



Scams Prevention Framework – Exposure draft legislation consultation

PUBLIC SUBMISSION

4 October 2024



Contents

- 1. Summary 3
- 2. Background..... 3
- 3. Avoiding unintended consequences by providing greater certainty 4
 - The problem: Difficulty of accurately identifying scam communication..... 4
 - Potential unintended response: Highly risk-averse behaviour by telcos which disrupts legitimate communication 5
 - Potential unintended response: Regulation which crowds out cross sector collaboration and innovative solutions..... 6
 - Suggested solutions..... 6
 - Define reasonable steps by reference to systems and processes..... 7
 - Safe harbours 7
 - Remove or reduce open-ended private class action risk 8
 - Codification of SPF principles in SPF codes 8
 - Worked examples 9
 - EDR scheme operation 9
 - Create greater certainty over extra-territorial application.....10
- 4. Avoiding regulatory burden through codification of unnecessary and onerous processes10
- 5. Review of telco sector scam code under SPF 11
- Annexure A..... 11



1. Summary

Telstra supports the objectives of the proposed Scams Prevention Framework (**SPF**), which is consistent with our existing efforts to fight scams. We welcome a more coordinated approach to combatting scams and recognise the benefit in greater cross-sector coordination that includes banks and digital platforms. In this submission we provide some input to assist with development of the SPF to:

- provide greater certainty for businesses trying to do the right thing and thereby limit unintended consequences and make it a workable framework; and
- avoid codifying unnecessary processes which would add regulatory burden without improving scam prevention outcomes.

In this submission we also highlight some of the difficulties in distinguishing between scams and legitimate communications in the telco context, which we believe should be considered in the development of the SPF. We have set out specific proposed amendments to the SPF at Annexure A and would welcome the opportunity for ongoing discussions on this policy.

2. Background

Telstra recognises the severe impact scams can have and are committed to combatting scams. We have already invested substantial amounts of money, time and expertise in setting up extensive scam detection and prevention systems and processes, while recognising that due to the ever-evolving nature of scam activity there is always more to be done.

There is no silver bullet to stop scams. Scammers are agile and able to pivot their tactics and techniques more rapidly than the industry can often respond. We go to great efforts, across multiple mediums, including voice, SMS/MMS, email and domains, to try to prevent scams from reaching our customers. Along with investing in awareness campaigns for our customers and the public. However, we simply cannot prevent every scam from reaching end users – we face highly sophisticated and well-resourced bad actors actively trying to get around our defences and deceive consumers into falling victim.

Effective economy-wide scam protection efforts do not end with the industries initially to be designated under the SPF. Ultimately, it will have to be an end-to-end (or whole of ecosystem) undertaking.

- End users need to be made aware of, and encouraged to enable, the security capabilities of their devices.
- Businesses will need to design products and services which are more scam resistant and consider taking advantage of service offerings from the market which help them combat scams.
- Current practices adopted by businesses/government service providers which makes their customers more susceptible to scams (such as the use of unsecure communications channels for one-time passcodes, poor data hygiene, URL-shortening, use of multiple numbers) also need to be addressed.

A punitive and prescriptive regime is not required to get us to take scams seriously and could in fact:

- have unintended consequences by driving risk-averse behaviours that would impede legitimate communications between end-users and business activity, with consequent negative social and economic impacts for all Australians;
- crowd out incentives for cross sector collaboration to combat scams; and
- create a large compliance burden without delivering any meaningful benefit.



To avoid such outcomes, we have suggested some amendments to clarify the intended operation of the proposed SPF and avoid unnecessary codification of record keeping and reporting processes.

3. Avoiding unintended consequences by providing greater certainty

The problem: Difficulty of accurately identifying scam communication

It is often incredibly difficult to accurately distinguish between scams and legitimate communications. Fundamentally, this is because scammers are highly motivated to make their communications appear legitimate – most scam messages are almost identical to legitimate communications, differing in only a small detail such as a single digit in a hyperlink or phone number.

