4 October 2024

Director
Scams Taskforce
Market Conduct and Digital Division
The Treasury
Langton Crescent
Parkes ACT 2600

via email: scamspolicy@treasury.gov.au

Dear Sir/Madam

Scams Prevention Framework –Exposure Draft Legislation

The ASBFEO welcomes the opportunity to provide comments to the Treasury regarding the draft legislation for the Scams Prevention Framework (the Framework). We support the objective of the framework to set clear roles and responsibilities for the Australian Government, regulators and the private sector to prevent, detect, disrupt and respond to scams, initially focusing on the banking, telecommunications and digital platform sectors.

Small and micro businesses in Australia surveyed by the Australian Competition and Consumer Commission (ACCC) lost $13.7 million to scams in 2022 across 2,019 reports. The survey reveals that 'phone and email scams had the highest impact on small and micro businesses, accounting for $10.8 million of the losses.[1] Additionally, a survey of small businesses in 2021 by the Australian Cyber Security Centre found that 16% of cyber security incidents involved scams and fraud.[2]

This reform will not only help reduce the opportunity for scammers to exploit small and family businesses, but also provide a mechanism to require key sector businesses to take timely steps to recover payments made to scammers where possible.[3]

Recommendation 1: Treasury should amend the draft bill to include compensation as an available remedy in Internal Dispute Resolution (IDR) and External Dispute Resolution (EDR).

Paragraphs 1.197 and 1.203 of the Exposure Draft Explanatory Materials establishes that the intent of the framework is to provide victims of scams with compensation or other remedies following IDR or EDR. However, section 58BZC (1)(a)(b) of the Framework, while outlining the requirement for an accessible and transparent internal dispute resolution, does not clarify that compensation or other remedies by the regulated entity is a potential outcome of IDR and EDR.

Treasury should amend the framework to define the intent of IDR and EDR to provide a pathway for redress, including compensation, to a Framework consumer for a regulated service where a regulated entity has not complied with their obligations under the Framework.

[1] Australian Competition and Consumer Commission (ACCC), *Targeting Scams, Report of the ACCC on scams activity 2022,* ACCC, Australian Government, April 2023, p.12
[2] Australian Cyber Security Centre (ACSC), *Cyber Security and Australian Small Businesses, Results from the Australian Cyber Security Centre Small Business Survey,* ACSC, Australian Government, Accessed 31 January 2024
[3] The Treasury, *Scams – Mandatory Industry Codes – Consultation paper,* the Treasury, Australian Government, November 2023, p.6

We support the framework's requirement that regulated entities have internal dispute mechanisms. To prevent dispute resolution timeframes being extended indefinitely, Treasury should require entities to resolve disputes within 28 business days of receiving notice. IDR mechanisms should comply with International Standards, setting out:

- timeframes for dispute resolution
- what methods of dispute resolution will be offered
  - International Standard ISO 10003 outlines the functions of facilitative, advisory and determinative methods of dispute resolution[4]
- what criteria will be used for dispute resolution
- what remedies are available through internal dispute resolution
- the escalation process if IDR fails to resolve the dispute

Recommendation 2: Safe Harbour provisions should include the requirement for regulated entities to return small businesses to business as usual as rapidly as possible while investigating claims of scams.

Section 58BZ of the Framework provides regulated entities with 28 business days safe harbour for any proportionate temporary disruptive action while investigating actionable scam intelligence it has received. We consider that small businesses, whose digital platforms are locked after being flagged as potential scams, should be provided the opportunity to promptly engage with the regulated entity to ensure their legitimate business activities are not unfairly disrupted. Regulated entities should have processes in place to remove potential scam material, while allowing small businesses to continue business operations while the matter is investigated.

Digital platforms have fundamentally changed the way in which Australian small businesses do business. Digital platforms are a valuable tool for small businesses to attract new customers, advertise and sell products and services, and build brand loyalty. They serve as single points of contact for businesses to reach a significant portion of the Australian and international markets, with many small and family businesses relying heavily on these platforms. Despite the benefits, we are aware of small business concerns arising through the increased use of, and dependence on, digital platforms.

A common issue affecting small businesses is loss of access to their social media account through cybercrime. Hackers may target small business accounts to exploit their public reach and trust as well as any payment credentials that have been set up, to pay for and disseminate fake advertisements designed to scam Australian consumers and social media users. While this is ongoing, the affected small business cannot resolve the issue with the social media platform because the platform's dispute-resolution process requires account access to be initiated. These inadequacies in digital platforms' complaint pathways and dispute-resolution processes are causing significant harms to affected small businesses and the broader public.

As part of our assistance for small businesses that are hacked, we have developed extensive relationships with digital service providers, so that we can organise support for small businesses

[4] International Organisation of Standardisation (ISO), *International Standard 10003, Quality management – Customer Satisfaction – Guidelines for dispute resolution external to organisations,* ISO, 2018, p

even when they are locked out of their accounts. However, this is the type of access that platforms should directly provide to their small business customers that encounter such issues.

In the case of one provider that ASBFEO Assistance works with, 69% of cases resolved in 2024 took longer than one month to resolve, and 44% took longer than two months. Changes in the number of support staff coincided with an increase in resolution timeframes, as the number of disputes continues to grow.

