



9 January 2025

Senate Standing Committee on Economics
PO Box 6100
Parliament House
Canberra ACT 2600

Submitted by email: economics.sen@aph.gov.au

Dear Senate Economics Legislation Committee

RE: Scams Prevention Framework Bill 2024

Thank you for the opportunity to provide feedback on the *Scams Prevention Framework Bill 2024 (the Bill)*. CHOICE also supports the joint submission led by Consumer Action Law Centre (**Joint Consumer Submission**). This submission primarily focuses on the role of digital platforms in enabling scams, an area which CHOICE has focused on in recent years.

Summary

There is a desperate need for laws to require businesses who enable their services or platforms to be exploited by scammers to do more to protect their customers. Digital platforms provide perhaps the best example of this. Many digital platforms are operated by trillion dollar companies that are at the cutting edge of technological development. However, these businesses are not currently incentivised to use their technological prowess or ample resources to adequately protect consumers. The platforms of companies like Meta and Google are currently inundated with scam accounts, communications and advertisements that are causing consumer harm.

The current voluntary approach to scam protection is not working and we need strong laws, with penalties, to incentivise the tech giants, as well as banks, telecommunications platforms, super funds and other businesses that might be captured in the future, to take scam prevention seriously. The Bill would establish vital obligations to take reasonable steps to protect their customers from scams and introduce a baseline set of obligations that should have existed at law years ago. There are no clear equivalent obligations under our current legal framework, and this desperately needs rectification.

For this reason, **we urge the Committee to recommend that the Bill is passed**. Our current laws leave victims of scams carrying the entire burden of scams, and let big businesses off the hook for inadequate security and safety. To improve the scam prevention framework, we also **urge the Committee to recommend that the Government prioritises work to expand the Scams Prevention Framework (SPF) to apply to online marketplaces, superannuation firms and crypto platforms**, and provides a timeline for their inclusion as soon as possible.

It is also important that consumers can get their money back when businesses fail to protect them from scams through a fair, fast, simple and effective mechanism. The details of how this will work under the framework to be established by the Bill requires further clarification. A legislative framework establishing a presumption that victims of scams would be reimbursed would be the simplest and most consumer friendly approach. However, we remain hopeful that the approach to dispute resolution and redress to be established under the scam prevention framework could also work. **We endorse the recommendations made in the Joint Consumer Submission** to ensure this. CHOICE also notes that the effectiveness of any consumer redress mechanism should be considered as part of the three-year review of the SPF proposed in the Bill.

If the Bill is not passed, industry scam prevention standards will continue to fall short of expectations and consumers will bear the consequences. We also expect that the threat of impending regulation has contributed to the recent goodwill and efforts of some industries to cooperate to improve scam prevention, via the National Anti-Scams Centre (**NASC**). Without new legal obligations, the incentive for industry to prioritise scam prevention is likely to recede. Delays will also push back the timeframe to extend obligations to other industries susceptible to scammers, like online person-to-person marketplace operators (eg Facebook Marketplace), superannuation firms and crypto platforms.

Business scam efforts are insufficient under current legal framework

Despite ample public scrutiny of scams in the media and the looming threat of legislation over the last few years, the efforts of digital platforms to prevent scammers exploiting their services continue to fall well short of community expectations. The multi-national companies in this sector will not dedicate meaningful resources to addressing scams unless they are forced to do so.

In the ACCC's Targeting Scams report on scam losses in 2023, scams using social media or email contact methods were the two listed categories of scams for which losses increased compared with 2022 reports.¹ Losses to scams on social media reported to the ACCC in 2023 represented a 249% increase on 2020 figures.²

Consumers have little faith in digital platforms to protect them from scams. In June 2024, CHOICE conducted nationally representative research on people's experience and understanding of scams and scam prevention. We asked respondents about whether particular businesses did enough to protect them from scams. 68% of respondents disagree that social media and digital platforms like Google, Facebook and

¹ ACCC, Targeting Scams: Report of the National Anti-Scam Centre on scams activity 2023, published April 2024.

