Chapter 3

Non-government entities' restriction on accessing register information

3.1 A key concern of many submitters with the exposure draft bills and the draft regulations is the restriction on non-government entities, such as credit checking organisations, from verifying information on the proposed National Business Names Register. Currently, third party credit providers are able to verify the identity and business details of customers seeking access to credit and financial services with the information on state and territory business register databases.

3.2 Verifying this information is a requirement of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act). The Australian Bankers' Association (ABA), AMEX, the Australian Retail Credit Association (ARCA), Veda Advantage and the Australian Finance Conference (AFC) have all expressed concern that the bill and regulations as currently drafted will not enable their members to verify information on the national register. They may therefore be in breach of the AML/CTF provisions.

3.3 The government has noted that the bill's restriction on allowing non-government entities to access personal information on the National Business Names Register is in accordance with the Information Privacy Principles. Under these principles, the Commonwealth must use information for the purpose for which it is being collected. As the data has not been collected for the purpose of private organisations verifying their data, it cannot be obtained by these organisations.

3.4 This chapter examines these issues. It is divided into the following sections:

- the relevant clauses of the main bill and draft regulations;
- entities' obligations under the AML/FTC Act;
- the current capacity of credit checking organisations to verify their data from state and territory business registers;
- the argument of credit checking organisations that draft regulation 9 will affect their capacity to comply with the AML/CTF;
- clause 77 of the bill and the difficulties in matching data; and
- the *Privacy Act* and Information Privacy Principles.

Relevant clauses and regulations

3.5 This section outlines the provisions that restrict non-government entities from accessing personal information on the national register: clauses 60 and 62 of the Business Names Registration Bill 2011 and draft regulation 9 of the proposed Business Names Registration Regulations 2011. These provisions are interrelated: a change to one of these provisions, as suggested by some submitters, may change the other two provisions.

3.6 Clause 60 of the main bill states:

Access to certain information in the Business Names Register by request

(1) A person may lodge an application with ASIC for a copy of:

(a) the entry in the Business Names Register relating to a particular business name; or

(b) the entries in the Business Names Register relating to a particular entity.

(2) The application:

(a) must be in the prescribed form; and

(b) must be lodged in the prescribed manner; and

(c) must be accompanied by the application fee.

(3) If a person lodges an application under subsection (1), ASIC must give the person a copy of the entry or entries sought.

(4) However, before a copy of an entry is given to a person, ASIC must excise from it:

(a) any detail which under the regulations made under subsection (5) is to be excised; and

(b) any detail that ASIC is prohibited from disclosing under subsection (6).

(5) The regulations may provide that details of a kind specified in the regulations are to be excised from a copy of an entry before it is given to any person, or any person of a prescribed class.

(6) If:

(a) a person lodges with ASIC an application for a detail in relation to a business name or the person not to be disclosed; and

(b) ASIC is satisfied that it is not appropriate to disclose the detail;

ASIC must not disclose the detail under this section.

(7) An application mentioned in paragraph (6)(a):

(a) must be in the prescribed form; and

(b) must be lodged in the prescribed manner.

3.7 Draft regulation 9 of the proposed Business Names Registration Regulations 2011 states:

> **Accessing Register by request**
>
> For subsection 60(5) of the Act, the following details are to be excised from a copy of an entry in the Register before it is given to any person:
>
> (a) the date and place of birth of:
>
> (i) an entity that is an individual; or
>
> (ii) any other person if those details were provided in accordance with subsection 23 (6) of the Act;
>
> (b) any alternative contact details provided by an entity;
>
> (c) if a home address is provided as the principal place of business in Australia of an entity that is an individual — all of the address other than the suburb and the State or Territory in which the entity lives;
>
> (d) if the entry identifies a notified successor that ASIC believes is not itself an entity — the details for the notified successor mentioned in paragraphs 8 (c), (d) and (e).

3.8 Clause 62 of the main bill distinguishes between government and security agencies and private third-party organisations by providing exemptions for government bodies that are not available to private entities. It provides that ASIC must make available certain information 'of a kind prescribed by the regulations' to:

- a government body if the body has requested ASIC to make the information available for purposes of the enforcement of the criminal law, the enforcement of a law imposing a criminal penalty or the protection of public revenue (among other purposes); and
- an intelligence or security agency, if the agency has requested ASIC to provide the information for the purposes of the exercise of the agency's functions.

3.9 The submitters listed in paragraph 3.2 collectively claim that these clauses, and in particular regulation 9, prohibit the use of ASIC's database for the purposes of identity verification. This restriction limits their ability to comply with the AML/CTF Act.

