The Hon Tony Burke MP
Minister for Home Affairs
Minister for Cyber Security
Department of Home Affairs
6 Chan Street
Belconnen ACT 2617

28 August 2025

By webform: homeaffairs.gov.au

By email: CSSH2@homeaffairs.gov.au

Dear Minister Burke,

DEVELOPING HORIZON 2 OF THE 2023-2030 AUSTRALIAN CYBER SECURITY STRATEGY

The Mortgage and Finance Association of Australia (**MFAA**) welcomes the opportunity to make a submission to support the progress of Australia's cyber security strategy (**Strategy**). Over 97% of businesses in Australia are small businesses.[1] Therefore core to the success of the Strategy will be strengthening the cyber resilience of Australia's small business sector.

The MFAA is Australia's peak body for the mortgage and finance broking industry with over 16,000 members.

Mortgage and finance brokers are an essential part of Australia's financial ecosystem, supporting over 37,000 jobs and contributing $4.1 billion to the Australian economy each year.[2] Over time, consumers have increasingly sought the services of a mortgage and finance broker with the latest MFAA quarterly market share showing mortgage brokers facilitated 76.8% of all new residential home loans[3] and approximately four out of ten small business loans[4] in Australia.

[1] ASBFEO, Small business data hub, 97.2% of all Australian businesses were small businesses in June 2024. The Australian Bureau of Statistics defines small businesses as those with less than 20 employees.

[2] Deloitte, *The value of mortgage and finance broking 2025*, <https://www.mfaa.com.au/policy-and-advocacy/research>.

[3] MFAA media release, *Mortgage broker market share reaches new peak*, <https://www.mfaa.com.au/news/mortgage-broker-market-share-reaches-new-peak>, 2 June 2025.

[4] Productivity Commission, *Small business access to finance: The evolving lending market Research paper*, September 2021, <https://www.pc.gov.au/research/completed/business-finance/business-finance.pdf>, pg 44.

OUR SUBMISSION

Cyber security is a central priority for the MFAA in the way we support our members, the vast majority of which are small businesses.[5]

Mortgage and finance brokers play a critical role in intermediated lending, providing access to credit and promoting choice and competition in both consumer and business finance. Brokers hold a position of deep trust, managing some of the most sensitive financial and personal information their clients share such as identification documents, tax file numbers and details about income and financial assets. The high value of property transactions and a broker's responsibility to collect and store large volumes of data, creates a unique cyber risk exposure that often intersects with scams. Where manual processes are used across parts of property lending and settlement, the threat is amplified.

Brokers are a prime target and vulnerable to cyber risk – incidents of email compromise scams, phishing attacks, credential theft and supply-chain attacks are rising. When a cyber-attack occurs, it has a significant impact on business continuity as well as client harm, reporting obligations and reputational damage for the small business.

Brokers are also predominantly small and medium-sized (**SME**) businesses without the skills, expertise or resources of large businesses to navigate cyber threats. This means that uplifting cyber resilience for the SME sector must be prioritised and resourced in a way that's simple, practical and affordable, reflecting the sector's limited capacity to manage increasingly complex cyber risks alone.

To that end, we make the following recommendations:

1. Strengthen technology enablers critical to secure data transfer and security
2. Ensure regulatory settings support small businesses to uplift cyber resilience
3. Collaborate with industry bodies to deliver resources that lift awareness and develop capability

RECOMMENDATION 1: STRENGTHEN TECHNOLOGY ENABLERS CRITICAL TO SECURE DATA TRANSFER AND SECURITY

Brokers handle highly sensitive financial and personal information on behalf of their clients and maintaining secure data-sharing practices is essential to protecting both consumers and small businesses. Digital solutions, including the use of artificial intelligence (**AI**) tools, are becoming increasingly vital to a broker's business operation – helping to automate tasks and increase efficiency so that they can spend more time helping their clients. However, current practices such as screen-scraping (digital data capture) expose clients and brokers to unnecessary risk and are not sustainable in the long term.[6]

---

[5] Of the MFAA's membership, 97% are mortgage and finance brokers. Sole operators make up 42% of the mortgage broking population according to the MFAA Industry Intelligence Service Report, 19th Edition, <https://www.mfaa.com.au/policy-and-advocacy/research>.

[6] Assistant Treasurer Stephen Jones' speech to CEDA, *Putting consumers first in the Consumer Data Right*, 9 August 2024, <https://www.ceda.com.au/newsandresources/news/technology-innovation/assistant-treasurer-stephen-jones-speech-to-ceda>.

The rollout of the Consumer Data Right (**CDR**), alongside interoperable Digital ID solutions, offers a more secure and trusted framework for sharing and verifying data. CDR and Digital ID are critical as they provide brokers with secure, trusted tools to transact client information. Importantly, CDR reduces reliance on insecure methods like screen-scraping, and Digital ID on current verification of identification (**VOI**) processes that often rely on manual checks at time of mortgage settlement.

