9 July 2024

Joint Select Committee on Social Media and Australian Society
PO Box 6100
Parliament House
Canberra ACT 2600

via email: socialmedia.joint@aph.gov.au

Dear Sir/Madam,

Protecting Australian small businesses and consumers from social media harms

The Australian Small Business and Family Enterprise Ombudsman (ASBFEO) appreciates the opportunity to make a submission to the Joint Select Committee on Social Media and Australian Society. The ASBFEO's submission aims to inform the Committee as to how social media scams can originate, the associated costs on small businesses, and policy steps that can be taken to prevent or mitigate their harms.

Social media can be a valuable tool for small businesses to attract new customers, advertise and sell products and services, and build brand loyalty. Despite these benefits, cybercrime involving social media accounts and inadequacies in how social media platforms deal with hacking disputes are causing significant harms to small businesses and other users. This is evidenced by the prevalence of social media-related concerns raised with the ASBFEO Assistance function. In the financial year 2023-24, more than 1 in 8 cases handled by the ASBFEO related to disputes with a social media platform.

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.[1]

This common occurrence results in significant harms to affected small businesses and the broader public. Affected small businesses suffer direct financial loss, sometimes amounting to tens of thousands of dollars, due to unauthorised payments for fake advertisements. Affected small businesses also suffer indirect harms including loss of income due to loss of a primary (and sometimes their only) sale channel, reputational damage (at times so enduring and significant that the business is forced to exit), and significant mental health costs to owners and staff.

These harms are consistent with those reported by the Australian Signals Directorate (the ASD) as affecting small businesses due to cybercrime more broadly. The ASD also reports that more than 60% of surveyed small businesses have encountered a cyber incident, and most cyber incidents

[1] See, for example, the difficulties that a Melbourne MMA gym business had in regaining access to its Facebook and Instagram accounts as reported by the ABC. Michael Aitkin, 'Hacked Facebook accounts leave businesses out of pocket as ombudsman records spike in Meta complaints', *ABC*, 23 April 2024, accessed 3 July 2024.

reported to the Australian Cyber Security Centre (ACSC) are from small businesses.[2] Among cyber incidents reported to ACSC by small businesses in 2022-23, the average loss to the business was $45,965.[3]

The broader public also suffers harms from fake advertisement scams. Members of the public who are scammed suffer direct financial losses, while other consumers and social media users are affected by a loss of small business diversity and reduced credibility of information received on social media. The ACCC found that social media scams resulted in $93.5 million in reported losses in 2023, second only in terms of financial loss to phone call scams.[4] Concerningly, the average financial loss per social media scam report was $5,330, which is significantly higher than the average financial loss per phone call, email, internet or text message scam report.[5] This highlights the greater vulnerability for Australian consumers and social media users to social media scams, which often leverage the reputation of longstanding local small businesses to attract victims.

Accordingly, the ASBFEO urges the Committee to not only consider the impacts of scams on Australian consumers and social media users, but to also address and look to disrupt how scammers operate. This necessitates a policy response to how social media platforms resource and manage their internal dispute resolution (IDR) processes, particularly for small businesses that have been hacked, as well as a focus on improving cyber awareness and cyber protections for Australian small businesses and consumers.

The ASBFEO has been active in delivering and advocating for solutions aimed at addressing these issues. In May 2024, the ASBFEO published a guide for small businesses using social media as their business platform.[6] The free guide covers tips to reduce the chances of being hacked and steps that can be taken to secure and recover a Facebook or Instagram account if it is has been hacked.

The ASBFEO also puts forward the following recommendations, which build on its submission made to the Senate Standing Committees on Economics in February 2023.[7]

Recommendation 1: Digital platforms should be required to improve and clearly outline their internal dispute resolution processes for small business.

It is crucial that clear, appropriate and standardised procedures are in place to facilitate timely resolution for small business disputes with digital platforms. Disputes between small businesses and digital platforms are typically difficult as digital platforms use automated complaint handling mechanisms, often with no human escalation point.

A typical small business dispute with a social media platform received by the ASBFEO is that of a small business owner being locked out of their Facebook account after their account has been hacked. The small business is unable to make a complaint through Meta's internal dispute process

[2] ASD, *Cyber Security and Australian Small Business*, ASD, Australian Government, November 2020, p. 11; ASD, *ASD Cyber Threat Report 2022-2023*, ASD, Australian Government, November 2023, p. 34.
[3] ASD, *Small Business Cyber Security*, Australian Cyber Security Centre website, n.d., accessed 21 March 2024.
[4] Australian Competition and Consumer Commission (ACCC), *Targeting Scams*, ACCC, Australian Government, April 2024, p. 14.
[5] ACCC, *Targeting Scams*, ACCC, Australian Government, April 2024, p. 14.
[6] Australian Small Business and Family Enterprise Ombudsman (ASBFEO), *Small business Ombudsman's guide to using social media securely* [media release], ASBFEO, Australian Government, 28 May 2024, accessed 3 July 2024.
[7] ASBFEO, *Inquiry into the influence of international digital platforms operated by Big Tech companies*, ASBFEO, Australian Government, 27 February 2023.

as they cannot gain access to their account to raise the dispute, as required by Meta. After unsuccessful correspondence with Meta and further research, the small business brings their dispute to the ASBFEO. The ASBFEO then makes use of its direct escalation points with Meta to help resolve the small business's dispute.