Entities' obligations under the AML/CTF Act

3.10 As its title suggests, the AML/CTF Act was twin objectives. The first is to address the problem of money laundering in Australia, which is estimated to have a

value of approximately $11.5 billion per year.[1] The second objective is to mitigate the threat to national security posed by the financing of terrorism.

3.11 The AML/CTF Act, which is regulated by the Australian Transaction Reports and Analysis Centre (AUSTRAC), implements Australia's international obligations to align Australian legislation with the Financial Action Taskforce on Money Laundering (FATF).

3.12 Under the AML/CTF Act, businesses have strict identification, reporting and record keeping obligations. Section 4 of the Act requires reporting entities to verify a customer's identity before (or in special cases after) providing a designated service. As part of these requirements, credit and finance providers must be able to verify the following information:

- the name of the person (other person) who is proposed to be registered as a remittance affiliate of the applicant; and
- the business name(s) under which the other person is carrying on a business, or proposes to carry on a business, of providing a registrable designated remittance service;
- a description of whether the other person is operating as an individual, company, partnership, trust or through any other legal structure;
- if the other person is a subsidiary of another entity, the name and address of that entity;
- if applicable, the address of the registered office of the other person;
- the full street address at which the other person provides or proposes to provide registrable designated remittance services, including the full street address of each branch of the person;
- if the other person has an ACN, ABN or ARBN – that number;
- the other person's telephone number, facsimile number and email address at its principal place of business;
- the full name and address (not being a post box address) of:
    - if the other person is an individual—that individual; or
    - if the other person comprises a partnership—each partner and, where relevant, the beneficial owner(s) of those partners;
    - if the other person is a company—the beneficial owner(s) of the company;

1 Explanatory Memorandum, *Anti-Money Laundering and Counter-Terrorism Financing Bill 2006*, p. 3.

- if the other person is a trust—the individual who has effective control of the business.[2]

3.13 AUSTRAC states in its Explanatory Note on requirements that in respect to the authorised individual and each of the key personnel, the following details need to be verified:

- full name;
- date of birth;
- position or title;
- business telephone number;
- facsimile number;
- business email address; and
- full address (not being a post box address).[3]

3.14 In its submission to this inquiry, AUSTRAC elaborates on entities' obligations under the AML/CTF Act:

> The AML/CTF Act embodies five key areas that are internationally recognised as best practice in deterring and detecting money laundering and terrorism financing (ML/TF). Broadly speaking, reporting entities are required to:
>
> - conduct ML/TF risk assessments. Businesses must understand and manage the ML/TF risks they are exposed to when they provide different products and services, use different distribution channels, deal with different customers and operate in different jurisdictions.
> - implement systems and governance to manage their ML/TF risks. Businesses must establish appropriate oversight of ML/TF risk by senior management, ensure there is an employee due diligence program and that staff are trained to detect ML/TF behaviour and regularly review the effectiveness of their systems and compliance with their obligations.
> - know their customers. Businesses must verify the identity of their customers, monitor their customers' behaviour and keep appropriate

---

2 These requirements are listed in AUSTRAC's Explanatory Note for the draft rules prescribing matters required or permitted under the AML/CTF Act, available at: http://www.AUSTRAC.gov.au/files/draft_rules_spec_regist_app_info.pdf (accessed 25 July 2011).

3 AUSTRAC's Explanatory Note http://www.AUSTRAC.gov.au/files/draft_rules_spec_regist_app_info.pdf (accessed 25 July 2011)

records of these actions. Financial institutions must also appropriately identify any other financial institutions with which they do business.

- make themselves known to AUSTRAC. Most reporting entities must advise AUSTRAC that they have obligations under the AML/CTF Act, either through submission of a compliance report (CR) under section 47 or, if they are a remittance service provider, by registering under Part 6 of the AML/CTF Act. Under recently enacted cost recovery arrangements, all reporting entities will be required to enrol with AUSTRAC in 201 1/12.
- report to AUSTRAC. Businesses must provide reports to AUSTRAC on cash transactions above a $10,000 threshold, instructions for international funds transactions and suspicious matters. Most must also report regularly on their own compliance with their obligations under the AML/CTF Act through a CR.As part of a reporting entity's AML/CTF program, it must both identify and verify a customer before providing a designated service. This identification and verification process is referred to in the AML/CTF legislation framework as the "applicable customer identification procedure" (ACIP).[4]

3.15 According to the ARCA, Veda Advantage, AMEX, the AFC and the ABA, most of these identifiers will not be available on the new National Business Names Register, and these details will be excised from the business extracts issued by ASIC.[5]

The current capacity of credit checking organisations to verify their data from state and territory business registers

3.16 To evaluate the merit of these submitters' claims, the committee sought to ascertain what personal details information brokers can currently verify from the state and territory business registers. If it is not possible for these organisations to verify data currently from state business registers, how are they able to comply with the AML/CTF Act?

