PRIVACY IMPACT ASSESSMENT REPORT

ELECTRONICALLY VERIFYING IDENTITY UNDER THE *ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING ACT* 2006 USING CREDIT REPORTING INFORMATION

For: Attorney General's Department

8 OCTOBER 2009

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

1.1 BACKGROUND

The Attorney-General's Department (AGD) has asked Information Integrity Solutions Pty Ltd (IIS) to conduct a Privacy Impact Assessment (PIA) on a proposal to amend the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) to expressly authorise the use and disclosure of credit reporting information for electronic identity verification (EV) under the AML/CTF Act.

Under the AML/CTF Act rules, identity verification can be undertaken by the inspection of physical documents, for example, drivers licence or birth certificates or by EV. EV involves checking specified identity details – at a minimum name, address and date of birth (DOB) or transaction history – against information held by other reliable organisations. While reporting entities, particularly those who only operate online, indicate strong interest in using online identity verification, in practice take up is affected by the limited options for confirming details, in particular DOB.

The Australian Law Reform Commission considered the question of the use of credit reporting information for EV and, while recognising the sensitivity of the proposal, recommended that it could be used for EV subject to further consideration of a range of issues.[1] The Government has since decided in principle to allow the proposed amendments to the AML/CTF Act to proceed subject to appropriate privacy protections.

1.2 PURPOSE OF THE PIA

AGD is now in the process of developing a proposal for the use of credit reporting information for EV for consideration by the Government and Parliament. If the proposal is adopted, the draft legislation giving it effect could be introduced later in 2009 or early in 2010.

The purpose of the PIA is to assess the privacy impacts of the current AGD proposal to assist it to develop its advice for Government. The PIA will consider:

- the proposal as put by AGD including the amendment to the AML/CTF Act, options in relation to some aspects of the proposal and a range of privacy safeguards;
- the issues identified by the ALRC in its report as needing further consideration, and by key submitters to that report including the Office of the Privacy Commissioner (OPC); and
- the views of stakeholders consulted in the course of the PIA.

While the context for the proposal, including alternatives, is relevant to the PIA, IIS has not been asked to consider these alternatives in detail.

1.3 METHODOLOGY

A PIA is a process that enables organisations to "anticipate and address the likely impacts of new initiatives, foresee problems, and negotiate solutions." [2]

[1] ALRC report *For Your Information: Australian Privacy Law and Practice* Recommendation 57-4 available at www.alrc.gov.au

[2] See www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html

In preparing this report IIS applied a particular framework for analysing privacy risks. This included considering compliance with the privacy principles in the *Privacy Act 1988* (Cth) (the Privacy Act), in particular in relation to the National Privacy Principles (NPPs) and to Part IIIA of the Act which sets out the provisions relating to credit reporting and also considering broader privacy risks, including how these are allocated as between reporting entities, credit reporting agencies (CRAs) and the citizen.

The PIA involved the following steps.

- Information gathering including reviewing the material available with a particular focus on submissions to the ALRC and to AGD – a list of the material considered is at Appendix 1.
- Analysis of the information using the framework noted above to identify key aspects of the project that may potentially have an impact on privacy.
- Consultation with key stakeholders including privacy and consumer advocates, reporting entities and their representatives, CRAs and other EV service providers. The consultation process involved:
    - Contacting stakeholders on 20 July 2009, providing them with a short consultation paper and inviting them to a meeting and/or to provide submissions by 21 August 2009 (submissions received are listed at Appendix 2); and
    - Conducting a series of meetings in the period 5-10 August 2009 as listed at Appendix 2; and
- Developing a draft report and recommendations which were provided to AGD and then to stakeholders who had previously provided submissions or attended meetings on 24 September 2009 with request for comments by 29 September 2009 and, following consideration of these comments (those making comments are listed at Appendix 2) and discussions with AGD, developing this final report.

In developing it recommendations IIS drew on its "layered defence" approach. This applies a number of possible "tools" to arrive at practical solutions the fit the particular circumstances. These tools include:

- "Business as usual" good practice, including education, process and culture change regarding the expectations about the way things are done by staff, and the actions that users need to take to protect themselves.
- Additional law where risks are particularly high (eg specific use and disclosure limitations, criminal penalties, special measures to ensure review before critical changes are made;
- Technology, including design limits on information collected, what can be connected and who can see what;
- Governance, including transparency and accountability;
- Safety-net mechanisms for citizens when failure or mistakes.

