CUSTOMER OWNED BANKING ASSOCIATION

1 November 2019

Cyber Security Policy Division
Department of Home Affairs
4 National Circuit
BARTON ACT 2600

Lodgement via: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020/submission-form

Dear Sir/Madam

Australia's 2020 Cyber Security Strategy

The Customer Owned Banking Association (COBA) appreciates the opportunity to provide a submission on the development of Australia's 2020 Cyber Security Strategy.

COBA is the industry association for Australia's customer owned banking institutions (mutual banks, credit unions and building societies). Collectively, our sector has $121 billion in assets, 10 per cent of the household deposits market and 4 million customers. Our members provide a unique point of difference in the retail banking market through their customer-owned rather than investor owned model. Our members range in asset size from around $200 million to $15 billion.

As the functioning of modern banking is dependent on a secure cyber environment our members understand the evolving nature of cybercrime and dedicate considerable resources towards maintaining and developing defences. We recognise and understand the important role Government can take towards building increased Cyber resilience with all Australians.

We support the adoption of a strategic approach that is built on partnerships with financial services sector that works to educate Australians on changing risks and provides defences that are both practical and proactive. The customer owned banking sector strongly supports the theme that cyber security is a shared risk between government and the entire community of all Australians.

In consultations with our member organisations we identified eight specific questions of the 26 sought for feedback and provide collective responses as follows:

Q.6 What customer protections should apply to the security of cyber goods and services?

Our member banks identified a strong need for consumer products to have inbuilt malware and intrusion detection within the operating system or when connected to the internet. In an increasingly connected world from computers to whitegoods and children's toys, end point compromises make consumer products inherently vulnerable. We believe that proactive security measures such as built in cyclical updates could provide Australians with practical protections recognising that not every user understands the importance of updating in response to system vulnerabilities.

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

Member feedback identified consumer protections could be strengthened by identifying products with proactive security inbuilt to operating systems for rebates or tax incentives. It was further suggested that product suitability especially for various vulnerable groups be linked to stronger purchase protection under legislation potentially through future amendments to consumer protection laws.

Q.7 What role can Government and industry play in supporting the cyber security of consumers?

Our sector strongly supports the role of government leadership in the area of cybersecurity recognising a shared intelligence need. COBA and its members value and are committed to strengthening our strategic partnerships with law enforcement and Australian Cyber Security Response Centres in each state.

We note that specific technical expertise from financial services providers is needed in conjunction with law enforcement to ensure vulnerabilities are recognised, triaged and treated to minimise impact on trusted infrastructure. In respect of this we believe that joint staffing programs and dedicated co located resources would assist develop shared capabilities and understanding.

There is a specific and urgent need to develop policy initiatives that provide for cybersecurity awareness for older Australians. Dedicated programs such as e-Safety, Stay Smart Online and ScamWatch have all contributed to raising awareness. However, there is a growing need for more accessible and centrally maintained safe computing channels for older and vulnerable Australians. An example of this might be specific hubs where older Australians can safely utilise government digital services to build confidence, co located with government services or partners.

COBA members have overwhelmingly acknowledged the strong need for education and awareness commencing in primary school with continuing targeted education for seniors. We recognise that as younger Australians prepare for employment social media presents opportunities but also barriers for those with disabilities and vulnerable persons. Programs could be run in conjunction with existing services and linked to government education initiatives.

Members believe that regional and remote locations need to be a priority for cyber awareness particularly small business. There is an opportunity to formalise partnerships with government to deliver the targeted cyber security awareness programs that many of our members have in place across Australia. Customer owned banking institutions have been delivering education to their customers through these programs since the early 2000s partnering with COBA, local law enforcement and Australian Federal Police.

Q.10 Is the regulatory environment for cyber security appropriate? Why or why not?

Direct feedback from a vast majority of COBA members has been that there are urgent regulatory changes needed to protect ordinary Australians. Specifically, changes need to address the jurisdictional problem of scammers operating globally and out of reach of enforcement agencies. Members have told us that they believe the damage to onshore brands including government infrastructure such as NBN needs specific regulation and strong penalties.

The problem of scammers operating offshore targeting Australians is having a detrimental effect on trusted networks and adds significantly to the social and human cost of fraud. Building on initial work underway by some Telco's to block millions of scam calls reaching Australians daily, we believe domestic Telco's and Internet Service Providers can play a more active role in prevention through identification of fraudulently used services regularly used to mimic or replicate domestic numbers to make calls seem more authentic.

There is an opportunity for Government to provide direct funding to support victims of Cybercrime such as Identity theft and scams. As an industry we recognise and value the role played by non-profit organisations such as IDCare. The growing numbers of victims adds significantly to the cost of

providing counselling for victims. We believe Government funding is urgently needed for these organisations dealing with victims of Government issued identity fraud ATO, Centrelink and identity and travel documentation. Government co-funding would assist to lower costs for all industry sponsors many for whom the formal costs of participation may be prohibitive.

Q.11 What specific market incentives or regulatory changes should Government consider?

With scam losses passing half a billion dollars in 2019 there is an urgent need for law enforcement resources to target international cybercriminals victimising Australians through joint operations with offshore law enforcement. Prosecution of those engaged in cybercrime needs strong penalties to provide deterrence measures.

Q.12 What needs to be done so that cyber security is 'built in' to digital goods and services?

COBA has been advocating on behalf of its members with industry groups to mandate stronger identification before a mobile phone is ported to another carrier. Specifically, we have been advocating for the introduction of active consent to porting by the mobile device operator before a port takes place. We congratulate the Government on recent actions to strengthen identity measures to prevent misuse of identity information that enables the fraudulent porting of mobile phone numbers.

COBA members have told us they believe that the creation and deployment of specialised application software programs (apps) for financial or personal information collection should pass a higher level of stringency in security testing. Moreover, the adoption of stronger authentication of one-time passwords and utilisation of cryptographic hash functions would assist to render valueless the interception of data.

Q.16 How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

Further to Q6, on this topic, members have told us they believe that malware detection and updates to devices need to be in built to applications with proactive updating rather than relying on consumers to activate. The provision of Internet Service Provider "safe routes and hubs" for elderly and vulnerable customers is suggested. These could be products, services or a combination of both by suppliers. Providing consumers with a clear and simple security software that can be easily explained and understood we believe would encourage use and adoption.

Q.19 What private networks should be considered critical systems that need stronger cyber defences?

Our members believe inclusion should extend to all financial institutions, utilities, Telco's, medical providers, superannuation funds and third-party providers to these sectors. Members have told us that all these sectors are considered critical to the functioning of our society and need highest levels of protection. In addition, the protection against cyber-attacks needs to be a functional enterprise operation to maintain trust. Certification and accreditation of third-party providers to these sectors would assist in helping to establish defences.

Q.22 To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

Member feedback has been that consumers are driven by price rather than safety especially when e-safety is not a prerequisite for either government service or banking. In some cases, consumer protections can have opposite effect by fuelling scams and malware distribution. Not all organisations have capital to invest in front end detection of these devices when shopping or performing other services making them inherently riskier to deliver products and services to consumers. Members believe that there is opportunity for incentives to be considered for those social media platforms and websites that work to block identified scams and help raise awareness with the public.

We thank you for allowing us the to present our members' views on this very important, nationally significant issue and look forward to the finalisation of the strategy. If you wish to discuss any of the issues raised in this submission, please contact Leanne Vale (Director - Services and Financial Crimes) on [redacted]

Yours sincerely,

MICHAEL LAWRENCE
Chief Executive Officer