3.17 Currently, there are two main methods for verifying information. The first method allows a credit or financial service provider to apply to the state and territory business registers for an extract which lists the personal and business information of a particular business.

3.18 The second method allows third-party credit and financial service providers to use a match/no match system. Crucially, this system ensures that no personal information is disclosed by the states and territories. Credit providers submit

4 AUSTRAC, *Submission 9*, p. 2.

5 See clause 60 of the main bill and draft regulation 9 of the proposed Business Names Registration Regulations 2011.

information received from the credit applicants to the relevant bodies. They then check the information provided and notify the credit provider whether there is a match or no match on their database.

3.19 The detail of information credit and financial service providers have access to may vary from state to state and other sources are used to cross-check and/or complete missing bits of information. In an answer to a question on notice, Veda Advantage informed the committee that:

> ...where a satisfactory match cannot be achieved, the information is not included. At present, the various state based registers provide a wide breadth of information which can potentially be used to enable matching; for instance, except for the Northern Territory, all jurisdictions can provide current address.
>
> Additionally, other data listed can potentially be used to provide matching capability eg address of other businesses is available except for Queensland and the Northern Territory. This will not be the case under the new Register, which will hold just seven data fields.
>
> Veda notes that these other data fields can be of assistance to matching, particularly when used in conjunction with information held on other databases. These other databases include public records, such as court defaults judgements, bankruptcies and ASIC extracts, as well as commercial inquiries for credit and default listings collected by commercial credit reporting agencies.
>
> Together, these data sources are used to create a trading history report, containing information on the business, its proprietors and the business relationships of the proprietors.[6]

3.20 On sourcing and verifying data, the ABA notes that:

> The aim of verification is to independently confirm relevant information that has been collected from the customer. Where members are unable to verify collected data via a State or Territory register, alternative methods of verification are sought, such as collecting and retaining on file passport or driver license details where there is a need to verify personal details, or a full company (ASIC) search from a subscriber service such as Veda.
>
> Members would prefer that the verification of customer details be obtained from the one source of truth rather than having to refer to multiple sources of data.[7]

3.21 In relation to providing a service that is consistent with current practices, DIISR informed the committee that this is not the intent of the database and it will not

---

6 Veda Advantage, answer to questions on notice, 4 August 2011 (received 8 August 2011).

7 Australian Bankers' Association, answer to questions on notice, 3 August 2011 (received 9 August 2011).

provide business information that third-party credit and financial service providers have historically used. In an answer to a question on notice, the Department of Innovation, Industry, Science and Research (DIISR) informed the committee that:

> The Branch advised that it could not support making such information available under the provisions of the current Bills because the Privacy Act 1988 requires agencies to only collect personal information that is for a lawful purpose directly related to a function of activity of the collector and, in their view, the Bills do not provide for personal information to be collected for information broker purposes.
>
> It should be noted that Clause 4.3 (b) of the Intergovernmental Agreement which underpins the national law that the Bills establish outlines the purpose of the law, namely the registration and use of business names. The purpose of the national law does not include provision of data for authentication and verification purposes (for example through "match/no match" functionality).[8]

3.22 Veda took issue with the Department's position not to allow private bodies access to information on the national register. It noted that:

> ...this appears to conflict with the Intergovernmental agreement for business names agreement, which provided for "an extract service for brokers on commercial terms agreed with individual brokers" [5.1(g)] and that the purposes of the national BNR included "the parties agree that the levels of service provided by the Commonwealth's national business names registration scheme will not be less than the levels of service currently provided in the State/Territory systems [1.1 (2)].[9]

3.23 Moreover, DIISR told the committee that 'only three states collect date of birth; the other five do not'. The Department later clarified that all states and territories collect date of birth information, but only three give out the date of birth of adults: these states are Queensland, New South Wales and South Australia.[10] Only Queensland verifies date of birth data. In this context, DIISR asked:

> ...I suppose the question is whether this sort of information should be used when it is currently not checked and will not be in the future either—apart from in Queensland.[11]

---

8 DIISR, answer to question on notice, 4 August 2011 (received 8 August 2011).

9 Veda Advantage, *Letter to committee*, 8 August 2011, p. 3.

10 Ms Ann Bray, Acting Head, Industry and Small Business Policy Division, *Clarification of Hansard record*, 5 August 2011.

