Executive summary

The Financial System Inquiry has been thorough in uncovering issues impeding the Australian economy; Veda, a data analytics company best known as Australia's leading provider of consumer credit reports and an innovator of fraud, identity and credit risk solutions offers the following policy response.

Consumer credit reporting

Australia's new Privacy Act – including comprehensive credit reporting - started in March 2014. While most significant lenders have given customers notice of the collection of additional data, provision to credit reporting bodies is just starting. The most valuable element, repayment history, is particularly complex, and accuracy is paramount. As such, Veda expects significant volumes will not be provided until 2015.

The FSI highlights aspects of the Australian arrangements that are inconsistent with international trends, such as the data elements not allowed to be collected (eg outstanding balance) and broader access to the credit reporting information, such as non-credit licence holders. In addition, the Inquiry raises the question of whether or not Australia should mandate contribution of the new data elements.

We believe the best approach is to be consistent with the Inquiry's recommendation for an assessment of the impact of the new Privacy Act in 2016. This review should include consideration of the new credit reporting arrangements. Such a review would not be the wholesale review done by the ALRC but should examine, with the assistance and rigour of Treasury, if the reform's goals of greater financial inclusion and better credit risk practices are being met.

Practically, given the timeframe for provision of data, the credit reporting review should be scheduled for late 2016/early 2017.

Two issues with significant consumer benefit should be given immediate priority:

- Long-standing Government policy issues relating to reuniting lost members superannuation and unclaimed monies will be helped by use of discrete credit reporting information (name/DOB/address) to reunite consumers with their money. Authorised use, based on a privacy impact assessment, should be a priority for Government.

- There is long-standing support for exchange of credit reporting data with New Zealand. Enabling free exchange of credit reporting information between Australia and New Zealand is a basic economic reform with broad support on both sides of the Tasman – it simply needs prioritisation by Governments.

Small-and-medium-enterprise lending

Australia has a competitive market for the provision of commercial credit risk assessments and the proposal for a Government–initiated new financial database would be disruptive and unnecessary. Commercial credit information is protected by the Australian Privacy Principles and access to new information should not bring increases in regulatory-burden. Government can make the lending process easier for SME businesses by enabling them to access and disclose, online and in real time, key information needed when applying for credit.

Better use of Government information

Government data contribution to research and innovation, be it scientific or commercial, is a national economic resource. Its availability, subject to the Australian Privacy Principles, should be dramatically expanded with Government agencies shifting to presume in favour of automatic release of datasets.

We note the Productivity Commission's statement that:

> "*Unlike many other countries, Australia makes relatively little use of its public data resources even though the initial costs of making data available would be low relative to the future flow of benefits…a rich vein of information is held by governments in the form of 'administrative data' collected for regulatory requirements (e.g. vehicle registrations and taxation declarations), program administration (e.g. Centrelink and Medicare payments, school, university and vocational enrolments and completions, and hospital admissions) or as a by-product of transactions (e.g. fines and fees*)"[1]

Veda recommends Australia follow the example of the United Kingdom, with the establishment of a single source of access to Government datasets and reporting requirements for agencies on progress with data release. Negotiations with the States and Territories should start on ensuring a uniform approach to provision of datasets, through the single Commonwealth site.

Finally, we note a scoping study is soon underway into ASIC registry. As a general Government policy, responsibility for improving existing data products and services, and the creation of new data products should be contracted to the private, via licenced access. In addition, Government policy should assume any new proposed registries are to be privately-run.

Identity

While Government can foster innovation in verification techniques and set standards for identity checking resilience, Government policy should not restrict identity validation to a single provider, or a single method. Verification based solely on Government-issued identity or Government controlled processes is not a desirable practice, both from a resilience and privacy point of view. While the use of

[1] "Using administrative data" chapter one, Productivity Commission annual report 2012-2013

MyGov as a portal to services is a decision for the Commonwealth, wider imposition for identity carries the risk of an "Australia Card by keyboard".

Veda believes any policy framework should be technologically neutral and recognise that Australia's identity and fraud roadmap should be a public/private partnership, allowing for innovation of identity practice and recognising that multiple independent data sources create a much more resilient process.

With the on-line economy demanding more efficient identity checking, any organisation that has a reasonable requirement to verify identity must have equal access to identity resources, such as the Commonwealth's Document Verification Service (DVS). Given the DVS does not actually disclose any information, access to the DVS should not involve unreasonable regulatory burden or cost, reflecting the existing standards used for other Government sources such as the PPSR.

Finally we note access to state birth and marriages information is particularly convoluted, via a different, slower process to the DVS (Certvalid). There is an urgent need to modernise the disparate holdings of each state and bring them into a uniformly accessible fashion for use in the DVS.

Privacy breaches

Carelessness, accidents and malicious attacks mean that regardless of the very best efforts, data breaches will happen. From Wikileaks to botnets, uncovering information is no longer the province of lone hackers.

In Australia, the rapid uptake of the on-line economy is matched with increasing anxiety over on-line security. A 2013 Veda survey showed that while around 37 per cent of respondents were concerned with personal security within their home, 68 per cent were concerned about putting their personal details on-line.

Respondents have justification to be anxious, with high profile data breaches by well-resourced organisations including Ebay (145 million records - 2013) and Sony playstation (24 million records, including some bank details - 2010). Government agencies have suffered significant incidents, with the State of Texas in 2010 accidentally publishing 3.5 million names, including DOB, Drivers licence and address.

Data breaches will happen; the question is how do the organisations impacted respond?

Currently, Australia has no mandatory data breach reporting requirements, despite the ALRC in 2008 recommended data breach notification encompassing both notice to the OPC and the individual where "there is a real risk of serious harm to any affected individual" .

Nearly seven years after the ALRC first recommended data breach obligations and with one failed attempt at legislation, there needs to be a remedy for individuals suffering a breach of their data.