

15 February 2024

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

via email: scampolicy@treasury.gov.au

Dear Minister

Scams – Mandatory Industry Codes

The ASBFEO welcomes the opportunity to provide comments to the Treasury regarding the proposed Scams Codes Framework (the Framework). We support the objective of the framework to set clear roles and responsibilities for the Government, regulators and the private sector to prevent, detect, disrupt and respond to scams.

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 provide a mechanism to require relevant key sector businesses to *take timely steps to recover payments made to scammers where possible*.³

Recommendation 1: Consider expanding the framework to include online marketplaces in a future review

The proposed framework will initially include Digital Communications Platforms but will exclude transaction-based digital platforms such as online marketplaces.⁴ While the reported use of business receiving orders via a third-party website, platform, app or online marketplace is at 12% for the financial year ending 30 June 2022, this is expected to grow and will present a risk for small and family businesses.⁵ 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.

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.

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

⁴ The Treasury, *Scams – Mandatory Industry Codes – Consultation Paper*, Treasury Australian Government, 2023, p.10

⁵ Australian Bureau of Statistics (ABS), *Characteristics of Australian Business E-commerce*, ABS, Australian Government, June 2023, accessed 6 February 2024

Recommendation 2: Digital Platforms should improve and clearly outline their internal dispute resolution processes for small business

The proposed response obligations require an organisation to have *user friendly, effective, efficient, transparent, and accessible options for consumers or users to report a scam*. However, in our interactions with the digital platforms, their complaints systems are not always consistent and can use automated systems with no human escalation point.

We recommended that the government work with the digital platforms to develop appropriate small business dispute resolution processes and provide escalation contact points, including identifying and promoting ASBFEO as an external escalation point where internal dispute resolution processes are unresponsive or not able to resolve a dispute. Implementing adequate internal dispute resolution processes and dedicated contacts would enable small businesses to have their dispute handled efficiently and resume operating their businesses sooner.

Recognising the need for these mechanisms and key attributes in a Code would advance the informal arrangements ASBFEO has in place with a number of digital platforms and where we are responding to increased requests for dispute assistance between small businesses and digital platforms.

Recommendation 3: 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.

Digital platforms provide a mechanism for small businesses to undertake their sales and marketing activities, but they can also facilitate fraudulent activities. A 'notice-and-action' mechanism would allow any individual or entity to notify digital platforms of potential illegal content on their service, and a requirement for the digital platform to act on this notification.

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. The inaction on these fake reviews and fraudulent misrepresentations during investigation processes often results in small business owners watching the damage to 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.

Recommendation 4: The Australian Government should refresh an e-invoicing education and awareness campaign for small businesses.

With the increasing prevalence of scams and cybersecurity incidents many small businesses are vulnerable to invoice scams. We often hear of reports from small businesses where they have sent an invoice for payment to a client only to have the email intercepted by malicious actors who change the bank account details on the invoice.

E-invoicing provides a mechanism for small businesses to send an invoice directly to the accounting software of another business or government securely via the Peppol network. The adoption of e-invoicing is estimated to be between 10 to 15 per cent of all businesses in Australia and

approximately 90 per cent of small and medium enterprises still operate in a manual environment with paper and emailed PDF invoices.

To further support the government initiatives to reduce scam activity we recommend the government refresh an e-invoicing education and awareness campaign for small businesses.

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 via email at advocacy@asbfeo.gov.au.

Yours sincerely



The Hon Bruce Billson

Australian Small Business and Family Enterprise Ombudsman