11 Ms Ann Bray, Acting Head, Industry and Small Business Policy Division, *Proof Committee Hansard*, 2 August 2011, p. 3.

3.24 Upon further investigation, the committee has found that all states and territories collect residential address data in their business registers. The committee remains unclear which states and territories verify this data.

3.25 Veda Advantage provided Table 3.1[12] to the committee to demonstrate the large variety of information to which they currently have access. They compare this information to that which will be available under the proposed National Business Names Register. Veda is concerned that a reduction in available information would make it difficult to verify the identity of individuals behind businesses for the purposes of credit and finance checks, as required under the AML/CTF Act and its associated KYC requirements.[13]

3.26 DIISR has contested Veda's claims that the business registers are a primary source of information for information brokers. In an answer to a question on notice, the Department challenged the claim that they even use the state and territory registries to verify information:

> DIISR also notes that one of the private entities seeking the additional data (in particular, date of birth and home address) is Veda Advantage, and draws to the attention of the Committee that Veda's privacy policy (included on the Veda Advantage web site) does not include state/territory business names registers as a source of personal information.[14]

3.27 However, the committee notes that DIISR only quoted an extract of Veda's privacy policy. On the same webpage quoted by DIISR, Veda states that it collects information from publicly available sources.

3.28 Further, Veda Advantage has informed the committee that the website quoted by DIISR is dedicated to the Consumer Credit Bureau Section of Veda and does not relate to their Commercial Branch. Veda states that in relation to their commercial practices, they have individual commercial arrangements with states and territories that provide access to the various business names registries.[15] In their Trading History Product Guide, Veda stipulates that in providing business trading history reports, Veda refers to business names extracts and the credit reports of each proprietor.[16]

3.29 Veda also objected to a statement made by DIISR in relation to the use of personal information by information brokers. In an answer to a question on notice,

---

12 See Appendix 3.

13 Veda Advantage, *Submission 5*, pp 2–3.

14 DIISR, answer to questions on notice, 4 August 2011 (8 August 2011).

15 Veda Advantage, answer to question on notice, 9 August 2011 (9 August 2011).

16 Veda Advantage, *Trading History Product Guide*, p 6.

Veda dispute the claim made by DIISR that '[o]nce data is provided to private bodies there is no control over what they might do with it'. It responded:

> This statement is not correct. Not only are there the obligations of the National Privacy Principles, but in addition, contractual terms and conditions can be imposed by agencies for private bodies seeking access.[17]

The problem with draft regulation 9

3.30 The AFC, AMEX and the ABA each submitted that the provisions in draft regulation 9—which excises residential addresses and date of birth from business extracts—will make it very difficult to fulfil their obligations under the *AML/CTF Act*. The AFC was direct in its criticism of the proposed arrangements:

> We have recently been made aware that the draft Regulations for the Business Names Register make using it to verify the identity of the proprietor behind the business name more difficult. This is a bizarre outcome when taken in the context of the Government's AML/CTF laws which place considerable responsibilities, backed up by severe penalties, on financial institutions to verify the identity of their clients.
>
> We understand that contrary to the pre-existing ability to verify the details of the business proprietor (e.g. date of birth, address) via the state registers, the draft Regulations propose only to have the national register confirm the proprietor's name. This is hardly an improvement to the seamless national economy! Moreover it would mean that if a director applies to open an account with a financial institution in the company name, it would be able to verify against an ASIC register the name, address, date and place of birth details that had been provided for the account, but if the application is made by a proprietor in the business name, the ASIC register will only be able to confirm the proprietor's name. This anomalous result falls well short of the financial institution's legal requirement for customer verification and due diligence.

3.31 The AFC correctly presumed that the policy intent behind the regulation lay with the purpose imperative of the Privacy Principles. However, it argued that in present circumstances, this position is 'confused' and 'contrary to the Government's AML/CTF policy purpose'.[18]

3.32 AMEX highlighted the Know Your Customer (KYC) requirements of the AML/CTF Act and 'associated Rules and Regulations'.[19] It emphasised that these AML/CTF obligations:

---

17 Veda Advantage, answer to questions on notice, 8 August 2011.

18 Australian Finance Conference, *Submission 4*, pp 1–2.

19 AMEX, *Submission 7*, p. 2.

> ...often cannot be met without recourse to external data sources to obtain the necessary information sets. The proposed structure of the Business Names Register is of immense concern to us, not only because of the likely impact on our business but the potential risk of intervention by regulators should we fail to meet our regulatory obligations due to the absence of a critical data set.
>
> Whilst this may not have been the intended consequence, we urge the Committee to consider the regulatory impact of preventing access to an independent and reliable data set.[20]

