Ross McEwan
Group CEO
Level 12, 395 Bourke Street
Melbourne, VIC 3000, Australia
Telephone: +61 3 7038 1838

7 November 2022

Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra
ACT 2600

Dear Committee Chair

National Australia Bank (NAB) welcomes the opportunity to provide a short submission on the introduction of legislation to increase the penalties for serious data breaches, namely the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022* (the Bill). As a member of the Australian Banking Association (ABA) and Business Council of Australia (BCA), NAB has also contributed to their submissions.

NAB has actively engaged with Government on both privacy law reform and cyber security. We have also made considerable investments to boost our capacity to tackle fraud, cyber crime and related threats, which have only become more critical as the global and national threat landscape has worsened. We are absolutely committed to detecting and preventing criminal behaviour, especially when customer data may be impacted and believe it is of utmost importance for the corporate industry to be a constructive ally to Government in strengthening resilience against cyber threats.

NAB is cognisant that Australian communities need to trust that their information will be protected and not misused. This will help to drive sustainable long-term value and economic benefit for Australia. Part of earning and maintaining this trust is ensuring that we have a robust privacy framework that balances safe data use and innovation, with strong protections.

In light of the above, NAB requests that the Parliament give further consideration to the intention of the Bill. Whilst there is a role for penalties to incentivise data holders to invest in their cyber security and protect customer data, we believe the increase in penalties – and particularly the calculation for determining penalty that relates to adjusted annual turnover- are disproportionate and create a much greater maximum penalty than similar privacy and data protection laws across the globe. As drafted, these provisions may cause significant negative impacts on privacy and information security within Australia. Excessive penalties and uncertain penalty provisions are likely to act as a deterrent for some companies who may be less willing to promptly disclose data breaches to Government for fear of facing potentially terminal penalties. Further, penalties of this magnitude, without appropriate containment measures, will have the capacity to effectively put an organisation out of business. It can also appear to punish companies who are increasingly the victim to an upsurge in malicious and sophisticated hacks. To illustrate the cyber threat environment companies are currently operating in, NAB detects and fights up to 50 million cyber hack attempts per month. We see an opportunity here to incentivise

Government and business to work together on tackling this global threat, with punitive measures reserved for egregious failures of compliance and risk management.

The Bill outlines three measures of calculation to determine the maximum penalty for serious or repeated privacy breaches. NAB's main concern lies with the penalty provision of 30 per cent of a company's adjusted turnover in the 'relevant period'. This proposed civil penalty is significantly higher than the strictest regimes in other jurisdictions, such as the European Union's General Data Protection Regulations (GDPR), which caps penalties at 4% of global turnover. For context, a data breach from a major Australian company subject to the maximum penalty in the Bill could be in the region of four times the largest civil penalty order ever made against an Australian corporate. Whilst we acknowledge that elements of the existing penalty regime may be inadequate in disincentivising poor behaviour, we believe that the maximum penalty proposed is excessive and should be reviewed in line with global standards.

We therefore strongly urge consideration of a range of other measures designed to mitigate the risks to individuals that arise as a result of cyber crime, in addition to an enhanced but appropriately measured penalty regime. This includes asking the Government to review its requirements on businesses to retain certain data. For example, under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006,* reporting entities such as banks are required to keep customer identification records for seven years after the banking relationship has concluded. This mandated retention period is much longer than we would otherwise require and significantly increases our risk profile. We would also like to see greater public/private sector collaboration to combat cyber threats and an increased investment in cyber skills training and assistance both for individuals and businesses.

We understand that a 'serious breach' will be determined by a number of factors including the recklessness of the company. We support a raft of measured considerations for the courts when assessing liability and potential penalty, including the nature and extent of the breach, compliance with relevant privacy and data security laws and standards, and the extent of any negligence of the company that contributed to the severity of the event. However this does not wholly ameliorate our concerns as to the magnitude of the proposed penalties.

Recent events have also substantiated the call for greater data minimisation, particularly for smaller companies that are required to hold significant personal information to confirm customer identity or other data points. Such information could instead be guaranteed, with zero knowledge proof, by another trusted institution, e.g. through the trusted digital identity framework (TDIF). Digital identity is a critical enabler for safe commerce and communications, and a range of public and private solutions are emerging for important use cases. The public and private sectors each have crucial roles to play, bringing together modernised versions of government credentials with customer choice in authentication services. NAB advocates for the Government to recommence discussion around the TDIF legislation, prioritising interoperability between public and private solutions to promote the data minimisation agenda.

NAB welcomes the opportunity to continue working constructively with the Government in its fight against cyber crime and the timely reconsideration of Australian privacy law.

Yours sincerely

Ross McEwan