² National Anti-scams Centre in action, Quarterly update, October to December 2023 available at: https://www.nasc.gov.au/system/files/National-Anti-Scam-Centre-in-Action_quarterly-update-October-to-December-2023.pdf

Twitter do enough to protect them from scams.³ This was the highest disapproval rate of any industry, and compared with 39% for banks and financial institutions. This level remains unchanged from the findings in June 2023, where 66% of respondents found social media and digital platform companies were not doing enough to protect users from scams.⁴

In recognition of these shortcomings, in November 2024, CHOICE 'awarded' Meta a Shonky for failing to protect Australian consumers from scammers.⁵ We 'award' Shonkys to businesses annually that we have identified as the worst products and services of the year.

CHOICE reports likely scam ads

To test Meta's performance on scam prevention, in mid-2024, CHOICE reported three highly suspicious scam advertisements on Facebook. Two of the ads were promising thousands of dollars of "guaranteed returns" if you invested in their crypto advice, while the other featured an image of TV personality Robert Irwin promising that he would pay you 500 euros if you downloaded an app.

Two of the ads were taken down within 24 hours of being reported, however, the account that posted the Irwin ad was allowed to quickly re-post a near identical ad soon after. The other 500 active sponsored ads held by the account also remained active. The third ad was taken down, but this took over four days.⁶

Meta has since announced it will introduce verification of financial licencees for advertisements from February 2025 - something it already does in other countries like the UK,⁷ and Google has been doing since 2022.⁸ While this is welcome news, it does not reduce the need for legislative obligations - we strongly suspect it is only with the very real threat of the Bill passing that Meta has decided to take this step.

While Google has led Meta on verifying financial service advertisers, other CHOICE investigations indicate that its platforms are still plagued by scam advertisements. In 2023, CHOICE reported a number of scam advertisements on Google for well known Australian fashion brands, such as Decjuba, Country Road and Peter Alexander. Google responded to CHOICE reports about these ads, indicating that it had taken 'appropriate action', yet the ads

³ CHOICE Consumer Pulse June 2024 is based on an online survey designed and analysed by CHOICE. 1,010 Australian households responded to the survey with quotes applied to ensure coverage across all age groups, genders and locations in each state and territory across metropolitan and regional areas. The data was weighted to ensure it is representative of the Australian population based on the 2021 ABS Census data. Fieldwork was conducted from the 12th of June to the 28th of June, 2024.

⁴ CHOICE Consumer Pulse June 2023 is based on a survey of 1,087 Australian households. Quotas were applied for representations in each age group as well as genders and location to ensure coverage in each state and territory across metropolitan and regional areas. Fieldwork was conducted from 7th to 22nd of June 27, 2023

⁵ <https://www.choice.com.au/shonky-awards/hall-of-shame/shonkys-2024/meta>

⁶ Ibid

⁷ <https://en-gb.facebook.com/business/help/719892839342050>

⁸ <https://blog.google/intl/en-au/australian-financial-services-advertisers-verification/>

were still online 7 days later. CHOICE identified the scam Decjuba ad was live for at least 58 days.⁹

While Google told us it removed over 5.2 billion ads from its platforms in 2022, that is a significant number of problematic ads that Google is being paid to publish in the first place. Clearly, there are fundamental shortcomings in Google's approach to publication if this many ads require removal.

Signs of action from the digital sector as a collective have also been concerningly poor. In July 2024, Digi, the industry association representing many major digital platforms, released the 'Australian Online Scams Code' (**Digi Scams Code**), a voluntary industry code that sets out a range of measures signatories will take to combat scams.¹⁰ The Digi Scams Code is weak and does not provide consumers with meaningful protections. Many of the commitments are described in vague terms, like 'move towards' having some kind of protection without clear timelines. Key protections (like verification of advertisers) are optional under the Code. Most importantly, there is no governance or enforcement mechanism for the Code so it is at best some vague aspirational statements. The Digi Scams Code is another clear sign that industry will not take adequate steps to stop scams unless it is forced to do so.