3.33 In its submission to the inquiry, DIISR argued that non-government entities are restricted from accessing information on the national register given the Commonwealth's obligations under the *Privacy Act 1988* and the National Privacy Principles. Compliance with the Privacy Act is a requirement under the Intergovernmental Agreement on the National Business Register.[21] In particular, DIISR noted that:

> For our Commonwealth legislation, we need to comply with the privacy laws and that means that under a number of the privacy principles we need to use information for the purposes for which it is being collected, and it has not been collected for purposes for private organisations to verify their data.[22]

3.34 DIISR also argued that ASIC has no control over the data it provides to third parties.[23]

3.35 However, the committee notes that ASIC would not be supplying information, because credit and financial service providers already have personal details, they would be merely checking these details against information held by ASIC; no personal details will be disclosed by ASIC to third–party organisations.[24] Therefore, ASIC would not be responsible in any way for what credit and financial service providers do with the information because they have attained personal information through lawful means without the help of ASIC, they are merely attempting verify personal details that business owners have provided.

---

20 AMEX, *Submission 7*, p. 2.

21 DIISR, *Submission 11*, p. 14.

22 Ms Ann Bray, Acting Head, Industry and Small Business Policy Division, *Proof Committee Hansard*, 2 August 2011, p. 5.

23 Ms Ann Bray, Acting Head, Industry and Small Business Policy Division, *Proof Committee Hansard*, 2 August 2011, p. 6.

24 Ms Ann Bray, Acting Head, Industry and Small Business Policy Division, *Proof Committee Hansard*, 2 August 2011, p. 6.

3.36 Veda Advantage argued that credit providers would only need a match/no match facility, which is a system whereby credit providers submit information to ASIC. ASIC would then notify the credit provider if there is a match or no match on their database. According to Veda, this system would protect identity, but at the same time provide the necessary information credit and financial service providers rely on:

> That avoids problems with disclosure and it is a solution that is available which we would be urging should be taken up.[25]

3.37 Veda Advantage stated that:

> The remedy we would suggest is the ability to use a name, a date of birth and an address, preferably a residential address, during the matching process to ensure that we match accurately to the person being inquired about.[26]

3.38 In an answer to a question on notice, the ABA wrote:

> The verification requirements are those defined in the AML/CTF Act and Rules. A definite match/no match service could meet these requirements however the question of whether the AML/CTF obligations could be fully satisfied by that service alone depends on the quality and accuracy of the data.
>
> A database that is overseen by a State, Territory or Federal body could provide a higher level of confidence to AUSTRAC and banks in relation to quality and accuracy of data.[27]

3.39 According to Veda, there is nothing in the draft legislation that would prevent a match/no match service being provided by ASIC; it appears to be an operational decision on the part of DIISR. Notably, the company argued that there is nothing in the legislation that dictates the manner of search of the register and as such, there is nothing preventing a search of the register based on match/no match. Rather, Veda's concern is with how the Department and ASIC will put the provisions into operation.[28]

3.40 The necessity for online verification of identity, as opposed to relying on other sources such as face to face verification, was also raised by Mr Graeme Alexander, Head of Compliance and Ethics, Australia and New Zealand, with AMEX:

---

25 Mr Strassberg, External Relations, Veda Advantage, *Proof Committee Hansard*, 2 August 2011, p. 26.

26 Mr Strassberg, External Relations, Veda Advantage, *Proof Committee Hansard*, 2 August 2011, p. 28.

27 Australian Bankers' Association, answer to question on notice, 4 August 2011 (received 9 August 2011).

28 Mr Strassberg, External Relations, Veda Advantage, *Proof Committee Hansard*, 2 August, p. 28.

> I think, from a competition perspective, whilst our colleagues here from banks have bricks and mortar, there are a range of financial players out there that operate in a branchless environment. It is increasingly difficult to rely on face-to-face verification in that sort of 24/7 online channel.[29]