Scammers seek to emulate real-life communications and scenarios, often involving a degree of urgency or immediacy (such as children requesting assistance from their parents), or routine types of communications from trusted and authoritative organisations such as banks, governments and service providers. Further, scammers may use personal information obtained via data breaches to give their communications the veneer of legitimacy. Or as another variant will use legitimate communications as the template, making only imperceptible changes to an SMS message for example.

More broadly, scammers operate in a dynamic way, modifying the content of their communications and tactics to evade controls, as shown by the ever-evolving scam landscape and new types of scams.

Often these tactics make it incredibly difficult to detect and validate whether a call or SMS is a scam until there is a critical mass of actionable intelligence about these tactics which can be validated, and the scam blocked. Due to this retrospective awareness, it is inevitable that some scam communications will be delivered to customers before preventative action is taken.

It will always be important for consumers to remain highly alert to the risks of scams which underlines the critical importance of the SPF being one part of a broader suite of measures to combat scams. This includes consumer awareness and education initiatives.

Another challenge for telcos is that scammers will use legitimate but more difficult to trace communications methods, including over-the-top (**OTT**) services which use the public internet. Telcos have limited visibility and control over such communications across our network, as these are owned and operated by third parties and often have end-to-end encryption preventing the content of the communication from being read.

Characteristics used to identify scam calls / messages (e.g. volume, length, message characteristics, CLI issues, time of day, originating from particular domains, hidden phone numbers and shortened URLs) cannot be relied upon as definitive evidence but are just some of the elements highly experienced individuals involved in combatting scams consider when determining if traffic is scam. As scammers change their tactics in real time to evade detection, this requires a dynamic and nuanced approach to taking action, and with decisions often made in ‘real time’. Acting “faster” or “harder” is not the solution and will lead to legitimate communications being blocked.

A feature of the telco sector is there can be multiple carriers or carriage service providers (**CSPs**) involved in delivering a call, SMS or email to an end-user. Along with the originating and terminating carriers, there may be one or more transit providers through which the traffic passes. With voice and messaging over IP technology, traffic may bypass the Telco’s network altogether. Each provider in the chain receives the information regarding the communication by the preceding provider. Only the originating provider has the ability to verify a customer’s rights of use to a number.



Further exacerbating the issue is that legitimate businesses often have poor data hygiene, including outdated or incorrect contact details or lists, or use primarily lower-cost communications solutions. This can lead to a range of false indications of scam communications, including:

- If an organisation uses outdated or incorrect contact details to send a communication, the recipient is more likely to conclude that it was a scam message. For example, if a health sector employer sends messages seeking shift workers to someone who is no longer (or never was) a worker in that sector then that message is very likely to be considered a scam message. This issue has the potential to resulting in a large number of incorrect scam reports / flags in response to a particular campaign.
- Primarily lower-cost delivery paths can lead to a variety of outcomes that make messages from an organisation have technical characteristics that could lead to incorrect flagging as scams. This includes multiple numbers for the same organisation (making 'whitelisting' more difficult and creating unexpected patterns of activity) and use of unencrypted or lower security communications methods.

Additionally, some communications that consumers report as 'scam' are legitimate communications, albeit they may be things like unwanted marketing messages. The overwhelming majority of reported 'scam' by our customers falls into the latter category, demonstrating that careful assessment often needs to be made on whether something should be blocked or not.

Potential unintended response: Highly risk-averse behaviour by telcos which disrupts legitimate communication

The above section outlines the various reasons why it is difficult to tell scams and legitimate communications apart. On this basis, we are concerned that the SPF does not allow organisations to have certainty over their legal liability via sufficient comfort that they have taken 'reasonable steps' to meet their obligations under the SPF. In turn, this could have the effect of incentivising a highly risk-averse response which could impact on the legitimate use of communication services in Australia.

