7 April 2022

Digital Platform Services Inquiry
Australian Competition and Consumer Commission

Via email: digitalmonitoring@accc.gov.au

Dear Digital Platform Services Inquiry

Discussion Paper for Interim Report No. 5: Updating competition and consumer law for digital platform services

Thank you for the opportunity to respond to this Discussion Paper.

COBA is the industry association for Australia's customer owned banking institutions (mutual banks, credit unions and building societies).

Collectively, our sector has more than $150 billion in assets and more than 4.5 million customers. Customer owned banking institutions account for around two thirds of the total number of domestic Authorised Deposit-taking Institutions (ADIs) and deliver competition and market leading levels of customer satisfaction in the retail banking market.

General comments

COBA shares the ACCC's concern that digital platforms have enabled a significant growth in scams that are contributing to large financial losses for both consumers and businesses.

Our sector commits significant resourcing to identify, prevent and otherwise disrupt scam activity. COBA itself has a Fraud and Financial Crimes team who provide specialist advice to member financial institutions where a customer is, or is at risk of being, a victim of a scam. We also participate in law enforcement information sharing activities to ensure scams, where identified, are swiftly addressed.

Customer-owned banks work hard to prevent and detect financial losses to their membership that are identified as being as a result of a scam, and we support the need for a holistic approach to the scam lifecycle. In this way, COBA agrees with this Paper's proposals to increase the accountability of digital platforms for the role they play in providing the platform upon which these scams are promulgated. The following submission addresses questions 11-13 on the need for improved consumer protection pertaining to scams.

COBA would like to see a co-ordinated national approach to addressing scams activity. A taskforce comprised of regulators, financial institutions, payment providers, digital platform providers, law enforcement, utility providers and government representatives should work together to establish an Australian framework for scams reduction, similar in approach to the development of the Australian Cybersecurity Strategy. We need a national strategy that will measure and influence scam and cybercrime reduction. Greater accountability of digital platforms will be a key plank in creating an effective scams mitigation strategy.

Suite 403, Level 4, 151 Castlereagh Street,
Sydney NSW 2000

Suite 4C, 16 National Circuit,
Barton ACT 2600

Customerownedbanking.asn.au

Customer Owned Banking Association Limited ABN 98 137 780 897

Question 11: What additional measures are necessary or desirable to adequately protect consumers against: b) scams, harmful content, or malicious and exploitative apps?

- *Parties who facilitate the scam should be liable for redress for loss*

Platforms that facilitate connection between a scammer and their victim should be obliged to prevent their platform being used this way. They have a role in providing compensation in some instances for example where a lack of due care and skill is evidenced.

Consumers who suffer financial loss from a scam are routinely directed back to their financial institution to seek redress. Banks have clear, time-bound obligations to attempt to claw back money lost, however in most cases the money has already been removed from the receiving account, leaving no money to return to the victim.

In cases where the bank rejects the request for redress, the matter can be escalated the Australian Financial Complaints Authority (AFCA). AFCA then determines what is fair in all the circumstances having regard to legal principles, applicable industry codes or guidance, good industry practice, and past decisions.

COBA members find that AFCA complaints are occurring even when the bank has directly and repeatedly alerted the customer to the likelihood they are being scammed. This includes where the bank has explicitly advised them not to provide the funds requested. Despite a bank's direct attempt to disrupt the transaction, the degree of psychological manipulation the scammer has achieved can make it impossible to convince a victim they are being scammed.

A bank must respect the wishes of a customer moving their own money at their insistence, where there is no law against it. This is at the heart of a bank's contractual relationship with its customers. A bank cannot simply refuse to provide a customer with access to their money when the customer insists on completing the transaction. Banks are increasingly frustrated as they watch scammers defrauding their customers with impunity.

Ultimately it is consumers and their banks who are presently bearing the entire cost of scam losses where scammers flourish on digital media platforms with impunity. Parties who facilitate scams should be accountable for losses directly resulting from playing a role in hooking victims. Compulsory membership of an external dispute resolution scheme should be part of such a regime.

- *Dating Sites: Dating website customer verification is inadequate*

The use of fake profiles on online dating sites seems to be a frequently used method to lure a romance scam victim. The scammer is often successful because of the existing vulnerability of the target and the willingness of the victim to receive the proffered companionship. Mandatory verification of the identity of the user has a key role in preventing scammers. While the red flags of the scammer profile may appear obvious to someone outside the scam, to the victim they are easily justified by the scammer who is skilled at manipulation. It is reasonable for consumers to expect a service they use dedicated to companionship to be rooted in authenticity. While we note the existence of the ACCC's Best Practice Guidelines for dating websites, we question whether a voluntary approach has proven effective to date and further support the requirement for dating sites to have a reporting function enabling the timely removal of false profiles.