3.41 Moreover, Mr Hardaker, Executive Director of the AFC, remarked on the need to verify business registration details:

> **CHAIR**: In that case, explain to me why access to the name, date of birth and home address of the proposed business registrant is so critical.
>
> **Mr Hardaker:** We have to verify who is behind the business name to meet our AML-CTF obligations. Just getting a person's name without being able to verify that they are that Ron Hardaker born on 7 February and living at that address means that we have not gone as far as we need to go to meet the AUSTRAC requirements.
>
> **CHAIR**: If Ron Hardaker of ABC Enterprises in New South Wales comes to the NAB branch seeking a loan of a quarter of a million dollars, there are other ways that the officers in the NAB branch would be able to check that he is indeed Ron Hardaker and does live at 16 Smith Street in a particular suburb and his birthday is what he says it is, are there not?
>
> **Mr Hardaker**: There are, but behind the business name you have to also verify him. It is one thing sitting in front of him with a drivers licence, but when you have got the business name there it provides that additional verification to say that is the proprietor of the business name.[30]

3.42 The ABA supported the AFC's views on the importance of accessing business names registers:

> **Senator BUSHBY**: As I asked about before, the challenge we had with people is that even if they can prove that they are a person of a particular name they may not be the person of that name who is behind the business, and current arrangements, at least within three states, enable you to at least find some corroborating evidence using other details like home address or date of birth that that person appears to be the same person.
>
> **Mr AJ Burke:** Yes.[31]

3.43 The AFC later argued the very purpose of a business register is to be able to verify business details:

---

29 Mr Graeme Alexander, Head of Compliance and Ethics, American Express, *Proof Committee Hansard*, 2 August 2011, p. 22.

30 Mr Ron Hardaker, Executive Director, Australian Finance Conference, *Proof Committee Hansard*, 2 August 2011, p. 22.

31 Mr A.J. Burke, Policy Director, Australian Bankers' Association, *Proof Committee Hansard*, 2 August 2011, p. 23.

> **Senator BUSHBY:** We have sought a copy of the legal advice the department have received. I do not know whether they have looked at that issue from that perspective or not. If we can get hold of that legal advice, I think it would be very interesting. It seems to me that the purpose for which you want that information is consistent with the purpose for which it was provided, and that is so those who interact with a business running under an alias know who is behind it.
>
> **Mr Hardaker:** Yes. It is hard to think of a more consistent use.[32]

3.44 This issue of intent and the purpose of the database was also raised with DIISR. The Department argued that the requirement to mandate an ABN with the registration of a business name provides greater proof of identity. The process of gaining an ABN requires a 100 point check. DIISR noted that through this process, ASIC can verify the name and the entity name.[33]

Clause 77 of the bill and the difficulties in matching data

3.45 As discussed in paragraph 3.42, it was suggested to the committee that nothing in the legislation prevents a match/no match system. However upon closer scrutiny of the bills and regulations it would appear that a number of changes would need to be made to clause 77 of the Business Names Registration Bill.

3.46 Clause 77 of the bill relates to the use of private information obtained by ASIC. It stipulates that:

> Protection of confidentiality of information
>
> (1) A person who obtains information in the course of performing functions or exercising powers under this Act or the Transitional Act must not:
>
> (a) make a record of the information; or
>
> (b) use the information; or
>
> (c) disclose the information.
>
> Penalty: Imprisonment for 1 year.
>
> (2) Subsection (1) does not apply if:
>
> (a) the information is recorded, used or disclosed for the purposes of performing functions or exercising powers under this Act or the Transitional Act; or

32 Mr Ron Hardaker, Executive Director, Australian Finance Conference, *Proof Committee Hansard*, 2 August 2011, p. 24.

33 Ms Ann Bray, Acting Head, Industry and Small Business Policy Division, *Proof Committee Hansard*, 2 August 2011, p. 7.

(b) the information is recorded, used or disclosed in accordance with a provision of this Act or the Transitional Act; or

(c) the information is recorded, used or disclosed with the consent of the entity that provided the information; or

(d) the information is given to a court or tribunal.

Note: A defendant bears an evidential burden in relation to the matters in subsection (2): see subsection 13.3(3) of the *Criminal Code*.

(3) A person commits an offence if:

(a) information is made available to a government body or to an intelligence or security agency under section 62; and

(b) a person obtains the information in the course of performing functions or exercising powers for the body or agency; and

(c) the person would not have had access to the information if it had not been made available to the body or agency under section 62; and

(d) the person records, uses or discloses the information for a purpose other than that for which it was made available; and

(e) the person is reckless as to whether the purpose for which the information is recorded, used or disclosed is that for which it was made available.

Penalty: Imprisonment for 6 months.

Note: Where a fault element for a physical element of an offence is not stated, see section 5.6 of the *Criminal Code* for the appropriate fault element.

(4) Subsection (3) does not apply if:

(a) the person discloses the information to another person; and

(b) the disclosure is reasonably necessary for:

(i) the enforcement of the criminal law; or

(ii) the enforcement of a law imposing a pecuniary penalty; or

(iii) the protection of the public revenue.