While the ASBFEO helps to resolve many small business disputes involving social media platforms, the above process is unsatisfactory for multiple reasons, including the following.

1. Although the ASBFEO advertises its assistance function broadly, not all small businesses are aware of the ASBFEO's ability to assist them to resolve disputes with social media platforms. This may mean that many small businesses that have been hacked are never able to resolve their dispute.
2. Even when the ASBFEO helps to resolve a dispute, delays stemming from the unnecessary complexity of the above process can result in harms to small businesses and consumers while the dispute remains unresolved.
3. The ASBFEO's role in helping to resolve disputes in this way results in use of public resources to subsidise deficiencies in how big tech social media platforms manage and resource their dispute resolution processes.

The ASBFEO therefore recommends that digital platforms be required to improve and clearly outline their IDR processes for small business. The requirement for adequate, timely and effective IDR processes should be supported by digital platforms promoting the ASBFEO as the external dispute resolution escalation point for small and family businesses where engagement with IDR processes has proven ineffective or unresponsive. Resourcing of this function should be canvassed with digital platforms, along with reporting mechanisms to regulators and policy makers to inform decisions about the adequacy of this intervention. This would help reduce delays to small businesses regaining access to hacked social media accounts, so that they can take down fake advertisements, recover control over their advertising payments, recommence operations, and rebuild their public trust and reputation.

This recommendation is consistent with 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'.[8] The ASBFEO notes that the Government has supported the ACCC's recommendation in principle and has called on the digital platform industry to develop voluntary internal dispute resolution standards by July 2024.[9]

The ASBFEO will be closely following these developments and urges the Committee to do the same, given the importance of timely and effective dispute resolution with digital platforms to disrupting scams and mitigating their harms to affected small businesses and the broader public.

[8] ACCC, *Digital platforms services inquiry: Interim report No. 5 – Regulatory reform*, ACCC, Australian Government, September 2022, p. 16.
[9] The Treasury, *Government Response to ACCC Digital Platform Services Inquiry*, The Treasury, Australian Government, pp. 2-3.

Recommendation 2: The ACCC's recommendation of a mandatory 'notice-and-action' mechanism should be implemented to protect small businesses and other users against scams, harmful apps and fake reviews.

While digital platforms enable small businesses to increase the reach of their sales and marketing activities, they can also facilitate fraudulent activities. A 'notice-and-action' mechanism that requires digital platforms to promptly act on reports of scams, harmful apps and fake reviews could provide small businesses with more timely and targeted protection than regulatory action.

Small businesses are vulnerable to fake review campaigns as they are often targeted and lack the means to address them directly. The ASBFEO has heard in consultation about certain small businesses being held to ransom over fake reviews, with scammers only removing them once they had received payment. The ASFBEO has also heard of markets for commissioning fake reviews to dishonestly facilitate new entry and distort competition.

Fake reviews not only impact small businesses that have been targeted with fake negative reviews or are competing with businesses backed by fake positive reviews, but also Australian consumers, whose purchasing decisions are impacted by them. One report found that 64% of consumers said they were likely to check Google reviews before visiting a business location, and another survey founded that 52% of respondents believe they had fallen for fake reviews.[10] As the ACCC states, this impedes participation in online commerce, with flow-on effects for the wider economy.[11]

The ASBFEO notes that the Government has supported the ACCC's recommendation in principle and has committed to considering whether disputes over fake reviews could be effectively managed through proposed dispute resolution processes. This reinforces the need to strengthen dispute resolution frameworks for small businesses and other users with digital platforms, for example by requiring platforms to improve and clearly outline their internal dispute resolution processes (Recommendation 1).

The ASBFEO is available to engage with the Committee further regarding social media risks and harms affecting small businesses. If you require any further information, please do not hesitate to contact the ASBFEO via email at advocacy@asbfeo.gov.au.

Yours sincerely,

The Hon Bruce Billson

Australian Small Business and Family Enterprise Ombudsman

[10] ReviewTrackers, *Online reviews statistics and trends: a 2022 report by ReviewTrackers*, ReviewTrackers 1 December 2021, accessed 3 July 2024; G Dixon, 'More than 50% of Australians Believe They've Fallen for Fake Reviews', Reviews.org, 13 August 2021, accessed 3 July 2024.
[11] ACCC, *Digital platforms services inquiry: Interim report No. 5 – Regulatory reform*, ACCC, Australian Government, September 2022, p. 77.