Four improvements needed on the Scams Prevention Framework Bill

DIGI agrees that further action on scams is needed, and digital platforms are ready to support the new scams framework to ensure Australians are better informed and protected online from financial harm. Vague legislation risks industry misinterpreting obligations, leading to overcorrection and negative unintended consequences for consumers and small business.

The *Scams Prevention Framework Bill 2024* (**SPF Bill**) creates a framework for the obligations of specific industries to address scam activity on their platforms. It is supported by sector-specific industry codes, which we support because the technical steps to combat scams via SMS, on social media and for banks are very different. The Bill is constructed around the six SPF Principles (governance, prevent, detect, report, disrupt and respond) and contains an extensive enforcement scheme of civil penalties and remedies for regulated entities who breach both their obligations under the Framework, and their sector-specific codes.

There are four technical problems with the SPF Bill that must be fixed prior to passage through Parliament in order to make sure the Framework approach works in practice.

Problem 1: The SPF Bill imposes dual sets of obligations

The Bill creates overlapping obligations under both the SPF Bill and the sector-specific codes.[1] This model creates a dual and potentially inconsistent set of obligations. All regulated entities must comply with both, and penalties for non-compliance under both sets of obligations apply.

However, the obligations imposed in the primary legislation under the SPF Principles are vague and not clearly defined, as they are based on the premise of a platform taking 'reasonable steps'. This means a platform may be in compliance with all obligations under the sector-specific code, but still be in breach of the obligations under the vaguely defined obligations in the primary legislation.

This overlapping obligation system is extremely uncertain. Regulated entities should have clear obligations imposed upon them to take action against scams, and potentially liable when clear expectations are not met. It is essential that the framework remove all areas of duplicative regulation so that industry has one clear set of obligations to follow when combating scam activities, and consumers can clearly establish whether a company has not complied.

Solution: Establish liability for code compliance in the legislation and place all detailed obligations in the sector-specific codes

DIGI supports amending the Bill so that:

a) The primary obligation to comply with sector specific codes is contained in the SPF Act;
b) Examples of the high level matters that may be dealt with by way of more specific measures in the industry codes are set out in the SPF Act; and
c) Detailed obligations applicable to each sector are fully contained in each sector-specific code.

[1] In Division 2 of the Bill, regulated entities must take "reasonable steps" to follow each of the SPF Principles, as well as meet specific obligations relating to each Principle. These provisions carry civil penalties for non-compliance.Division 3 of the Bill creates a framework for sector-specific codes to be made by legislative instrument by the Minister. Contravention of these codes also carries civil penalties.

This would mean that punitive measures for non-compliance would still apply, but that specific obligations could be more specifically tailored to each sector, as digital platforms, telecommunications companies and banks need to address different technical issues at different points of the scam cycle. This would guide the regulator as to the content of the codes but also remove the uncertainty created by the provisions imposing overly broad obligations by way of entities needing to take "reasonable steps", and ensure consumers, regulators and industry understand the specific action that needs to be taken on scams under the Codes. This model is similar to the approach under section 138 of the *Online Safety Act 2021*.[2]

Problem 2: The SPF Bill creates a complicated and confusing redress model for consumers

The SPF Bill means consumers will need to understand industry internal dispute resolution (IDR) schemes, a Minister-created external dispute resolution (EDR) scheme, as well as the regulator's wide enforcement powers.[3] However, the SPF Bill contains no criteria or basis for how platforms are to resolve complaints under internal dispute resolution, or when remedies imposed by the EDR Scheme would be appropriate. There is also no model for how liability for scam losses is distributed amongst entities within the scam cycle.

Although the EDR can provide consumers with financial and non-financial remedies, the complexity of the SPF Bill scheme is in stark contrast to the UK approach, which allows consumers to claim compensation directly from banks and payment service providers for scam losses. This lack of clarity leaves consumers in the dark when they make a complaint to a platform, about if and how they are entitled to compensation. The proposed approach is likely to frustrate consumer claims and delay recovery of losses. If consumers cannot navigate this complex and vague redress model, the SPF Bill fails to live up to its purpose.