1.4 OVERALL CONCLUSIONS

The issue that drives this PIA is the need to find a reasonably trustworthy, reasonably technologically accessible source of information about DOB to add to existing sources of information used by EV services or processes, in order to meet electronic identity verification requirements under the AML/CTF Act.

The policy development process, including the ALRC's review of the Privacy Act, has led to the conclusion that in the current environment DOB held by credit reporting databases would add considerably to the utility of EV systems. In the AML/CTF context this cannot be ignored.

IIS also notes that there is currently one EV service provider, and potentially others, offering alternative approaches to identity verification. However, it was beyond the scope of this PIA to consider the privacy risks in other EV models. IIS has also briefly considered other sources of DOB information that could be included in an online EV system. For a range of reasons these data sources are not currently available or are not viable for EV services. These reasons are discussed in section 5.2.1.1.

In the course of this PIA IIS has identified a number of areas of privacy risks that may arise should identity information held by credit reporting databases be made available for AML/CTF EV. These are:

- "function creep" meaning that the proposal extends the use of credit reporting data beyond that currently permitted by the law and expected by the community, potentially undermining community trust in credit reporting and, for example, willingness to consider other changes to the credit reporting system;

- the potential for the identity confirmation process to create new data about individuals that could then be used for new purposes, which may or may not be with the knowledge of the individual concerned and may or may not be to the advantage of the individual concerned;

- the potential for individuals to be disadvantaged if they "fail" the EV process should it involve the use of credit reporting information, for example because of inaccuracies in the information held by CRAs or because of the nature of the checking process, without inadequate advice or recourse;

- the extent of choice that individuals have in the process, for example about whether to provide paper documents in a face-to-face identity verification process or to proceed with electronic verification and if the latter to choose whether or not to have credit reporting information included as part of an EV check; and

- the extent to which CRAs or reporting entities might either incidentally or otherwise gain access to personal information beyond what is necessary for the purposes of identity verification for AML/CTF purposes and who bears the risk when problems or mistakes with electronic verification system arise.

IIS recognises that the proposal as given to it for conducting PIA has been crafted with considerable effort to minimise privacy impact including by minimising changes to the credit reporting system. The measures to minimise impact include:

- only allowing access to identifying information held by CRAs for the purpose of verifying name, residential address and DOB to proceed with the consent of the individual concerned;

- only allowing the EV process to return a yes/no response or matching score and no other information; and

- not permitting secondary use of information obtained as a result of a matching process.

IIS notes that some industry stakeholders consider the proposal as framed is quite restrictive and as such is not a proportional response to the privacy risks identified. However IIS considers that a more open approach would raise possibly different privacy and policy issues and would need to be subject of a further review and consultation process.

IIS considers that the proposal as circulated raises some significant privacy issues and that these need to be addressed. However, IIS considers that if the proposal is introduced in the limited way set out in the AGD proposal, and subject to the recommendations it makes in this PIA, then on balance the proposal is likely to have reasonably significant benefits, including privacy benefits, to individuals and the community.

1.5 LIST OF RECOMMENDATIONS

IIS has considered the issues in this PIA through the lens of its "layered" defence framework. At this early stage, the emphasis in the recommendations is on establishing the legal and governance framework that will build in strong and sustainable privacy protection from the start. The recommendations below are grouped by the relevant layer in the IIS framework.

Recommendations Relating To The Law

Recommendation 1 - Consent

IIS recommends that, if the proposal proceeds, the enabling legislation must provide that an EV process using credit reporting information should only proceed with the consent of the individual concerned and that a request for consent should be made separately from requests for consent for any other activities, should be easy to exercise and should be informed by detailed information about the EV process including that:

- an EV process may not succeed, or may not be sufficient, for a number of reasons because of the nature of risk bases processes allowed under the AML/CTF Act;
- the likely databases involved;
- how to find out more about the databases; and
- the alternative identity verification mechanisms available.

Recommendation 2 – Details to be checked in an EV process using credit reporting information

IIS recommends that, if the proposal proceed, the enabling legislation permit reporting entities in seeking EV using credit reporting information to provide only an individual's name, residential address and DOB to a CRA and that the CRA be permitted to use credit reporting information only to confirm the accuracy of these details on the basis agreed between the reporting entity and the CRA.

