5 January 2026

Director, Scams Legislative Policy Unit
Digital Policy and Corporations Division
The Treasury
Langton Crescent
Parkes ACT 2600

via email: scamspolicy@treasury.gov.au

Dear Sir/Madam

Scams Prevention Framework – Draft law package and position paper

The Australian Small Business and Family Enterprise Ombudsman (ASBFEO) welcomes the opportunity to comment on the Scams Prevention Framework's (SPF) draft designation instruments and position paper outlining the Treasury's preliminary thinking on the sector codes and rules. We support the SPF's objective to create obligations on designated businesses to take reasonable steps to prevent, detect and disrupt scams, initially focusing on banking, telecommunications and digital platforms.

Small and family businesses are the backbone of the Australian economy and, like individuals, are vulnerable to being scam victims and are targeted by scammers through a variety of channels. The National Anti-Scams Centre found that, in 2024, small businesses made 1909 reports to Scamwatch with financial losses totalling $13.1 million, with the highest losses resulting from investment scams and with false billing being the most reported scam type.[1]

The ASBFEO makes the following comments in relation to the draft instruments and preliminary thinking on sector codes and rules:

Draft Instruments – Designation

The ASBFEO notes that the proposal to limit the **banking sector** definition to authorised deposit-taking institutions (ADI) is intended to maintain consumer trust in ADIs who are reported to be the most common payment method by victims in scams. While this will enable the SPF to cover a substantial proportion of scam activity within the banking sector, scam activity can also be perpetrated through non-ADI providers of banking services, which is often a type of finance accessed by small business. These providers are likely to have weaker protections against cyber and scam risk, or can be exploited by scammers targeting small business.[2] Furthermore, as many are *not* required to be members of the Australian Financial Complaints Authority small businesses can struggle to have their issues resolved even when the provider may be at fault.

The ASBFEO notes that the proposed definition of the **digital platforms** sector, while covering services that are commonly used by small and family businesses, does not include online

[1] *Targeting Scams – Report of the National Anti-Scam Centre on scams data and activity 2024*, NASC, p30. NB: Small business reports are from businesses with less than 20 employees, suggesting much higher scam losses reported by entities defined as 'small business' under the SPF.
[2] For example, see *ASIC disqualifies former Viewble Media director for four years*, ASIC media release, 26 July 2022; and related ASBFEO news article.

marketplaces such as eBay and Amazon.com. Our assistance function sees a number of instances where small business sellers are being scammed on these platforms, for example, where scams are perpetrated by consumers purchasing through a platform falsely claiming chargebacks for goods that have been delivered.[3] While ASBFEO enjoys a constructive problems-solving relationship with eBay and Amazon.com, we consider that services of this kind should be covered by the SPF.

With the SPF designed as a whole-of-ecosystem framework that can be expanded over time, the ASBFEO urges the Government to, as soon as is practicable, expand into **other sectors and services** where small businesses are vulnerable to scam risk, for example, online marketplaces (see above), superannuation and settlement payment platforms (business email compromise).

Position paper – preliminary thinking on SPF codes and rules

For the SPF to be effective, regulated entities need to have a clear understanding of their obligations and how to achieve them with minimal compliance cost, while scam victims need clear and accessible pathways to seeking redress for scam losses and efficient and accessible mechanisms for resolving other disputes that may be judged as not being of a scam-nature, and for having their impacted service restored as quickly as possible. 'Clarity, certainty and minimising regulatory complexity' should therefore be **overarching policy considerations** to be taken into account when developing the SPF rules and codes obligations.

In this regard, the ASBFEO supports the codes and rules having, where possible, prescriptive obligations that enhance regulatory clarity and certainty. Where obligations apply to small businesses our experience is that they typically lack the time, systems sophistication and resources to work out how to comply with principle-based obligations, and instead ask the simple question: 'What do I need to do to comply?' Timeframes for handling scam complaints is one obvious area for prescription but there are likely to be others, and to support compliance we encourage the development of clear guidance that includes worked examples and case studies.

Moreover, ASBFEO believes that the specific obligations arising from the SPF should be nested in a more general duty for respondent entities to have accessible, efficient, effective and promoted internal dispute resolution (IDR) and escalation processes. ASBFEO has shared its extensive experience supporting dispute resolution for matters involving small businesses and services providers in designated sectors with policy makers and the ACCC. A duty on respondents to establish, resource and maintain effective and responsive IDR processes will support the fulfilment of the SPF public policy objectives by ensuring that there is no dispute delineation 'hurdle' to having matters appropriately addressed.

This will help address a gap in support for dispute resolution for digital platforms, in particular. We already have extensive experience supporting small businesses with a dispute with a digital platform, where their account deactivation or service exclusion is justified as an action being required by the regulator or platform's Community Standards, but is made without notice, finesse or human oversight. This more assertive intervention posture by digital platforms is said to arise

[3] For example, see *Small businesses losing thousands to fraudulent online chargeback claims*, ABC News, 3 December 2025.

from heightened threats and cyber risks posed by more capable 'bad actors', yet scam prevention may not be the catalyst or cause for the intervention. The reasonableness of these interventions and consequence for small businesses, reliant on the service that has been unilaterally withdrawn, seem not to be weighed or able to be questioned. For banking and telecommunications sectors, AFCA and the TIO requirements and mechanisms (respectively) offer existing mechanisms for support.

