25 October 2024

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security

Via email: pjcis@aph.gov.au

Dear Committee Secretary

Cyber Security Legislative Package 2024

COBA thanks the Committee for the opportunity to provide feedback on the Cyber Security Legislative Package 2024.

COBA represents Australia's customer owned banks (mutual banks and credit unions). Collectively, our sector has over $170 billion in assets, around 10 per cent of the household deposit market and around five million customers. Customer owned banking institutions account for around two-thirds of the total number of domestic Authorised Deposit-taking Institutions (ADIs).

COBA members range in size from approximately $15 million in total assets for our smallest member to around $25 billion in total assets for our largest member. While our member banks are currently not subject to the *Security of Critical Infrastructure Act 2018* obligations, they are still subject to extensive regulation and supervision on cyber security as APRA-regulated entities.

Key points

COBA supports the legislative package as representative of the proposals made to support the Australian Cyber Security Strategy 2023-2030.

COBA supports ransomware reporting for businesses but believes that the measures as proposed are duplicative of measures already addressed under APRA's CPS 234 Information Security and will add to the regulatory burden on our members.

COBA has consistently supported sensible measures to protect Australia's critical infrastructure and systems. We are supportive of the Australian Cyber Security Strategy 2023-2030 and believe that the measures proposed in this legislative package are representative of the measures proposed in the Strategy.

Our sector recognises that the functioning of Australia's banking system is dependent on a secure cyber environment. As such, our members dedicate significant resources towards maintaining and developing defences against these threats and to ensure compliance with existing cyber security obligations. Many of the changes in this legislative package have been long called for by our sector and we congratulate the Government for its delivery of this package.

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

Ransomware reporting for businesses

Duplicative reporting

While COBA has consistently supported the adoption of the ransomware reporting measures, we believe that the proposed measures are duplicative of obligations that already exist for banks under APRA's CPS 234: Information Security. If the ransomware measures are proceeded with, they will compel our members to report similar information to APRA, the Australian Signals Directorate (ASD) and to the Australian Cyber Security Centre (ACSC).

This reporting to multiple agencies will add complexity and regulatory burdens for our members with little gained by the Government, as any information reported to any one of these agencies should easily be shared among themselves rather than requiring our members make multiple reports. We suggest that APRA could be considered to be made a designated Commonwealth body under this Act with any relevant information reported to APRA under CPS 234 capable of being shared with ASD and ACSC.

In considering this regulatory reporting burden on our members, we draw the Committee's attention to changes in reporting on similar kinds of information that is being proposed in the Government's Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024 and its Scams Prevention Framework. The issue of burdensome and duplicative reporting obligations is a key issue of our sector and has been highlighted as an area of concern that will be considered by the Council of Financial Regulators in its upcoming review of the challenges facing small and medium sized banks.

We ask that the Committee consider this impact and seek to minimise duplicative and overlapping reporting from all these regimes.

Turnover threshold

If the Committee chooses to proceed with endorsing these duplicative reporting obligations, then we ask that the Committee considers mitigating its impact by recommending a higher turnover threshold. While we understand that the Government is seeking to align the threshold with the notifiable data breach scheme under the *Privacy Act 1988*, we believe that the $3 million annual turnover threshold to be very low. We also do not necessarily think that ransomware reporting is necessarily analogous to privacy breaches to use this as a benchmark.

We understand that this threshold will be prescribed in the rules and will be subject to further consultation in due course. We welcome the opportunity to work with the Government on determining a more appropriate threshold that does not cause undue regulatory burden on smaller Australian banks.

We thank the Committee for taking our views into account. Please do not hesitate to contact [redacted] if you have any questions about our submission.

Yours sincerely

[redacted]

MICHAEL LAWRENCE
Chief Executive Officer