Recommendation 3 – Results reported on a yes/no basis or as a score

IIS recommends that if the proposal proceeds that it should be on the basis of a legislative amendment specifying the information that CRAs would be permitted to provide to reporting entities. This should be limited to the results of a match, which could be reported on a yes/no basis or as a score as agreed between the reporting entity and the CRA.

Recommendation 4 – Separate individual EV record

IIS recommends that if the proposal proceeds, the enabling legislation should require a CRA to keep a separate record of EV attempts it has processed in relation to an individual and that the record should include the date of inquiry and the name of reporting entity, the details matched and a note of disclosures of the contents of the EV record. IIS further recommends that the EV record should be held separately from a credit information file and not be included as "permitted contents" of a credit information file, included in a credit report under Part IIIA of the Privacy Act.

Recommendation 5 – Limits on secondary use of EV process information

IIS recommends that the enabling legislation should specify that information obtained or generated as part of EV using credit reporting information must not be used or disclosed for any secondary purpose not related to EV under the AML/CTF Act, other obligations under the AML/CTF act or as otherwise authorised by law. In particular, the law should provide that CRAs are not permitted to use information obtained in the course of an EV request to create or update credit information files as defined by Part IIIA of the Privacy Act.

Recommendation 6 – Notice of EV failure

IIS recommends that if the proposal proceeds, AGD should undertake further work, in conjunction with reporting entities and including testing options with individuals, to develop an approach to advising individuals about an EV failure. The approach will need to balance the concerns of reporting entities and the need to alert individuals to the possible need to follow up possible inaccuracies in source records or other difficulties.

Recommendation 7 – Alternative to be available

IIS recommends that if the proposal proceeds, the enabling legislation should provide that should an individual fail an EV process offered by a reporting entity, the reporting entity must either offer an alternative means by which the individual may choose to attempt to verify their identity or must refer the person to an existing dispute resolution process such as the Privacy Commissioner, or the Banking and Financial Services Ombudsman.

Recommendation 8 – Individuals to be given reasonable access to EV files about them

IIS recommends that if the proposal proceeds the enabling legislation should specify that where an EV process involves the use of credit reporting information an individual should be entitled to access to their EV record held by a CRA on the same basis that access would be provided to credit reporting information under the access provisions in Part IIIA of the Privacy Act and the Credit Reporting Code of Conduct.

Recommendation 9 – Penalties for unauthorised access or use

IIS recommends that if the proposal proceeds, consideration should be given to the need for offence provisions for unauthorised access to EV records whether held by a CRA or a reporting entity taking account of any changes to Part IIIA following the Government's consideration of the recommendations in the ALRC report.

Recommendation 10 – Privacy Act coverage

IIS recommends that if the proposal proceeds, consideration should be given as to whether the Privacy Act protects personal information collected by reporting entities for the purposes of EV under the AML/CTF Act in all circumstances, including where a reporting entity (which is deemed by section 6E(1A) of the Privacy Act to be an organisation for the purposes of complying with the AML/CTF Act) uses, or misuses, this personal information for non- AML/CTF purposes. If any gap in coverage is identified the Privacy Act should be appropriately amended.

Recommendation 11 - Retention of EV information

IIS recommends that if the proposal proceeds the applicable retention period for EV information be five years unless there are policy reasons arising from the AML/CTF regime to keep EV records held by CRAs for longer than five years.

Recommendation 12 – EV using credit reporting information included in AML/CTF Act review

IIS recommends that any amendments to give effect to the proposal be subject to review as part of the required review of the AML/CTF Act in 2013. IIS recommends that this review should include consideration of alternative sources of information available for identity verification, the privacy implications arising from both alternative information sources and alternative EV process, and that it should include a wider review of Australia's ID management systems. IIS recommends that a review of EV using credit reporting information should be informed by detailed statistical information collected by the relevant regulation on EV including on the extent to which EV is successful and where it is not successful, the reasons.

Recommendations relating to Governance, including transparency and accountability

Recommendation 13 – Monitoring

IIS recommends that the proposal should not proceed unless it is clear that the relevant regulators and dispute resolution bodies are properly resourced to carry out appropriate monitoring of the use credit reporting information in EV processes in particular in relation to whether:

- the consent processes used by reporting entities mean that individuals are provided with appropriate information before deciding to proceed;
- reporting entities are providing appropriate advice to individuals about EV failure;
- failure in relation EV is not being taken into account in substantive decisions about an individual.