As a telco, our core business and regulatory obligation is to transmit communications. The services provided by telecommunications companies, whether calls, SMS or data services, underpin social engagement and economic activity across the country.

A regime which places too much responsibility on telcos for scams transmitted on their networks will incentivise telcos to treat a greater range of legitimate traffic as suspicious. This may result in increased blocking across the sector to further reduce the risk of scams reaching end customers. This will inevitably increase the likelihood of false positives, creating potential for delays or even blocks of legitimate communications, leading to poor customer experience and broader social and economic impacts from a less reliable telco service.

Specific examples of legitimate use cases which have characteristics that may result in them being falsely identified (by telcos and / or recipients) as scam communications include:

- myGov notifications;
- Emergency and Police notification alerts;
- schools sending SMS to confirm child absences
- multi-factor authentication one-time passwords;
- casual labour hire requests for coverage or shift notifications (for example in the health, construction and education industries);
- appointment or booking reminders;
- electronic prescriptions;



- medical test results;
- political communications including during election campaigns;
- parcel delivery notifications;
- credit management and debt collection;
- donation requests from charities; and
- marketing communications, particularly around specific days (e.g. Mother's or Father's Day / Black Friday) which may result in large spikes in traffic.

It is the daily experience of telcos that these types of communications are flagged by users or technology systems and automated technology as potentially scam or illegitimate communications. Telcos are already dealing with complaints and even legal action from organisations who have been negatively affected by their messages or calls being incorrectly identified as scam communications.

As such, telcos taking a substantially more risk-averse approach to blocking potential scam communications would be likely to result in disruptions to legitimate traffic, impeding a range of important social, health and economic activities.

Potential unintended response: Regulation which crowds out cross sector collaboration and innovative solutions

A regime which does not allow organisations to have certainty over their legal obligations and liability (including what might constitute 'reasonable steps') may also have other flow on unintended consequence. That is, there is a risk it could create a dynamic where different sectors are pitted against each other rather than collaborating to develop more effective economy-wide protections.

Global scamming syndicates are highly sophisticated and innovative, investing significant amounts in product development. To stay ahead of scammers there should be incentives to invest in innovation of capability over and above what is required by regulation in terms of information sharing across industries. If there is no incentive to innovate on a commercially sustainable basis, there is a risk the Australian ecosystem as a whole will not develop the most sophisticated technology solutions. This is a particular risk where the regime provides inadequate guidance for what a designated entity can do in terms of reasonable steps to meet their obligations (complicated by the multiple liability pathways they face).

The NASC has been established as a forum for industry and government to work together to protect the nation and make it a harder target for scammers. It would be unfortunate if a new regulatory regime worked against this aspect of the Government's long-term approach to combatting scams.

Suggested solutions

To mitigate the potential for disruption, businesses require greater certainty as to when they will and will not be held liable. Given the Government's intention to introduce a two-tiered model involving principles in primary legislation and sector specific SPF codes, we submit this can be achieved through:

- a more focused definition of reasonable steps based on systems and processes;
- providing additional safe harbours;
- removing or limiting the proposed private right of action;
- allowing the SPF codes to codify the SPF principles for each sector;
- providing additional worked examples; and
- providing greater clarity regarding the operation of the external dispute resolution (EDR) scheme.

Each of these suggested solutions is addressed in turn below.



Define reasonable steps by reference to systems and processes

The difficulty in distinguishing between scams and legitimate communications weighs in favour of defining reasonableness by reference to the adequacy of scam prevention systems and processes that a regulated entity has in place, rather than the circumstances of individual scams.

Considering the reasonableness of actions taken in the context of individual scams would require complex and inherently backward-looking assessments of, among other things:

- whether the particular scam ought to have been detected (and if so, why and when);
- what actions should have been taken by the regulated entity based on the information available to it at the time; and
- the extent to which there was contributory negligence on the part of the customer.

This would give rise to considerable variability depending on the scam and customer in question, resulting in a fragmented array of outcomes, and hence, substantial uncertainty as to when a telco is liable.

