THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: PDL:JBml160125

16 January 2025

Policy Manager, Policy and Legislation, Identity
NSW Department of Customer Service
2-24 Rawson Place
SYDNEY, NSW 2000

Dear Policy Manager,

DRAFT PERSONAL INFORMATION (IDENTITY PROTECTION AND RECOVERY) BILL 2025 (NSW)

Thank you for the opportunity to provide feedback on the draft Personal Information (Identity Protection and Recovery) Bill 2025 (NSW) (**Bill**). The Law Society's Privacy and Data Law Committee contributed to this submission.

We understand from the Guidance document that the Bill aims to provide the necessary legislative authority to ID Support (**IDS**), a business unit established in 2021 within the Department of Customer Service (**DCS**), to effectively support individuals, agencies and private entities that might be impacted by a personal data compromise. However, we are concerned that as currently drafted, the Bill does not achieve all its aims, nor does it appropriately balance the interests of potential fraud check customers with the privacy rights and interests of those individuals impacted by a personal data compromise.

Compromised ID register

Under Division 2 of Part 3 of the Bill, the Secretary must maintain the compromised ID register (**Register**). The Secretary has discretionary power to record an identity document in the Register, 'if the Secretary is of the opinion that it [the ID] has, or may have, been compromised' (clause 17(a)).

As currently drafted, the Bill requires the Secretary to take 'reasonable steps to notify an individual whose identity document is recorded on the compromised ID register' (clause 17(2)). However, there is no requirement for an individual to consent to their identity document being recorded. It is also unclear what type of information will be recorded, e.g. whether it will be the individual's name and the type of identity document, or whether other personal information such as address, or licence or passport number would also appear on the Register. The Bill should clearly set out what information from the identity document would be recorded and, in our view, should also include a requirement for an individual's consent to be obtained for the level and type of information the Secretary wishes to record on the Register.

The Bill requires that a request by the affected individual to remove that individual's information from the Register must be for a purpose prescribed by the regulations (clause 18(1)(b)). It is not clear what the approved purposes might be, and we suggest that any such requirements should not be onerous, and should

THE LAW SOCIETY OF NEW SOUTH WALES
170 Phillip Street, Sydney NSW 2000
ACN 000 000 699 ABN 98 696 304 966
lawsociety.com.au

T +61 2 9926 0333 F +61 2 9231 5809
E lawsociety@lawsociety.com.au

Law Council
OF AUSTRALIA
CONSTITUENT BODY

be consistent with the Information Protection Principles under the *Privacy and Personal Information Protection Act 1998* (NSW).

Disclosure

One of the mandatory requirements that determines if the Secretary can disclose information about whether an identity document is recorded on the Register to a fraud check customer, includes the following sub-clause 24(1)(b):

> *the Secretary is reasonably satisfied that the individual whose identity document, or purported identity document, is the subject of the disclosure has consented to the disclosure,*

We suggest that the Bill needs to clarify *how* consent is to be obtained from individuals to satisfy sub-clause 24(1)(b). It could be a requirement, for example, that consent from affected individuals for disclosure to fraud check customers is sought when notifying the individual under clause 17(2) about the initial data compromise. The mechanism for consent should be user-friendly and meaningful, and set out what information a fraud check customer can access, the limited purposes for use, and the privacy implications and risks.

Fraud check customers

The Guidance document indicates a fraud check customer may be 'any public sector agency or a private sector entity' but there is no further detail about the requirements when applying to be a fraud check customer, apart from the requirement for the Secretary to approve the application. We note that clause 23(4) provides that the criteria will be prescribed by the regulations. We suggest that the criteria must incorporate procedural safeguards, in addition to ensuring the 'stringent privacy and security requirements' referred to in the Guidance document, but which are not set out in the Bill.

As previously stated, we consider that an individual must be able to give informed consent before their information is disclosed to fraud check customers. Currently, there is no requirement in the Bill for fraud check customers to only use the information they have obtained from the Register for limited and relevant purposes. This is concerning, especially in the context of family violence or financial abuse. We suggest that the Bill should require fraud check customers to only use the information disclosed for the purposes for which disclosure was made, consistent with the NSW Information Protection Principles (IPPs)[1] (see, for example, IPP 10) and Australian Privacy Principles[2] (APP 6).

As a technical drafting matter, it appears there is a typographical error in the definition of 'fraud check customer' in clause 22, where the reference to 'an approval under section 22' should read 'an approval under section 23'.

[1] *Privacy and Personal Information Protection Act 1998* (NSW) pt 2 div 1.
[2] *Privacy Act 1988* (Cth) sch 1.

Exemption from privacy laws

We are also concerned with the proposed exemption from privacy laws that allows a partner authority or public sector agency to collect, hold, use, or disclose personal information for the purpose of exercising an IDS provider function or related service under clause 28. This clause, together with clause 30, granting exclusion of liability for disclosures otherwise prohibited, removes important privacy protections such as the IPPs, specifically IPP 11:

> *Only disclose personal information with a person's consent or if the person was told at the time that it would be disclosed, if disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the person would object, or the person has been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.*

In our view, the extent to which privacy laws are excluded under clause 27 is unclear. If a public sector agency may disclose personal information to the Secretary for the purpose of exercising an IDS provider function, do the requirements for security of data (IPP 5) or transparency (IPP 6) also not apply? We query how personal information can be protected under the Bill without this clarification, and why there is not a requirement for a public sector agency to first notify the affected individuals that their personal information may be disclosed to the Secretary for the purpose of IDS functions. Our query also extends to private entities regulated under the Commonwealth APPs.

We suggest that the Bill should clearly incorporate the IPPs, where appropriate, as these are necessary safeguards for protecting personal information against misuse, and clarify the extent of the exemption from privacy laws.

Reporting requirements

We suggest that there should be a requirement for the IDS to periodically report on how many individuals with compromised IDs are recorded in the Register in that period.

Additionally, there does not appear to be a requirement to publish a list of fraud check customers. An individual whose identity document is recorded on the Register would not know which entity (i.e. which fraud check customer) will have access to the information. That is, in future dealings with any government agency or private sector entity, the individual will not know whether the entity has information about any identity compromise relating to the individual. We suggest this could be remedied by requiring the regular publication of a list of fraud check customers.

Issue of new ID credentials

We note that one of the objects in clause 6 (a)(ii) of the Bill is to 'facilitate the remedying of compromised ID information of individuals'. However, it is not obvious how individuals who are victims of ID compromise will benefit from the Register, without incorporating further options for remedying the compromise. We suggest consideration be given to how affected individuals may be promptly issued with new valid ID credentials that will facilitate their engagements with public sector agencies and private sector entities, preferably through a

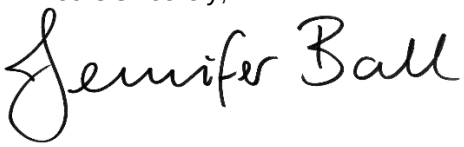
fast-tracked process, ensuring that the onus is not solely on the affected individual to re-apply for new ID credentials. Once the new ID credentials are issued, the individual's previously compromised ID information should be automatically removed from the Register, and public sector agencies and private sector entities should be required to recognise the newly issued credentials without unreasonable delay.

Statutory review

Given the important implications of the Bill for the safeguarding of personal information, we suggest there should be provision for a statutory review every two years from commencement.

If you have any queries about the items above, or would like further information, please contact Mimi Lee, Policy Lawyer, on 02 9926 0174 or mimi.lee@lawsociety.com.au.

Yours sincerely,



Jennifer Ball
President