- *Online advertising: Verification of a business or product should be required as part of advertisement placement*

As is noted in the Discussion Paper, the value of reported losses from scams delivered online has increased significantly, with investment scams responsible for the largest consumer losses in Australia in 2021. The existence of public registers freely accessible to the investor to verify the lawful existence of an entity and/or Australian Financial Service Licence holder is insufficient as a reliable and complete prevention of investment scams. The provision of online real estate for the promulgation of a business

for which a fee has been charged should reasonably come with the assumption that a) the advertised services exist and b) they exist to the true extent that they have been advertised.

Case Study 1: Shipping Container Scam

Multiple COBA members based in regional NSW have reported customers losing money in shipping container scams. In these scams, shipping containers are promoted via search engines as being for sale; however after payment is made, no actual goods are received, and it is likely they never existed in the first place. One COBA member has 5 customers who each lost approximately $10,000 through the scam. The scammers used the name, ABN and business location details of a genuine NSW based towing business to create a ".com" website purporting to sell shipping containers. When the consumers sought to verify the business using these key details, they were led to believe the business was genuine. The genuine business owner reported the existence of the scam through the relevant search engines but some 6 months later, the scam website still appears at the top of the search results and it has been left up to the genuine business owner to use his genuine search engine business advertisement to advise of the scam.

Better verification of advertised products such as investments that use digital media platforms for promotion should be required to provide and have verified an Australian Financial Service Licence number, and Australian Business Number and other forms of identification prior to any paid promotion. As with the Romance Scam victim, members of the public who fall victim to cryptocurrency or binary trading (for example) investment scams are vulnerable in the sense that they lack the financial knowledge and understanding required to be able to perform appropriate due diligence. The onus can only fall onto the digital platform to confirm the products they are being paid to promote to consumers is genuine.

Finally, products using the image of an easily identifiable celebrity to endorse or advertise a product should be fact checked prior to acceptance of a paid promotion.

Case Study 2: Cryptocurrency Investment Scam

A COBA member has reported a customer losing more than $130,000 through the fake purchase of cryptocurrency in an investment scam advertised on a popular social media site that used the identity and photograph of a high-profile Australian to falsely endorse the scam. The initial small value transaction by the customer was detected by the COBA member's Financial Crimes Team and the customer was contacted to inquire about the validity of the transaction. Having been primed by the scam broker through multiple long phone conversations, the customer assured the member's Financial Crimes Team that the transaction was genuine, and all due diligence had been appropriately completed. The customer continued to make payments to the Digital Currency Exchange, each time assuring the Member of the deliberate intention of the transaction, each of which was authorised by the customer using 2 factor authentication. Some 2 weeks later, the customer became uneasy when he was unable to access his digital wallet and then contact the scam investment broker. Upon interview with the bank, the customer advised he was initially wary of the scam broker but reconciled these feelings with the use of the high-profile public figure as the scheme endorsement on a highly public digital platform.

Question 12. Which digital platforms should any new consumer protection measures apply to?

Consumer protection measures as are the subject of the Discussion Paper should be applied to all publicly available digital platforms including social media, search engines, dating and social connection sites and online marketplaces where goods and/or services on offer exceed a specified value threshold.

Question 13. Should digital platforms that operate app marketplaces be subject to additional obligations regarding the monitoring of their app marketplaces for malicious or exploitative apps? If so, what types of additional obligations?

COBA acknowledges the existing levels of app marketplace monitoring with respect to identifying and blocking malicious or exploitative apps. However, we remain concerned about loopholes whereby

malicious content is able to be spread through version upgrades to an existing app after it has been cleared for download to the consumer's device. COBA supports increased obligations for app marketplaces to ensure scrutiny over such apps for the entirety of their usability.

Concluding comments

Banks undertake a range of activities to detect and prevent scams and fraudulent payments. We need much more effort being made to disrupt the pipeline that sees scammers getting to customers, and better apportioning of redress for customer losses to scammers.

I hope this submission assists. Please do not hesitate to contact Emma Lawson [redacted] or Sarah Wilson [redacted] if COBA can be of any further assistance.

Yours sincerely

[redacted]

MICHAEL LAWRENCE
Chief Executive Officer