By contrast, consideration of systems and processes would allow for a more consistent and forensic examination of concrete steps taken (or not taken) by the regulated entity to combat scams in what is a highly unpredictable and dynamic environment. Such an approach would provide greater comfort to regulated entities that are doing the right thing, incentivising investment in technological tools and process improvements to reduce exposure to liability.

This would also be in line with other comparable regulatory regimes, such as the anti-money laundering and counter-terrorism financing (AML/CTF) regime, which requires “*appropriate risk-based systems and controls*”. We submit that that the AML/CTF regime is a relevant and analogous regulatory scheme, as it also is a regulatory regime which exists in an environment in which there are bad actors actively seeking to undermine efforts to combat them, such that it would be logical to adopt a similar approach.

As another example, Standards under the Online Safety Act regime which detect, delete and/or deter certain types of material – rather than setting the bar at stopping all forms of online harms outright (which is recognised as an impossible standard to meet).

Safe harbours

Although the proposed safe harbour for taking actions to disrupt an activity while investigating whether the activity is a scam is a good starting point, it is not sufficient.

As a threshold point, we are concerned that parties affected by scam activities will seek to allege that good faith conduct taken for the purpose of compliance with the SPF provisions might be alleged to be disproportionate. Given that there are many factors which go into the assessment of whether a particular action is proportionate or not, uncertainty over this possibility could chill providers into taking necessary action to combat scams in good faith due to uncertainty over civil liability.

As such, we urge that s 58BZ(2)(c) be removed. Parties that might be affected by activities to combat scams will still have the protection of:

- Sections 58BZ(2)(a) and (b), which require such actions to be taken in good faith and for the purpose of complying with the SPF provisions; and
- Section 58BZ(e), which requires the relevant actions to be reversed if the activity is identified as not a scam and it is reasonably practicable to reverse the action.



In the telco context, we also propose a safe harbour for terminating traffic from other telcos be included in the relevant SPF code, such that the obligation is on originating telcos (or where the originating telco is based overseas, the first transit telco in Australia) to ensure rights of use and that the communication is not a scam. This is because the terminating telco does not have a relationship with the originating party, whereas the originating telco does and hence has the greatest visibility of upstream rights of use, being best placed to prevent scam conduct.

Additionally, we propose a safe harbour for where action is not taken to block or disrupt a suspected scam call, SMS or email where a request by law enforcement agencies to pause our activities.

Remove or reduce open-ended private class action risk

The proposed right for private parties to commence actions for damages under section 58FZ has the potential to create a significant and open-ended risk of private class action following a novel scam campaign which is successful despite good faith scam prevention efforts. With the increasing prevalence of litigation funding for class actions in Australia, the significant cost of defending such actions and the potential for very high damages that could be awarded following a novel and successful scam campaign, the risk of private class actions is particularly likely to drive highly risk averse behaviour.

It is important to emphasise that the nature of risk in a private class action context is fundamentally different from the nature of legal risk that businesses will face from regulators tasked with enforcing the SPF. The regulators that will be responsible for administering the SPF are public agencies which seek to take appropriate action in the public interest, and which apply well-established principles of regulatory enforcement. They are robust regulators, which will be expected to enforce the law strongly by all parties involved, but they are public institutions acting in the public interest. The prospect of such regulatory enforcement action is already sufficient to incentivise compliance.

By contrast, class actions are fundamentally driven by profit motives. As such, a private class action litigant is much more likely to commence action, without proof of serious wrongdoing that is against the public interest, in the hope of obtaining information through discovery that could be used to pressure the target into a settlement due to the financial costs and adverse reputational consequences of defending a lawsuit. The key SPF principles are based on standards of reasonableness which do not provide an unambiguous basis to defend good faith conduct which will provide opportunities for class action litigants to continue litigation and seek settlement.