These reforms will enhance consumer protection, reduce fraud and cyber risk, and improve efficiency across the lending process. Importantly, they will also enable small businesses in the broking sector to participate confidently in a digital economy, ensuring their clients benefit from innovation without compromising privacy or security.

RECOMMENDATION 2: ENSURE REGULATORY SETTINGS SUPPORT SMALL BUSINESSES TO UPLIFT CYBER RESILIENCE

Small businesses recognise the importance of cyber resilience but are often time-poor and lack the knowledge, skills, or resources to implement effective safeguards. For many, the pace at which cyber threats evolve is likely to outstrip their capacity to respond.

Regulatory frameworks must be designed with proportionality and practicality in mind, ensuring they support rather than unduly burden small businesses.

For example, under the Cyber Security Act 2024 and associated rules, from 30 May 2025 businesses with an annual turnover of $3 million or more are required to report any ransomware or cyber-extortion payment, whether monetary or non-monetary, to the Australian Signals Directorate within 72 hours.[7] This threshold was deliberately designed to minimise the compliance burden on small businesses. We welcome the decision to exempt them from onerous reporting requirements and encourage government to maintain a policy approach that supports and incentivises small businesses in strengthening their cybersecurity, rather than penalising them.

Similarly, the Scam Prevention Framework is principles-based, allowing the Federal Government to designate additional sectors as scam activity evolves.[8] While this flexibility is sensible, care must be taken to ensure that obligations imposed on designated sectors do not spill over, either directly or indirectly, to non-designated participants such as small businesses. If obligations are poorly scoped, there is a risk that non-designated businesses may feel compelled to adopt compliance measures designed for larger entities, despite not having the resources or risk profile to do so.

A deeper consideration is the balance between resilience and regulatory burden. Small businesses are often at the frontline of cybercrime and scams because of their reliance on digital tools, their handling of sensitive financial information, and their relatively limited cybersecurity budgets. Yet, unlike large institutions, they do not have compliance teams or in-house expertise to absorb heavy regulatory requirements. Imposing formal obligations without tailored support risks discouraging innovation, raising costs, and diverting resources away from core business activities. Conversely, if regulation is too light-touch, small businesses may be left vulnerable and underprepared for the consequences of cyber incidents.

---

[7] Cyber Security (Ransomware Payment Reporting) Rules 2025 apply to businesses with annual turnover over $3 million.

[8] MFAA Submission to Senate Standing Committees on Economics, 19 December 2024, <https://www.mfaa.com.au/policy-and-advocacy/submissions>.

The answer lies in proportional design. This means reserving the heaviest compliance obligations for sectors and businesses with the greatest capacity and systemic impact, while ensuring small businesses are not ignored. Governments and regulators should prioritise practical measures such as guidance, templates, awareness campaigns, and voluntary reporting channels that build confidence and capability without disproportionate burden. Doing so ensures that regulation enhances resilience across the economy, without creating unintended compliance creep or widening the gap between large and small entities.

RECOMMENDATION 3: COLLABORATE WITH INDUSTRY BODIES TO DELIVER RESOURCES THAT LIFT AWARENESS AND DEVELOP CAPABILITY

The range of initiatives delivered under the Strategy's Horizon 1 demonstrates meaningful progress but also highlights the need for sustained awareness programs that specifically target small businesses. Tools and resources such as the Essential Eight (cyber.gov.au), the Cyber Wardens program and the Small Business Resilience Centre complement each other, and all contribute to uplifting SME cyber resilience. Greater reach and success depend on clear, consistent, and accessible messaging.

Industry bodies are well placed to raise awareness and deliver practical resources to their members. For example, in September 2024 the MFAA partnered with the Council of Small Business Organisations of Australia (**COSBOA**) to deliver Cyber Wardens training to our members.[9] We are embedding this training into our education and professional development programs, reinforcing that developing cyber resilience is a continual process. Alongside this, the MFAA has released a dedicated resource, What to do if you've been scammed, which provides brokers and their clients with clear, step-by-step guidance on responding to scams and practical advice on how to mitigate cyber risks before they occur.[10] Supporting associations like ours to expand these initiatives ensures that small businesses receive advice that is relevant, accessible and trusted.

CLOSING REMARKS

[redacted]

Yours sincerely,

[redacted]

Mortgage and Finance Association of Australia

[9] MFAA News, *Don't let your personal devices be a backdoor into your business,* 30 September 2024, <https://www.mfaa.com.au/news/don-t-let-your-personal-devices-be-a-backdoor-into-your-business>.

[10] MFAA Media Release, *Protecting brokers and customers: MFAA launches practical scam resource,* 25 August 2025, <https://www.mfaa.com.au/news/protecting-brokers-and-customers-mfaa-launches-practical-scam-resource>.