Solution: Provide clarity for consumers
DIGI considers the UK Payment Service Regulator's recently introduced model for compensation a workable approach to addressing scam losses for consumers, as opposed to the SPF Bill's model vague IDR and EDR schemes. As the Payment Services Regulator's policy indicates, financial liability should be limited to the parties with the most insight and involvement in the actual fraudulent financial transactions, i.e. banks and other financial institutions.

However, if both IDR and EDR are to be retained as redress for consumers, the SPF Bill should clearly articulate:

- In what situations are regulated entities liable for non-financial or financial remedies within internal and external dispute resolution schemes? Any liability should be linked to a breach of the relevant sector specific code.
- How is which remedy is appropriate in the circumstances to be determined?
- How are the liability for remedies to be shared across entities involved in the scam loss?
- What safeguards will be introduced to prevent abuse? (for example materiality thresholds, exclusion of vexatious claims, time frames to bring claims, minimum standards for substantiation of claims etc)
- How do IDR, EDR and the enforcement provisions overlap?

[2] Section 138 of the *Online Safety Act 2021* operates similarly, in that the Act lists examples of matters that may be dealt with in industry codes and standards, but civil penalties arise from non-compliance with the codes/standards, not the primary legislation.
[3] See clause 58DC of the SPF Bill.

Problem 3: The definition of a 'scam' is overly broad and unworkable

The current definition of a 'scam' within the SPF Bill is exceptionally broad, and could extend even to a person on a messaging app asking for names or birthdays. This means platforms must take action against a wide range of communications, not just "real scams", potentially impacting genuine consumer and small business communication.[4]

It is a broad definition because it is intended to apply to a wide variety of sectors regulated by the SPF Bill. However the nature of scam activity means that scams appear differently at different points of their 'life', making one definition applicable to all sectors unworkable, and requiring sectors to over-compensate to meet obligations.

Solution: Rework the definition of a scam
The definition of a scam should target the real danger of scam activity. Whilst DIGI believes the definition of a scam should sit within sector-specific codes and tailored specifically for each sector, if the definition is to sit in the SPF Bill it should:

- Be limited to obtaining personal information alongside a financial or other benefit
- Be limited to direct attempts, and not include indirect attempts
- Be limited to ensure overcorrection is not required to meet any SPF obligation

DIGI suggests removing 'personal information' from the definition of a scam so that there is greater focus on the obtainment of financial benefit. Alternatively, at a minimum, the second 'or' in 58AGb should be replaced with 'and'.

Problem 4: The definition of 'actionable scam intelligence' is too broad

The definition of 'actionable scam intelligence' is also unhelpfully broad. Under a platform's obligation to 'Report', they must notify the ACCC of actionable scam intelligence. This means:

1. The ACCC is likely to be inundated with millions of low-quality reports about potential scams. It is unclear what the ACCC will do with all of that information, how they will receive it, and how they will use it to inform consumers about potential scams.
2. Since the bar for information to be 'actionable scam intelligence' is so low, there is a real question of exactly how much action could be taken by a platform on such limited information. It also risks diverting resources away from addressing high risk harms.

Solution: Refine the definition of 'actionable scam intelligence'
The definition of actionable scam intelligence should specify that a singular report about scam activity does not constitute 'actionable scam intelligence'. DIGI calls on the Government to clarify how significant any intelligence about scam activity needs to be to make a report (for example, clarifying that reports are only required for scams that present a serious risk of harm to consumers). This should be accompanied by introducing a provision in the SPF Bill to clarify that reporting should only be required when the information received is credible and there is a known potential for the intelligence to assist other companies to take action against scams to protect consumers.

At a minimum, it would also reduce the volume of low-quality scam reports to the ACCC if the knowledge threshold for actionable intelligence in s.58AI was amended so that an entity is not required to report when they have reasonable grounds to "suspect" that a communication is a scam. It would be more consistent with the objectives of the SPF Bill if the reporting obligation was triggered when an entity had "reasonable grounds to believe" that a communication is a scam.

[4] See Clause 58AG of the SPF Bill for the definition of 'scam' and 58AI for the definition of 'actionable scam intelligence'.