Once again, we draw a parallel to the AML/CTF regime, which does not include a private right of action for damages for breach.

To avoid driving overly risk-averse behaviour seeking to limit exposure to this risk, we strongly urge the Government to remove the private right of action from the SPF. At the very least, this right should be limited to scenarios where the plaintiff can demonstrate some degree of negligence on the part of the regulated entity.

Codification of SPF principles in SPF codes

While there are overlapping obligations as between the SPF principles and SPF codes, compliance with the SPF codes does not necessarily entail compliance with the SPF principles, such that the obligations to which regulated entities are subject will be spread across multiple locations. So as to provide a single source of truth, we suggest that the legislation be amended to clarify that compliance with the SPF codes also amounts to compliance with the relevant aspects of the corresponding SPF principles. Alignment of liability under the various instruments would remove residual risk of exposure to regulatory enforcement or private class action risk where there has been compliance with the relevant SPF code,



providing greater certainty as to the scope of regulated entities' obligations. This would also be consistent with the proposed ss 58B(2), 58BP and 58BY.

Worked examples

Additional worked examples in the SPF principles, codes and explanatory materials are required to provide concrete guidance as to what amounts to reasonable steps or what actions taken to disrupt suspected scam activity would be proportionate for the purposes of ss 58BW and 58BZ in specific factual contexts, including scenarios involving:

- multiple telcos (including originating, transit and terminating telcos); and
- telcos, banks and digital platforms.
- Mass market known scam campaigns versus more targeted scams at lower volumes.

EDR scheme operation

We understand that the Australian Financial Complaints Authority (**AFCA**) is intended to be the single external dispute resolution EDR scheme for the three initial sectors proposed to be designated under the SPF. Given the complexity of the telco sector and the accrued technical knowledge residing in the TIO, we believe the TIO would be a better choice to oversee the EDR scheme for the telco sector.

Under s 1055 of the *Corporations Act 2001* (Cth), AFCA determinations are largely based on the ambiguous and subjective standard of whether it is satisfied that decisions or conduct are fair and reasonable in all the circumstances.

For reasons similar to those articulated in the section regarding reasonable steps above, we submit that this is inapt in the context of the SPF, such that AFCA's assessment should instead be directed to whether the regulated entity had "*appropriate risk-based systems and controls*" in place.

Further, we note that the SPF is silent as to apportionment of liability for compensation between regulated entities where more than one regulated entity has breached an SPF principle or SPF code.

In a similar vein to the section regarding worked examples above, we urge the Government to prepare and publish a set of principles to guide AFCA decision-making regarding apportionment of liability in scenarios involving:

- multiple telcos (including originating, transit and terminating telcos); and
- telcos, banks and digital platforms.

Specifically, we support there being a mechanism for clearly and unambiguously allocating responsibility among different parties, without a need for complicated factual findings of contributory negligence (which are likely to be highly complex and time-consuming).

We submit that a cascading compensation model akin to that under the Monetary Authority of Singapore's proposed Shared Responsibility Framework (as referred to in Attachment A to the Consultation Paper) is appropriate. A description of that model (which only accounts for banks and telcos, not digital platforms) is extracted below:

Assessment of liability involves a 'waterfall' approach, which assesses the bank as the first line of responsibility as the custodian of consumer monies. If the responsible financial institution has breached any of its duties under the framework it is expected to fully compensate the consumer for the loss. If it is found to have met its obligations, telecommunications organisations will be assessed to ensure they have upheld their obligations and will be required to compensate the consumer for their loss if they have breached requirements. If both the responsible financial



institution and telecommunications organisation are found to have upheld their obligations, the consumer will bear the loss and may seek recourse via dispute resolution bodies. The responsible bank and telecommunications organisation will be responsible for conducting the investigation in the first instance.

Such a model would have the benefit of clarity in both responsibility and order – i.e. it clearly defines the ‘first line of defence’ and any claim for compensation from a telco or digital platform would need to wait until after the question of whether there was a responsible financial institution was determined.

