



25 June 2026

Director, Scams Prevention Policy Unit  
Digital Policy and Corporations Division  
The Treasury  
Langton Crescent  
PARKES ACT 2600

via email: [scampolicy@treasury.gov.au](mailto:scampolicy@treasury.gov.au)

Dear Ms George,

### **Scams Prevention Framework codes and rules exposure draft**

The Australian Small Business and Family Enterprise Ombudsman (ASBFEO) welcomes the opportunity to comment on the Scams Prevention Framework (SPF) codes and rules exposure draft. We support the SPF's objective to prevent and respond to scams impacting small businesses in Australia.

Small businesses are at risk of harm from scams and are being targeted through a variety of methods, including phishing attempts and fake invoices.<sup>1</sup> In 2025, small businesses lodged 2,228 reports to Scamwatch, with 287 reporting financial losses amounting to \$9.5 million.<sup>2</sup> While reported losses declined by 27.9% compared to 2024, this does not necessarily mean a reduction in harm as it does not account for unreported scams.<sup>3</sup> Continued efforts are therefore required to protect small businesses from scams and the ASBFEO supports implementation of the SPF.

The ASBFEO makes the following comments in relation to the common, banking and digital platforms draft code, and the internal dispute resolution (IDR) position paper:

#### **Exposure draft and explanatory statement – Competition and Consumer (Scams Prevention Framework – SPF Codes) Instrument 2026**

##### ***Principles 2 and 5: Prevent and Disrupt (Digital platform provisions)***

Many small businesses use social media accounts as a key part of running their business, including to advertise their goods and services, generate sales and bookings, and communicate with customers. Any disruption to the account — even for a few days — can have a devastating impact on the business, for example, through lost sales and bookings, disrupted customer communication, reputational damage, and significant emotional and financial stress for the business owner.

The ASBFEO has received a large — and growing — number of complaints from small businesses who have had their social media account deactivated following an assessment by a digital

---

<sup>1</sup> National Anti-Scam Centre, *Targeting scams - report of the National Anti-Scam Centre on scams data and activity 2025*, National Anti-Scam Centre, Australian Competition and Consumer Commission, Australian Government, 2026. NB: small business includes reports from small (5-19 employees) and micro-businesses (0-4 employees).

<sup>2</sup> National Anti-Scam Centre, *Targeting scams - report of the National Anti-Scam Centre on scams data and activity 2025*.

<sup>3</sup> National Anti-Scam Centre, *Targeting scams - report of the National Anti-Scam Centre on scams data and activity 2025*.



platform's algorithmic tool against their community standards.<sup>4</sup> These businesses have had their account deactivated without warning and digital platforms lack IDR processes that enable the business to have their complaint promptly reviewed and resolved. This has brought into question the accuracy of default algorithms driving decisions that lack any human oversight, and highlights shortcomings in digital platform complaints handling processes and the significant consequences that account deactivation can have for a small business.

The ASBFEO notes the draft code and explanatory statement require that a digital platform include in its terms of service that it will take action — which may include banning users and disabling digital platform accounts and content — if it reasonably suspects a scam, including during and following an investigation. This action includes issuing a warning and taking steps to 'suppress, reduce, or otherwise limit the activity from being displayed to its SPF consumers'.

While we recognise the need for digital platforms to take decisive action to prevent further scam activity, they should also be required to make the necessary investments into tools and processes that accurately detect scams and, in doing so, minimise the risk of false positives that result in innocent small businesses having their social media account disrupted.

We are also concerned that the 28-day timeframe for investigation is far too long for small business users given the significant business impact of an account disruption. We recommend a much shorter timeframe — of 14 days or less — for addressing scam incidents involving small business that includes providing regular updates during the investigation. When a digital platform is investigating a scam, we suggest requiring the digital platform to work with the affected business to re-route customer traffic to an alternative platform (e.g. business email, official business website or phone number) while the account is disrupted. Digital platforms should also establish clear and accessible IDR processes for small businesses seeking resolution of a complaint regarding account deactivation (see below).

The explanatory statement also notes that, currently, references to prohibiting scams and taking action against scam activities in digital platforms' terms of service are inconsistent, sparse or absent. The ASBFEO supports the SPF obligating digital platforms to cover such matters in more detail that is expressed in plain-language and is easy for users to locate.

### **Position paper - internal dispute resolution (IDR)**

Digital platforms do not currently have effective IDR processes. It is therefore imperative that digital platforms establish complaints-handling capability and effective IDR processes. The obligations imposed by the SPF provide a strong incentive to do this.

The ASBFEO supports regulated entities establishing accessible and transparent IDR for scams complaints. We note that a multi-party IDR approach may be necessary given a scam event can involve more than one regulated entity. However, while this approach may need to be more complex than typical IDR processes, it is important it be clear and accessible to all SPF consumers, including small business.

---

<sup>4</sup> In Quarter 1, 2026, digital platform disputes were the most common type of dispute where ASBFEO provided one-to-one support, accounting for 35.4% of the 548 new actively managed cases, Source: Australian Small Business and Family Enterprise Ombudsman (ASBFEO), *ASBFEO Quarterly Report: 1 January to 31 March 2026*, ASBFEO, The Treasury, 2026, accessed 24 June 2026, p 6.



The ASBFEO supports an IDR approach that handles investigations and complaints in a way that is proportionate to the value and complexity of the scam loss. The proposed automatic reimbursement for lower-value complaints would provide for a streamlined process that is both timely and efficient, particularly where the investigation costs would exceed the value of the loss.

The ASBFEO continues to advocate for digital platforms establishing IDR processes that handle all types of complaints, not just scam complaints. While the multi-party IDR approach may be specifically designed to handle scams complaints, the IDR capability that digital platforms develop under the SPF should be expanded to handle other complaints on their platforms (e.g. small business account deactivation).

**Designation: ‘covered digital platform service’**

Regarding the designation of digital platforms, the ASBFEO encourages the Government to expand the definition of ‘covered digital platform service’ to include a broader range of digital platform services utilised by small businesses.

The definition should include online marketplaces, online shops (e.g. Amazon.com and eBay), and food and drink delivery services (e.g. Uber Eats, DoorDash) where we note that impersonation scams are currently targeting users of food delivery platforms, including restaurants, customers and delivery workers.<sup>5</sup>

If you require any further information, please do not hesitate to contact the Policy and Advocacy team via email at [advocacy@asbfeo.gov.au](mailto:advocacy@asbfeo.gov.au).

Yours sincerely

**Lynda McAlary-Smith**

Australian Small Business and Family Enterprise Ombudsman

---

<sup>5</sup> ScamWatch, *Scam alert: Food delivery scams*, ScamWatch website, 12 June 2026, accessed 18 June 2026.