. Along with regulatory and policy measures, Optus also encourages continued education efforts by Governments and regulators on consumer awareness of scams. Investment scams continue to be the overwhelming source of loss for Australians[5] and where scammers use more sophisticated approaches and tactics, education, awareness and financial literacy will continue to play an important role in minimising scam success.

[5] https://www.scamwatch.gov.au/research-and-resources/scam-statistics