To the extent both telcos and digital platforms are involved, we submit that the liability of digital platforms should be determined first, given that their platforms will have served as the point of contact between the consumer and scammer and communications via such platforms are delivered in an OTT manner.

To the extent that a telco is held to be liable, we submit that it should be the telco that has the greatest ability to control the scam activity (i.e. the originating telco or first transit telco in Australia), rather than just the terminating telco merely by reason of having the customer relationship.

Create greater certainty over extra-territorial application

The draft legislation proposes to insert a new provision relating to extra-territorial application of the SPF provisions (s 58AJ). It is not clear why a new and untested provision relating to extra-territoriality is necessary, given the existing and well understood provision in the CCA relating to extra-territorial application (section 5).

As currently drafted, the new provisions (along with the definition of SPF Consumer) imply that international entities which do not carry on business in Australia, but which might supply services to Australian tourists, from time to time, would need to directly comply with the SPF framework. This would be an unprecedented extension of Australian regulatory obligations into foreign jurisdictions and would create significant uncertainty about compliance.

As an alternative, we suggest that Part IVF be added as one of the sections to which the existing extra-territoriality provisions in section 5 of the CCA apply.

4. Avoiding regulatory burden through codification of unnecessary and onerous processes

There is a risk that the reporting and record-keeping requirements under SPF principles 1, 4 and 5 could prove highly onerous, while being of little probative value.

As a telco, we deal with an immense volume of communications. Hence, reporting and record-keeping obligations would still capture a huge number of communications, putting a strain on both regulated entities and the SPF general regulator.

As already mentioned at section 3 above, it is difficult to distinguish between scams and legitimate communications, such that caution should be exercised in imposing obligations in relation to merely suspected scam activity.

Scams are generally conducted as campaigns, which will exhibit similar (if not identical) contents and from which patterns may be discerned. Further, there is a large amount of duplication – regulated entities and regulators will already be aware of many types of scams that have been repeated over many



years – for example the “Hi Mum” scam or the “Nigerian prince” scam. To best direct efforts, the focus should be on material, new developments.

In addition, scammers constantly change their tactics, such that historical reporting of known incidents is of limited utility. It is only information that allows for responses to new tactics which provides probative value.

Further, activities undertaken to combat scams are highly dynamic, with judgement calls needing to be made in real time, such that they do not lend themselves to reporting and record-keeping.

To that end, we propose specific amendments to streamline the definition of ‘actionable scam intelligence’ and ensure that it filters out noise, focusing on confirmed novel scam activity occurring at meaningful volumes, aggregated at a higher level of generality – this is more likely to be of use to regulators, other regulated entities and consumers.

More broadly, the SPF, including both the SPF principles and codes, should be reviewed on an ongoing basis to ensure they are operating effectively, without imposing an undue compliance burden. We have suggested that this occur at least once every six months.

5. Review of telco sector scam code under SPF

The telco sector has been subject to a regulated code on scams since 2020. This Code sets out processes for identifying, tracing, blocking and otherwise disrupting Scam Calls and Scam SMS.

As part of the introduction of the SPF, we support a review (and/or replacement) of this Code, using the current code as a starting point, to create one under the SPF to be administered by the ACMA. We have been engaging with the ACMA to assist with their understanding of the problems with aspects of the existing scams code and the interaction with the existing Numbering Plan.

Given the existing deficiencies in the current code, it is our view that the Telco sector should not be designated until the new SPF Code has been registered.