Note: A defendant bears an evidential burden in relation to the matters in subsection (4): see subsection 13.3(3) of the *Criminal Code*.

(5) Subsections (1) and (3) are not intended to have an operation that would infringe an implied constitutional immunity of a referring/adopting State.

3.47 The permitted uses of information under subclause 77(2) may prohibit the use of information by ASIC to verify identity for credit lending purposes. However, this is

not clear cut because subparagraph 77(2)(c) states that information can be used or disclosed in different ways if ASIC has consent.

3.48 If the courts deem that consent is not enough to enable ASIC to match data, then clause 77 would need to be amended.

3.49 However, ASIC could issue extracts to third party credit providers with the necessary information if regulation 9, which restricts the information available on extracts, was amended. In this way, the main bills need not be changed, only the regulations which are still in consultation draft phase and have not yet been settled with the states and territories.

The Privacy Act and the Information Privacy Principles

3.50 As mentioned earlier in the chapter, the government's key rationale for the drafting of regulation 9 is to ensure that the Commonwealth complies with the Information Privacy Principles outlined in section 14 of the *Privacy Act 1988*. In its answer to a question on notice, DIISR informed the committee that:

> ...section 14 of the Privacy Act 1988, and in particular IPP 1, limits the collections of personal information by agencies to lawful purposes directly related to a function or activity of the collector (and the BNR Bills do not provide for collection for credit provider/agency related purposes). IPP 11 prohibits disclosure of such information, without consent, for purposes other than that collected, to, in summary, circumstances where:
>
> - there is an imminent threat to life or health of an individual;
> - authorised or required by law; and
> - it is reasonably necessary for enforcement of criminal law or law imposing a pecuniary penalty or for the protection of public revenue.[34]

3.51 As noted above, DIISR has emphasised the need for Commonwealth legislation to comply with privacy laws and in particular, the tenet that information is used for the purposes for which it is being collected. It argues that the purpose for collecting information on the business names register is not for private organisations to verify their data.[35]

3.52 However, the committee notes that government agencies are treated differently to private agencies in respects to identity verification. Government agencies verify identity for a number of reasons, including but not limited to:

---

34 DIISR, answer to question on notice, 4 August 2011 (received 8 August 2011).

35 Ms Ann Bray, Acting Head, Industry and Small Business Policy Division, *Proof Committee Hansard*, p 5.

- the investigation and/or prevention of crime;
- the investigation of fraud and white collar crime;
- regulatory functions; and
- administrative purposes.

3.53 Private information brokers, such as Veda Advantage and members of the ABA, verify identity in an effort to achieve similar outcomes. As credit and financial service providers, they are at the cold-front of preventing fraud and white collar crime. Through their verification services, fraud can be detected and stopped before incidents are escalated to involve the police and other government agencies.

3.54 Therefore, in light of this evidence, the committee believes that the distinction between government agencies and private third-party information brokers warrants further consideration.

3.55 In rationalising this distinction between government and private bodies, the department also maintains that the Inter-Governmental Agreement (IGA) signed by the states and territories would prohibit the sharing of personal information for the purposes of identity verification. DIISR states that:

> It should be noted that Clause 4.3 (b) of the Intergovernmental Agreement which underpins the national law that the Bills establish outlines the purpose of the law, namely the registration and use of business names. The purpose of the national law does not include provision of data for authentication and verification purposes (for example through "match/no match" functionality).[36]
>
> Furthermore, Clause 4.4 (12) of the Intergovernmental Agreement states that "All business names data held by the Commission [ASIC], whether originating in State or Territory agencies or collected directly by Commonwealth agencies, will from the commencement of the national law be subject to the Commonwealth's privacy and secrecy legislation."

3.56 However, the committee notes that the IGA specifically permits credit providers access to ASIC's database in subparagraphs 5.1(f)(g) of the agreement:

> 5.1. The Commission will use its best endeavours to provide the following services as part of the national system:
>
> a) business name registration services via the Internet;
>
> b) on-line business name registration point at the Commission's Services Centres in capital cities;
>
> c) on-line business name registration points via appropriate agents and networks;

36 DIISR, answer to question on notice, 4 August 2011 (received 8 August 2011).

d) paper forms, in an electronic format, which may be printed at the various service points and, after completion, lodged with the Commission;

e) a telephone support system for those registering, or considering registering, a business name;

f) an online service for the searching of the business names register by the public, States and Territories, and information brokers; and

g) an extract service for brokers on commercial terms agreed with individual brokers.

