Australian Competition and Consumer Commission (ACCC)
23 Marcus Clarke Street
Canberra ACT 2601
Australia

9 September 2022

By email only: digitalmonitoring@accc.gov.au

Australian Payments Network (AusPayNet) thanks ACCC for the opportunity to respond to its sixth Issues Paper, '*Digital Platform Services Inquiry – March 2023: Report on Social Media*.' We support its policy objective of addressing significant consumer harms that can arise through the use and abuse of social media services, including through scams and advertising featuring misleading and deceptive claims.

In our submission, we suggest that ACCC should consider ways social media platforms can (a) stop scams at source and (b) collaborate with the wider scams lifecycle – including the payments industry – to prevent scams, including sharing intelligence for scam defences and detection and co-sponsoring end-user awareness campaigns. We believe placing obligations on social media platforms to prevent scams and to enable cross-sectorial collaboration will make Australia a hard target for scammers.

About AusPayNet - Membership and role

AusPayNet is the industry association and self-regulatory body for the Australian payments industry. We manage and develop procedures, policies and standards governing payments in Australia. Our purpose is to enable competition and innovation, promote efficiency, and control and manage risk in the Australian payments ecosystem. AusPayNet currently has over 150 members, including financial institutions, operators of Australia's payment systems, merchants, and financial technology companies.

Context: Scale of consumer harms through social media platforms and the need for collaboration

Released In July 2022, the ACCC *Targeting Scams* report estimated that Australians lost more than $2 billion to scams in 2021. The ACCC also rightly observed that, "the true cost of scams is far more than just financial – it leads to emotional stress and can have life changing consequences for many individuals, families, and businesses." [1] As an example, scammers were able to exploit social media features (e.g. followers and testimonial videos) as a veneer of legitimacy, to generate buzz and increase the popularity of a scam product. Using these sophisticated tactics, scammers groom victims not to heed effective warnings and even turn them into victimisers by spreading the word on their scam product, causing deep feelings of guilt and embarrassment.[2]

[1] ACCC, July 2022, 'Targeting Scams', *Report of the ACCC on Scams Activity 2021,* p 1 (link).

[2] Australian Broadcast Corporation Everyday, 3 May 2021, '*The Crypto Scam on Instagram that Cost Jonathan and his Friends $20k*', (link).

To avoid such financial and emotional harm, we need to make Australia a hard target for scams. To do so, will require:

- A focus on preventing scams, rather than compensating for them; and
- Collaboration between all the actors in the scams ecosystem.

While compensation can reduce financial harm, it cannot reduce emotional harm and further, does not serve as a deterrent to scammers. We therefore suggest that there needs to be a focus on prevention over compensation as a way of avoiding consumer harm before it happens.

In 2021, social media was the second highest contact method in terms of scam losses, after phone (voice).[3] Social media and digital platforms therefore need to play a key role in preventing scams.

In terms of collaboration, the scams lifecycle is complex, with many touchpoints at which scams can be prevented. The owners of these touchpoints – including consumers as the first link in the lifecycle, the digital platforms that support their activity, and banks and payment providers as the last link in the lifecycle – each play a role and should therefore collaborate to prevent and, as necessary, remedy scams.

As an example of such collaboration, it is increasingly important for payments providers to receive real-time intelligence from digital platforms for early scam detection and to raise effective warnings and responses.

Responses

The ACCC seeks views from anyone who participates or interacts with social media platforms, including consumers, small businesses and other organisations that maintain a presence on social media, advertisers, and the social media platforms themselves. Please include in your submission a description of your role(s) as a market participant.

Combatting economic crime is a top priority for AusPayNet, who are working closely with the wider banking and financial sectors, law enforcement and government to minimise the impact of scams. Our Members experience many cases where scammers groom their customers on social media platforms to bypass technical controls/warnings, financial institution intervention, or even law enforcement intervention. In most cases (e.g. in the case of investment and dating/romance scams), because the payer has been groomed, such a payment is being made to the payer’s intended payee. Since our industry sits at the end of the scam chain of events, our members are often unable to detect prior social grooming and are generally required to facilitate payments once they have received consent and instruction to process a payment.

[3] Ibid p 10.

Q20. Are businesses impacted by potentially misleading and/or deceptive claims through display advertising, including sponsored advertising or posts featuring influencers?

Scams affect corporates as well as consumers. They are obviously affected by specific scam types, such as business email compromise. However, they are also affected reputationally by misleading and deceptive claims, for example in investment scams, which erode consumer trust in investment. This is also true of the banking and payments sectors where consumer confidence in payments is diminished by both scams and any disruption of a payment necessary to halt suspected scam activity.