We provide the following example of a small business helped by the ASBFEO Assistance team whose digital platform account was hacked and used to run fraudulent advertisements. The small business owner was locked out of their account and reached out to their digital platform provider in February 2024. In the absence of a response, ASBFEO Assistance contacted the provider in March. However, the provider did not confirm a fraudulent spend until May, and the dispute was not resolved until June. The small business owner advised that the inability to run adds through their digital platform provider for 4 months led to a loss of sales of approximately $10,000 per month.

While many digital scam disputes are valued less than $10,000, losses in this range can still be highly damaging for small businesses. Approximately 43% of small businesses failed to make a profit and 75% of small business owners take home less than the average wage.[5]

Recommendation 3: The definition of consumer in the ePayments code should be amended to align with the new definition in the Treasury Laws Amendment Bill 2024: Scams Prevention Framework

Clause 58AH of the Framework, defines consumers as Australian citizens, residents and small businesses having fewer than 100 employees, which is more expansive than the ePayments Code. The definition of consumer in the ePayments code should be amended to align with the definition in the Framework to provide protections to businesses having fewer than 100 employees.

Further, to help align the ePayments Code with the Framework, the definition of 'mistaken internet payment' in the ePayments Code should be amended to remove the exclusion of scams from the definition. Section 29 of the ePayments Code requires the Authorised Deposit-Taking Institution (ADI) to investigate a report of a mistaken internet payment and provide the consumer of the outcome of the investigation in writing within 30 business days of the report being made.

Where an Authorised Deposit-Taking Institution rejects the claim that a mistaken payment has occurred, the ePayments Code stipulates that the small business must be provided with information about the ADI's IDR process, as well as information about lodging a complaint through the Australian Financial Complaints Authority, if the dispute remains unresolved. Aligning the ePayments Code and the Framework will clarify the obligations of regulated entities.

Recommendation 4: Include transaction-based digital platforms such as online marketplaces in future tranches.

The proposed framework initially applies to banks, telecommunication service providers and Digital Communications Platforms but will exclude transaction-based digital platforms such as online marketplaces. While the reported use of businesses receiving orders via a third-party website, platform, app or online marketplace is 12% for the financial year ending 30 June 2022,

[5] Australian Small Business and Family Enterprise Ombudsman (ASBFEO), Small Business Matters, ASBFEO, June 2023, pp 15-16

this is expected to grow and will present a potential risk for small and family businesses.[6] The ACCC's Digital platform services inquiry – Interim report No. 4, notes that while Australia lags behind the United States and the United Kingdom in online retail sales, the situation in Australia has significant potential for change. [7]

We encourage the government to continue to monitor the activity of online marketplaces and consider expanding the framework to include online marketplaces in a future review.

Recommendation 5: The Australian Government should implement the ACCC's recommendation of a mandatory 'notice-and-action' mechanism for digital platforms to protect against scams, harmful applications, and fake reviews.

In our May 2022 submission to the ACCC Digital Platform Services Inquiry Interim Report No.5, we recommended that digital platforms develop appropriate small business dispute resolution processes and provide escalation contact points.[8] We acknowledge that the Australian Government has:

- supported in principle the ACCC's recommendation for digital platforms to be subject to 'mandatory internal dispute-resolution standards that ensure accessibility, timeliness, accountability, the ability to escalate to a human representative and transparency'
- called on the digital platform industry to develop voluntary internal dispute resolution standards by July 2024.[9]

Nonetheless, at the time of writing, our cases are evidencing that any movement in this regard is insufficient and does not appear to extend across all platforms.

Regulated entities should have processes in place to remove potential scam material, while allowing small businesses to continue business operations while the matter is investigated.

Small businesses are especially vulnerable to fake review campaigns and fraudulent misrepresentation, as they lack the knowledge and resources to prevent and combat scams. In our consultations, we heard about cases of small businesses being held to ransom over fake reviews, with scammers only removing them once they had received payment. We have heard of commercial service providers that claim to support consumer traction for new entrants by generating hostile contrived reviews for existing providers in a target market.

Enforcement action is retrospective, applied on a case-by-case basis, and investigations can take a long time. These lengthy processes are damaging to small businesses engaging with digital platforms, as fake reviews and fraudulent misrepresentation of their business may remain visible while investigations take place, often resulting in small business owners watching the damage to

[6] Australian Bureau of Statistics (ABS), *Characteristics of Australian Business E–commerce,* ABS, Australian Government, June 2023, accessed 6 February 2024
[7] The Australian Competition and Consumer Commission (ACCC), *Digital platform services inquiry Interim report No. 4 – General online retail marketplaces,* ACCC, Australian Government, March 2022, p 2
[8] ASBFEO, *Submission to ACCC Digital Platform Services Inquiry,* ASBFEO, Australian Government, May 2022, accessed 16 August 2024
[9] Australian Competition and Consumer Commission, *Digital platforms services inquiry: Interim report No. 5 – Regulatory reform,* ACCC, Australian Government, September 2022, p. 16; The Treasury, Government Response to ACCC Digital Platform Services Inquiry, The Treasury, Australian Government, pp. 2-3.

their business occur in real time with no ability to stop it. This can impact not only business viability but the mental health of the small business operator and their employees.

If you require any further information, would like us to supply small business case studies or have any questions regarding our submission, please contact the ASBFEO Policy and Advocacy team via email at advocacy@asbfeo.gov.au.

Yours sincerely

The Hon Bruce Billson
Australian Small Business and Family Enterprise Ombudsman