Regulators lack appropriate powers to address scam failures

In March 2022, the ACCC commenced enforcement action against Meta for false, misleading or deceptive conduct in relation to scam advertisements published on Facebook. Many users of Facebook are likely familiar with the advertisements in question, in which celebrities appeared to endorse get rich quick schemes, or investment in cryptocurrency.¹¹ While Meta did not create these advertisements, it received payment for their publication on its platforms.

Such advertisements have used the images of many different celebrities – to name just a few, scam investment ads in the last few years have included:

- Prime Minister Anthony Albanese,¹²
- Andrew 'Twiggy' Forrest. Dr Forrest also commenced litigation against Meta for this, which Meta has attempted to resist using every legal avenue available to it;¹³
- David Koch, who also took to social media to alert people it was a scam;¹⁴ and
- Robert Irwin.¹⁵

⁹ More information available at:

<https://www.choice.com.au/shopping/online-shopping/buying-online/articles/scam-ads-on-facebook-google-instagram>

¹⁰ <https://digi.org.au/scams/>, accessed 13 December 2024

¹¹ <https://www.accc.gov.au/media-release/accc-takes-action-over-alleged-misleading-conduct-by-meta-for-publishing-scam-celebrity-crypto-ads-on-facebook>, accessed 13 December 2024

¹² <https://www.theguardian.com/media/2023/jan/10/scam-facebook-ads-using-fake-images-of-pm-albanese-being-arrested-removed-from-site>, accessed 13 December 2024

¹³ <https://www.theguardian.com/technology/article/2024/jun/19/metas-bid-to-dismiss-case-brought-by-andrew-forrest-over-facebook-scam-ads-dismissed-by-us-court>, accessed 13 December 2024

¹⁴ <https://www.theguardian.com/australia-news/2023/apr/25/channel-7s-david-koch-is-angry-about-an-inter-net-death-rumour-scam-what-is-it-all-about>, accessed 13 December 2024

¹⁵ <https://www.choice.com.au/shonky-awards/hall-of-shame/shonkys-2024/meta>

Under existing laws, attributing liability to Meta for the scam advertisements is complex and the ACCC case is still a long way off determination, nearly three years after it commenced.¹⁶ In the meantime, similar advertisements again featuring the Prime Minister were reported to be doing the rounds on Facebook as recently as November 2024.¹⁷ This is despite the NASC also investing significantly in attempting to stop investment scams, which included efforts specifically directed at scams using fake celebrity endorsements.¹⁸ It is unacceptable that a trillion dollar tech company has not found a way to stop publishing scam ads of this type by now.

In December 2024, ASIC also sued HSBC bank for failing to adequately protect its customers from scams, failing to adequately respond to reports of unauthorised transactions and taking too long to reinstate banking services to customers after a report of an unauthorised transaction. While this enforcement action is welcome, like the ACCC/Meta litigation, this litigation will be complex and may be heavily disputed. ASIC is testing the boundaries of financial services laws - something it should do as a regulator - but which will likely also take years. It is also very telling that despite the many well documented failures of banks to prevent scams in recent years, this is the only case ASIC has felt has a sufficient prospect of success under current laws to take to court.

Regardless of the outcome of the ASIC/HSBC and the ACCC/Meta cases, it is clear our current legal framework does not require sufficient action to prevent, detect or disrupt scams by the businesses that enable scammers to cause consumers harm. The biggest tech companies in the world should not be getting paid to publish obvious scam advertisements on its website, and consumers cannot wait years to learn whether the courts think one particular instance of this occurring is unlawful.