Regarding the proposal to enable individuals / users to opt out of certain SPF protections, the ASBFEO is wary about how this would work in practice. We would caution against implementing features that add substantial complexity to the framework and create uncertainty about how the obligations apply. We also suggest that any such arrangement should mitigate the risk of regulated entities pressuring a customer to opt out of important scam protections as a condition of using their service. The SPF protections should be dependable for small and family businesses.

We also note the proposal to reference existing industry standards to ensure alignment, noting the IDR process 'gap' for many digital platforms. ASBFEO broadly supports this approach, which can enable more streamlined implementation and compliance, but would expect that applicable standards are only referenced where they provide a sufficient level of scam prevention that supports the policy objectives of the SPF.

Principle 2: Prevent

It is essential that scam education efforts are inclusive and accessible to diverse user groups. To be effective with small business, strategies must recognise the time- and resource-poor nature of many small and family businesses, with many businesses owners having a CALD background. Multiple formats and communications channels should be utilised to maximise reach and accessibility, including leveraging the role of a business's trusted advisor.

Principle 3: Detect

Detecting potential scam activity is crucial to scam prevention and will require regulated entities to be proactive and urgent in their actions. Where an entity identifies potential scam activity on their service they must promptly notify the consumer in a way that is accessible (including utilising multi-factor authentication to ensure they are genuine), investigate in a timely manner, and if they need to act it must be proportionate to the risk to minimise disruption to the impacted service.

For a small business, losing access to a critical service can have a significant impact on their operations. For example, being locked out of a social media account or having a telco service blocked can see a business lose potential sales and bookings, and makes it much harder for the business to communicate with its customers, impacts which can be a drain on their scarce time, resources and income, and if the disruption is prolonged can even pose a threat to their viability.

It is therefore essential that code and rule obligations emphasise proactivity, timeliness and action that is targeted and proportionate to the identified risk, and minimises service disruption.

Principle 5: Disrupt

Similar to detect, the actions regulated entities take to disrupt scams must be timely, targeted and proportionate, and seek to minimise service disruption and avoid unintended consequences. The

entity should notify the consumer promptly and in a way that is accessible, and if the impacted service must be locked or blocked to disrupt the scam, every effort must be made to restore the service as soon as possible. Deactivation of the service should only be considered as a last resort, with the consumer promptly notified and having the ability to contact the service provider, including the ability to engage with a 'real' person at the service provider and expedited 'warm referrals' to competent ADR providers where appropriate, to enable early service restoration.

Principle 6: Respond

Timely and effective responses to consumers impacted by scams is key to the success of the SPF. The pathway to making a complaint and accessing dispute resolution must be clear, transparent and accessible, and the regulated entity must promptly act to resolve the dispute and provide an appropriate remedy, which may involve restoring the impacted service.

For small businesses, access to effective dispute resolution is essential, especially where it involves the disruption of an impacted service. In this regard, the proposed 30 calendar day timeframe for issuing a remedy (from receiving a scam compliant) may be appropriate for some remedies, but where that process involves service disruption we recommend a much shorter timeframe for restoring the service.

For many small business customers, accessing the service provided by the designated SPF respondents is vital to their ability to engage in trade and commerce. The timeframe for dispute resolution and service restoration should reflect greater urgency given the loss of customer contact, income earning capability and ability to function, while contested questions of fulfilment of preventative obligations may take longer to determine.

ASBFEO strongly supports the SPF requiring that regulated entities establish accessible and transparent IDR, as having a pathway for consumers to raise complaints and have them resolved should be apply to providers of any product or service. A number of digital platforms do not have effective IDR processes and we, along with State and Territory Small Business Commissioners, are receiving a growing number of complaints from small businesses who have had their social media account deactivated without warning, and who are unable to contact the platform to dispute the decision and have it promptly review and resolved (see article).

We therefore submit that the IDR processes regulated entities are required to have in place to handle scams complaints, should have the capacity to handle *all* consumer complaints. It is imperative this capability is developed as soon and possible and could progress alongside the uplift required by the SPF, supported by an EDR process for non-scams digital platforms complaints.

Small business definition

The ASBFEO supports the current SPF definition of small business of <100 employees and <$10m annual turnover. The definition captures a wider range of businesses than under a number of other small business definitions, recognising that many smaller businesses are vulnerable to scam risk. The employee component of the definition also aligns with the ASBFEO's own small business definition which provides for broader access to our dispute resolution and support services.

ASBFEO has been extensively involved in sharing our experiences, practical engagement and 'field evidence' on digital platform and non-AFCA lender business-to-business dispute with portfolio, policy maker and the ACCC (through the Commission's various digital platform inquiries) and is available to assist wherever possible with Treasury's Scam Legislative Policy Unit.

If you require any further information, or have any questions regarding our submission, please email the ASBFEO Policy and Advocacy team at advocacy@asbfeo.gov.au.

Yours sincerely

The Hon. Bruce Billson

Australian Small Business and Family Enterprise Ombudsman