Annexure A

Section	Proposed amendments	Rationale
s 58AIA (new)	<p><u>58AIA Meaning of reasonable steps</u></p> <p>(1) <u>An assessment of whether a regulated entity has taken reasonable steps for the purposes of subsections 58BJ(1), 58BK(2), 58BN(1), 58BO(1), 58BW(1) and 58BX(1) involves an assessment of the adequacy of the processes, systems and practices that the regulated entity has in respect of the relevant obligation.</u></p> <p>(2) <u>An assessment of whether a regulated entity has taken reasonable steps for the purposes of subsections 58BJ(1), 58BK(2), 58BN(1), 58BO(1), 58BW(1) and 58BX(1) must not take into account the circumstances of the individual scam or SPF consumer, including:</u></p>	



Section	Proposed amendments	Rationale
	<ul style="list-style-type: none"> (a) <u>the nature and sophistication of the scam;</u> (b) <u>the information about the scam available to the regulated entity;</u> (c) <u>when the scam was identified by the regulated entity; or</u> (d) <u>any act (or omission) by the SPF consumer that a reasonable SPF consumer would not have done which contributed to the loss or damage suffered by the SPF consumer as a result of the scam.</u> 	
s 58BL	<p>(1) Taking reasonable steps for the purposes of subsection 58BJ(1) or 58BK(2) requires more than merely acting on actionable scam intelligence in the form of information provided to the regulated entity by another person.</p> <p><i>Further sector-specific details can be set out in SPF codes</i></p> <p>(2) For the purposes of (but without limiting) subsection 58CC(1), the SPF code for a regulated sector may include sector-specific details about:</p> <ul style="list-style-type: none"> (a) what are reasonable steps; or (b) what are relevant resources; or (c) identifying the classes of SPF consumers who have a higher risk of being targeted by a scam; <p>for the purposes of this Subdivision.</p> <p>(3) <u>To the extent a regulated entity has complied with the SPF provisions set out in the SPF code for its regulated sector which specify any of the matters outlined in with subsection (2), the regulated entity is taken to have complied with subsections 58BJ(1), 58BK(1) and 58BK(2).</u></p>	
s 58BP	<p>(1) For the purposes of (but without limiting) subsection 58CC(1), the SPF code for a regulated sector may include sector-specific details about:</p> <ul style="list-style-type: none"> (a) what are reasonable steps; or (b) what is a reasonable time; <p>for the purposes of this Subdivision.</p> <p>(2) <u>To the extent a regulated entity has complied with the SPF provisions set out in the SPF code for its regulated sector which specify any of the</u></p>	



Section	Proposed amendments	Rationale
	<p><u>matters outlined in subsection (1), the regulated entity is taken to have complied with subsections 58BN(1) and 58BO(1).</u></p>	
s 58BR(1)	<p>(1) A regulated entity contravenes this subsection if the entity fails to give the SPF general regulator, in accordance with subsection 58BS(1), a report of actionable scam intelligence the entity has about a <u>class of suspected scams</u> relating to a regulated service of the entity <u>where:</u></p> <p>(a) <u>there is a substantial number of communications, transactions or other activities in that class; and</u></p> <p>(b) <u>the regulated entity has not previously provided a report about that class of communications, transactions or other activities under this subsection.</u></p>	
s 58BW (notes)	<p>Note 1: For example, if a bank has received a substantial number of similar reports of suspected scams, it may be appropriate to pause or delay authorised push payments while the bank investigates the suspected scams.</p> <p>Note 2: <u>If a terminating telecommunications company has received a substantial number of scam text messages through a particular originating or transiting telecommunications company, it may be appropriate to block traffic from that originating or transiting telecommunications company.</u></p> <p><u>Note 3:</u> For further details about the meaning of reasonable steps, see section 58BY.</p>	Worked example in telco context.
s 58BX(2)	<p>(2) A regulated entity contravenes this subsection if the entity:</p> <p>(a) has actionable scam intelligence about a <u>class of suspected scams</u> relating to a regulated service of the entity <u>where:</u></p> <p>(i) <u>there is a substantial number of communications, transactions or other activities in that class; and</u></p> <p>(ii) <u>the regulated entity has not previously provided a report about that class of communications, transactions or other activities under this subsection; and</u></p> <p>(b) fails to give the SPF general regulator a report that:</p>	