There is a desperate need for stronger laws to force businesses to meet a minimum standard of protections, so that the level of protection consumers can expect does not depend on which bank or social media platform they use. Passing the Bill (along with strong industry specific codes) would be a major step toward a baseline in the legal framework that recognises the essential obligations of businesses to make their services safe from scams. The Bill needs to be passed in 2025, as a priority.

Recommendation 1

The Committee should recommend that the Bill be passed to ensure businesses enabling scams to happen are required to meet minimum requirements to prevent, detect, disrupt and appropriately respond to scams.

¹⁶

<https://www.thelawyer.com.au/practice-areas/tmt-telecoms-media-technology/federal-court-orders-against-meta-claim-in-a-consumer-law-case-against-meta/501183>, accessed 14 December 2024

¹⁷<https://www.smh.com.au/national/not-good-enough-meta-probe-flagged-as-fake-albanese-makes-facebook-comeback-20241120-p5ks9r.html>, accessed 13 December 2024

¹⁸ NASC and ACCC, Investment scam fusion cell, Final Report, May 2024, available at: www.accc.gov.au/system/files/NASC-Investment-scam-fusion-cell-final-report-2024.pdf

Prioritise expansion of SPF as a priority

Finally, we also urge the Committee to recommend that the Government commits to a timeline for prompt expansion of the application of the SPF, to also apply obligations on:

- Operators of online marketplaces (**Online Marketplaces**);
- Superannuation funds; and
- Cryptocurrency, or digital asset, platforms.

We understand that Online Marketplaces will not be caught within the intended scope of the digital platforms to be designated to fall under the Bill in the first instance. This should be rectified in the near future, as a priority. CHOICE asked a number of questions about Online Marketplaces in the same nationally representative research conducted by CHOICE in June 2024 mentioned above. Concerningly, 63% of respondents who used Facebook Marketplace a few times or more reported that they had seen what they suspected to be a scam on the platform.¹⁹ For respondents who used eBay or Gumtree a few times or more, the corresponding figures were 33% and 49%. While the proportion of people seeing suspected scam ads on Facebook Marketplace is particularly alarming, the figures for eBay and Gumtree suggest that scams on all online marketplaces are far too common.

Likewise, superannuation companies are another industry that should be subject to the obligations in the SPF very soon. There are trillions of dollars in superannuation that will represent a very attractive bounty to scammers, and there have already been signs of some scams involving super that suggest the industry is woefully unequipped to deal with scams.²⁰

The Government is in the process of establishing a regulatory framework for the crypto/digital asset sector. As it has been reported that half of proceeds from scams and fraud are processed through crypto platforms,²¹ it is obvious the SPF should also be expanded to apply to businesses operating in the crypto space - ideally as part of the introduction of crypto regulation.

Further delays in the initial rollout of the SPF to banks, telcos and digital platforms will only further delay its rollout to additional industries and sectors. The Bill needs to pass before the election. The Committee should give the Government a clear mandate to expand the scope of the SPF to further industries in the near future.

Recommendation 2

The Committee should recommend that the Government prioritises work to expand the SPF to include Online Marketplaces, superannuation firms and crypto platforms, and provides a timeline for their inclusion as soon as possible.

¹⁹ CHOICE Consumer Pulse June 2024, see above reference 3.

²⁰ See for example:

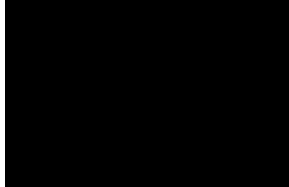
<https://www.abc.net.au/news/2024-06-27/superannuation-scam-hostplus-fraud-afca-court-cryptocurrency/103962762>, accessed 13 December 2024

²¹ <https://www.afr.com/companies/financial-services/crypto-platforms-a-getaway-for-half-of-scam-proceeds-20230810-p5dvhc>, accessed 13 December 2024

Further information

Thank you for considering our submission. To discuss this further, please contact Tom Abourizk, Head of Policy at CHOICE, at [REDACTED].

Yours sincerely,



Ashley de Silva
CEO
CHOICE