Financial institutions and payment services providers are also affected where they have:

- A lack of visibility of prior social engineering or grooming of victims on social media to enable scams detection and mitigation;
- Limited options for stopping the payment if a customer is determined to send money to a specific payee or the payment was duly “authorised” even though the victim’s cooperation was obtained under false pretences.

Stopping scams at source

For these reasons, social media platforms should monitor their platforms for the grooming of vulnerable individuals and advertisements with misleading and/or deceptive claims with the aim of stopping them. Ultimately, if it is proven that a social media/digital platform fails to reasonably manage the risks or take appropriate steps in their control, they should assist with remedying the consumer harm, akin to the ‘polluter pays’ principle in the UK.[4]

Q31. What is the process for consumers and business users to report potentially misleading and/or deceptive claims in advertising on social media, and what role do social media platforms play in these processes? How effective are these processes?

The lack of alignment and direct communication lines make reporting to social media platforms ineffective. There are different scam typologies being used across the reporting entities, with different scam categories being used by social media platforms, other industries and regulators. This complicates reporting for all concerned, creates misalignment across the digital ecosystem and increases the difficulty in attempting to consolidate data across all reporting sources. In addition, real-time communication and replies from social media platforms are, at best, ad hoc.

Data sharing and typology for swift scam detection

To facilitate clear communication, scam categorisation should be aligned, including with social media platforms. This will enable centralised scam data aggregation and reporting. Moreover, a more granular

[4] Finextra, 25 July 2022, Lloyds, Santander, Barclays, TSB demand Google, Facebook reimburse online fraud victims (link).

understanding of scam causes and types will help the anti-scams ecosystem devise better and more consistently applied strategies for preventing scams.

Real-time communication for scam preparedness and prevention

Intelligence sharing needs to be a critical part of preventing scams. There are opportunities to enhance and codify this sharing to ensure that all relevant industry participants have instant and equal access to critical information, enabling ecosystem-wide responses.

AusPayNet established the Economic Crime Forum (formerly the Fraud in Banking Forum) in June 2021 to ensure a more holistic approach to scams, fraud and cybercrime. This revised forum will enable collaboration among a wider set of participants in combating economic crime. We believe this Forum and the National Anti-Scam Centre[5] envisaged by the Albanese Government can and should be augmented with real-time insights from social media platforms.

Scam defence and response

There is no current ecosystem-wide understanding or codification of best practice scam defence and response capability (people, processes, technology). The burden to assist victims has fallen disproportionately on the local finance industry because of existing requirements for dispute resolution and in lieu of transparency and access to social media/digital platforms.

There are therefore opportunities to coordinate a national approach to provide better support to victims, potentially through the development of a national anti-scams code, mandatory for all actors in the scams lifecycle, to ensure a level of consistency for both customers and employees and avoid retraumatising victims.

Further Consideration

Sponsoring end-user awareness campaigns

Consumer awareness activity related to scams is being delivered in relative isolation by different companies/sectors, generating different messages to consumers and causing further confusion. Many of these awareness activities are also conducted sporadically and often only during Scams Awareness Week at the end of each year. Such lack of coordination and real-time warning make these activities ineffective.

Comparatively, UK industry bodies, through the 'Take Five' campaign, have developed centralised marketing toolkits and coordinated industry-wide messaging with succinct preventative steps outlined for the consumer.[6] This could be a model that Australia looks to replicate to drive more conversation about scams, and provide coordinated, ongoing guidance on what customers should look out for and do if they have been scammed. We believe social media platforms are a key partner in such awareness activity because of their reach to consumers.

[5] Australian Labor Party, 'Fighting Online Scams', *Policies,* (link).

[6] UK Finance, 2022, 'Take Five – To Stop Fraud, *Website,* (link).

Conclusion

Scam activity is growing across Australia and significant scam losses originate through social grooming on social media platforms. In summary, we suggest that social media platforms should ameliorate that through:

1. stopping scams at source as part of preventing consumer harms;
2. collaborating with the scam ecosystem by aligning scam categorisation and by sharing data and information;
3. being participants in any National Anti-Scams Code; and
4. contributing to joint customer awareness campaigns.

AusPayNet is grateful to the ACCC for the opportunity to provide its feedback and remains ready to assist the ACCC through its current work program, including through the facilitation of cross-industry discussions to mitigate scams. Please contact Mr Toby Evans, Head of Economic Crime, ([redacted]), or Ms Siew Lee Seow, Head of Policy, ([redacted]) if you have any further questions.

Yours sincerely,

[redacted]

Andy White
Chief Executive Officer
Australian Payments Network