Section	Proposed amendments	Rationale
	<p>(i) complies with subsection (3); and</p> <p>(ii) deals with the matters set out in subsection (5).</p>	
s 58BY	<p>(1) For the purposes of (but without limiting) subsection 58CC(1), the SPF code for a regulated sector may include sector-specific details about:</p> <p>(b) what are reasonable steps; or</p> <p>(c) what is a reasonable time;</p> <p>for the purposes of this Subdivision.</p> <p>(2) <u>To the extent a regulated entity has complied with the SPF provisions set out in the SPF code for its regulated sector which specify any of the matters outlined in subsection (1), the regulated entity is taken to have complied with subsections 58BW(1) and 58BX(1).</u></p>	
s 58BZ	<p>(2) The regulated entity is not liable in a civil action or civil proceeding for taking action to disrupt an activity that is the subject of that intelligence if the action:</p> <p>(a) is taken in good faith; and</p> <p>(b) is taken in compliance with the SPF provisions; and</p> <p>(c) is reasonably proportionate to the suspected scam, and to information that would reasonably be expected to be available to the entity about the suspected scam;</p>	Deletion to allow providers to take action to combat scams with a high degree of certainty that they will not face civil liability from affected parties.
s 58BZ (notes)	<p>Note: Assume the regulated entity temporarily blocks restricts access to an SPF consumer’s website internet domain or phone number while investigating whether an activity relating to the website internet domain or phone number is a scam. This subsection protects the regulated entity from civil actions brought by the consumer when the regulated entity is acting appropriately.</p>	Worked example in telco context.
s 58BZE	<p>(1) For the purposes of (but without limiting) subsection 58CC(1), the SPF code for a regulated sector may include sector-specific details about:</p>	



Section	Proposed amendments	Rationale
	<p>(a) conditions that must be met for a reporting mechanism for the purposes of this Subdivision; or</p> <p>(b) conditions that must be met for an internal dispute resolution mechanism for the purposes of this Subdivision; or</p> <p>(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.</p> <p>(2) <u>To the extent a regulated entity has complied with the SPF provisions set out in the SPF code for its regulated sector which specify any of the matters outlined in subsection (1), the regulated entity is taken to have complied with subsections 58BZB(1), 58BZC(1) and 58BZD(2).</u></p>	
s 58CC(2)(b)	<p>(2) Without limiting subparagraph(1)(b)(ii), an SPF code for a regulated sector may include the following:</p> <p>...</p> <p>(b) provisions dealing with the circumstances in which entities are, or may be, relieved from complying with requirements in the SPF code <u>or SPF principles</u> that would otherwise apply to them;</p>	
s 58CCA (new)	<p><u>58CCA Interaction between SPF principles and SPF codes</u></p> <p><u>To the extent a regulated entity has complied with the SPF provisions included in the SPF code for its regulated sector relating to a specific SPF principle, the regulated entity is taken to have complied with the corresponding SPF provisions of that SPF principle.</u></p>	
s 58EB(2)(a)	<p>(2) The functions and powers of the SPF general regulator include:</p> <p>(a) the function of reviewing, and advising the Minister about, the operation of the SPF provisions <u>in force at the time on an ongoing basis, and in any event, no less than once every six months after the commencement date;</u></p>	
s 58FZ	Delete.	



Section	Proposed amendments	Rationale
	<p>[Alternative in the event that this section is not deleted]</p> <p>(1) A person who suffers loss or damage by conduct of another person that was done in contravention of:</p> <p>(a) a civil penalty provision of an SPF principle; or</p> <p>(b) a civil penalty provision of an SPF code;</p> <p>may <u>only</u> recover the amount of the loss or damage by action against that other person or against any person involved in the contravention <u>if that other person or any person involved in the contravention acted (or failed to act) negligently.</u></p> <p>(2) Such an action may be commenced at any time within 6 years after the day the cause of action that relates to the conduct accrued.</p>	