16 May 2019

Ms Heidi Richards
General Manager, Policy Development
Policy and Advice Division
Australian Prudential Regulation Authority

Email: PolicyDevelopment@apra.gov.au

Dear Ms Richards

Draft Prudential Practice Guide CPG 234 Information Security

The Customer Owned Banking Association (COBA) welcomes the opportunity to comment on APRA's Draft Prudential Practice Guide CPG 234 Information Security (CPG 234). We appreciated the opportunity to discuss with APRA its Draft CPG 234 and implementation at COBA in Sydney last month.

COBA is the industry association for Australia's customer owned banking institutions (mutual banks, credit unions and building societies). Collectively, our sector has $118 billion in assets, 10 per cent of the household deposits market and 4 million customers.

COBA supports APRA's new prudential standard CPS 234 Information Security (CPS 234). COBA recognises that CPS 234 responds to the rapidly evolving nature of information security threats and that Australian financial services companies are being targeted with growing frequency and sophistication.

Given the complexity of this reform and the need to ensure that industry's implementation of CPS 234 is aligned with APRA's policy intent, COBA appreciates that APRA is consulting on the Draft CPG 234.

However, with the CPS 234 commencement date of 1 July 2019 fast approaching, COBA is concerned that the late consultation on the Draft CPG 234 may have a material impact on industry implementation.

It appears that APRA intended to consult on the Draft CPG 234 at an earlier stage, noting that APRA's 7 November 2018 Response to Submissions stated that APRA "will **shortly** be undertaking consultation on an updated cross-industry prudential practice guide on information security" (emphasis added).

COBA acknowledges that there have been a number of significant regulatory developments since November last year which have also required APRA's close attention, such as the Financial Services Royal Commission. However, the absence of the final CPG 234 at this very late stage of the transition process makes implementation of the new CPS 234 more challenging.

APRA's final CPG 234 is not only important from an entity-level implementation perspective, but also from an industry sector consistency perspective. Consistent interpretation of the CPS 234 requirements across the sector is likely to benefit APRA's future CPS 234 supervisory and/or audit activities.

COBA would like to emphasise that transitioning from the current, but outdated, CPG 234 to the new CPS 234 is not a simple process, particularly as we are shifting from high-level set of cross-industry guidance to a new law, the latter of which imposes a number of significant new requirements.

In this respect, the final CPG 234 is required for interpretation and to assist in directing resources and mitigate against the risk of inadvertently proceeding down a misinterpreted/incorrect path, which could be very costly to unwind.

As smaller ADIs, our members' resources for implementation are more limited compared to the larger banks, and therefore need to be more carefully managed.

As COBA emphasised in our 6 June 2018 submission to APRA on the Draft CPS 234, a significant number of our members rely heavily on third-party service providers for their core banking system and information technology service requirements.

In this respect, it is important that our members are provided regulatory certainty through the final CPG 234, so that they are able to engage and negotiate confidently with their third-party service providers on implementing CPS 234.

As APRA is aware, our membership has invested a significant amount of resources and time towards implementation with very good progress being made to date. However, the absence of the final CPG 234 at this late stage, coupled with the subjective nature of parts of CPS 234, heightens the risk that industry implementation at 1 July 2019 may not fully align with APRA's underlying policy intent.

Timing concerns aside, COBA broadly supports APRA's Draft CPG 234. We particularly welcome the level of detail that APRA has provided in the Draft CPG 234, given the subjective nature of CPS 234.

With that being said, we note that APRA has incorporated into the Draft CPG 234 a number of terms that we suggest should be clarified (such as "threat intelligence", "reconnaissance", "weaponisation", "fuzzing" and "timely manner"). Clarity around such terms would reduce ambiguity and help, for example, our members work confidently with their third-party service providers on the transition.

Building on our comments about third-party service providers, COBA emphasises that the customer owned banking sector continues to take its principal agent relationship seriously with respect to third-party technology vendors. The due diligence associated with selecting, monitoring and reviewing technology vendors as agents will continue to evolve positively with the commencement of CPS 234.

However, there is a risk that some vendors may not be fully up to speed with how CPS 234 may shape their products and services. To help minimise this risk, COBA suggests that APRA issue guidance directly to vendors to help support, for example, our sector's efforts in reaching out to vendors to work on the transition. For example, APRA could establish a central APRA contact that vendors can contact to discuss transition arrangements.

Finally, COBA welcomes the attachments to the Draft CPG 234 covering areas where APRA has determined that more detailed guidance is warranted. COBA notes the inclusion of Attachment F: Customer security, which includes APRA's suggested preventative, detective and response controls to address different types of customer security risks.

While COBA welcomes the inclusion of Attachment F, we note that in ADIs fraud risk is typically managed separately to information security risk. For regulatory certainty, as customer fraud risk does not appear to be explicitly captured in CPS 234, we would appreciate clarity from APRA in the final CPG 234 on how those risks fall within scope of CPS 234 and APRA's minimum expectations of entities.

COBA looks forward to continuing to work with APRA to finalise the Draft CPG 234 to help facilitate a smooth and efficient transition to the new CPS 234 environment.

If you have any questions or comments in relation to any aspect of our submission, please do not hesitate to contact Tommy Kiang, Senior Policy Manager, on [redacted].

Yours sincerely

[redacted]

MICHAEL LAWRENCE
Chief Executive Officer