3.57 If the interpretation of 'extract service' is consistent with that of the Corporations Regulations 2001,[37] then information such as date of birth and residential address could be provided to credit and financial service providers:

> For section 346B of the Act, the following particulars are prescribed for a company:
>
> a) ACN;
>
> b) name;
>
> c) address of registered office;
>
> d) address of principal place of business in this jurisdiction;
>
> e) for each director and company secretary:
>
> (i) the person's name; and
>
> (ii) the person's usual residential address, or, if the person is entitled to have an alternative address under subsection 205D (2) of the Act, that alternative address; and
>
> (iii) the person's date and place of birth.[38]

3.58 Additionally, in paragraph 5.4(1), the IGA states that ASIC will use 'its best endeavours' to provide the same levels of service as is currently provided by the states and territories, and that ASIC 'strive to enhance progressively existing levels of service in each referring state and territory.' This statement is also made in paragraph 1.1(2) of the Agreement, which stipulates that levels of service provided by the new national business names register will not be any less than that currently provided by state and territory systems.

---

37 Regulation 2N.2.01 which relates to Part 2N.2 of the *Corporations Act 2001* dealing with extracts.

38 The regulations quoted represent just a small section of other particulars, which are not relevant for businesses.

3.59 Moreover, the committee understands that the Information Privacy Principles are not breached because third-party credit and financial service providers use personal information for purposes consistent with the nature of their business and they obtain consent from clients/credit applicants who are business owners to verify their identity, thereby satisfying Information Privacy Principle 11 of the Act. It is reasonable to assume that credit providers would use the business register to verify business and associated personal details provided to them.

3.60 Consequently, the committee notes that there appears to be no conflict between ASIC's obligations under the IGA and the Information Privacy Principles of the Privacy Act and its ability to verify personal and business details.

3.61 Additionally, when a business name is registered, applicants typically provide consent for their information to be used for a variety of unspecified purposes. For example, the ACT Business Names Registration Form stipulates the following:

> The Act authorises the Registrar-General to collect the information required by this form for the purpose of establishing and maintaining the public register of business names registered under the Act. The public register is available for search pursuant to Section 22 and 23 of the Act, and is also made available to government agencies for statistical and administrative purposes, and to non-government persons and organisations.[39]

3.62 Therefore, by including a Privacy Statement on the application to register a business name, as exemplified by the states and territories, ASIC would not be in breach of its obligations under the Privacy Act.

3.63 Furthermore, during the public hearing, DIISR argued that the ASIC database cannot be used to verify identity because, firstly, the information it contains will not be verified data and secondly, identity verification is not the purpose of the register.[40] However, on the first issue, the committee notes that unverified information has been utilised successfully by credit providers for decades, with no complaints or issues. On the second issue raised by DIISR, business registration databases are provided for the purposes of verifying the identity of a business owner. Therefore, it can be argued that the business names registers are designed for the very specific purpose of identity verification, whether this verification is made by the public or by credit providers.

3.64 Veda contests DIISR's policy stance on the issue of privacy and the purpose of ASIC's business names registry. It argued that it is not possible to limit the use of databases to the extent that the bill proposes:

---

39 The *Particulars of Business Names* form is available at: http://www.ors.act.gov.au/business/business_names/forms_and_fees.

40 Ms Ann Bray, Acting Head, Industry and Small Business Policy Division, *Proof Committee Hansard*, p. 3.

> The reality is that datasets do have a life greater than what might originally have been intended. That has been the case with business names, where there is substantial information on the state registers. If you look at something even as simply as a driver's licence, does anyone really still believe the notion that a driver's licence is simply an authority to drive? The reality is that people produce and are required to produce their driver's licence in a whole range of situations that relate to the verification of their identity. Similarly, the passport is very often asked for as a form of identity not just as an authority to travel.[41]

3.65 Veda added that:

> ...the insistence of the department that business names be ascribed a solitary purpose is to take a bonsai approach to information. It is an artificial constraint. It is one that will inhibit the ability to detect potential fraud, which will hurt those small and medium enterprises that need to do much more diligent trading history report checks than in fact what larger businesses do.[42]

3.66 Therefore, in light of the foregoing discussion, the committee suggests that the government give further consideration to its decision to deny information brokers the same level of access to the business names register that they currently have.

41 Mr Strassberg, External Relations, Veda Advantage, *Proof Committee Hansard*, p. 28.

42 Mr Strassberg, External Relations, Veda Advantage, *Proof Committee Hansard*, 2 August 2011, p. 28.