IIS notes that the Office of the Privacy Commissioner, AUSTRAC and relevant dispute resolution bodies may need to liaise to clarify their respective roles in implementing this recommendation.

Recommendation 14 – No further use of credit reporting information without review

IIS recommends that there should be no further use of information held by CRAs for any new purposes without a wide-ranging review that is:

- independent;

- includes wide ranging public consultation; and
- follows PIA good practice.

IIS also recommends that the Government consider undertaking an investigation into Australia's online identity verification practices so as to identity processes and information sources and regulatory frameworks that are effective and which minimise privacy impact.

2 INTRODUCTION

The Attorney-General's Department (AGD) has asked Information Integrity Solutions Pty Ltd (IIS) to conduct a Privacy Impact Assessment (PIA) on a proposal to amend the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) to expressly authorise the use and disclosure of credit reporting information for electronic identity verification (EV) under the AML/CTF Act.

Under the AML/CTF Act rules, identity verification can be undertaken by the inspection of physical documents, for example, drivers licence or birth certificates or by EV. EV involves checking specified identity details – at a minimum name, address and date of birth (DOB) or transaction history – against information held by other reliable organisations. While reporting entities, particularly those who only operate online, indicate strong interest in using online identity verification, in practice take up is affected by the limited options for confirming details, in particular DOB.

The Australian Law Reform Commission considered the question of the use of credit reporting information for EV and, while recognising the sensitivity of the proposal, recommended that it could be used for EV subject to further consideration of a range of issues.[3] The Government has since decided in principle to allow the proposed amendments to the AML/CTF Act to proceed subject to appropriate privacy protections.

2.1 PURPOSE AND SCOPE OF THE PIA

AGD is now in the process of developing a proposal for the use of credit reporting information for EV for consideration by the Government and Parliament. If the proposal is adopted, the draft legislation giving it effect could be introduced later in 2009 or early in 2010.

The purpose of the PIA is to assess the privacy impacts of the current AGD proposal to assist it to develop its advice for Government. The PIA will consider:

- the proposal as put by AGD including the amendment to the AML/CTF Act, options in relation to some aspects of the proposal and a range of privacy safeguards;
- the issues identified by the ALRC in its report as needing further consideration, and by key submitters to that report including the Office of the Privacy Commissioner (OPC); and
- the views of stakeholders consulted in the course of the PIA.

While the context for the proposal, including alternatives, is relevant to the PIA, IIS has not been asked to consider these alternatives in detail.

2.2 METHODOLOGY

A PIA is a process that enables organisations to "anticipate and address the likely impacts of new initiatives, foresee problems, and negotiate solutions."[4]

In preparing this report IIS applied a particular framework for analysing privacy risks. This included considering compliance with the privacy principles in the *Privacy Act 1988* (Cth) (the Privacy Act), in

[3] ALRC report *For Your Information: Australian Privacy Law and Practice* Recommendation 57-4 available at www.alrc.gov.au

[4] See www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html

particular in relation to the National Privacy Principles (NPPs) and to Part IIIA of the Act which sets out the provisions relating to credit reporting and also considering broader privacy risks, including how these are allocated as between reporting entities, credit reporting agencies (CRAs) and the citizen.

In preparing this PIA IIS took the following steps.

- Information gathering including reviewing the material available with a particular focus on submissions to the ALRC and to AGD – a list of the material considered is at Appendix 1.
- Analysis of the information using the framework noted above to identify key aspects of the project that may potentially have an impact on privacy.
- Consultation with key stakeholders including privacy and consumer advocates, reporting entities and their representatives, CRAs and other EV service providers. The consultation process involved:
    - Contacting stakeholders on 20 July 2009, providing them with a short consultation paper and inviting them to a meeting and/or to provide submissions by 21 August 2009 (submissions received are listed at Appendix 2); and
    - Conducting a series of meetings in the period 5-10 August 2009 as listed at Appendix 2; and
- Developing a draft report and recommendations which were provided to AGD and then to stakeholders who had previously provided submissions or attended meetings on 24 September 2009 with request for comments by 29 September 2009 and, following consideration of these comments (those making comments are listed at Appendix 2) and discussions with AGD, developing this final report.

In developing it recommendations IIS drew on its "layered defence" approach. This applies a number of possible "tools" to arrive at practical solutions the fit the particular circumstances. These tools include:

- "Business as usual" good practice, including education, process and culture change regarding the expectations about the way things are done by staff, and the actions that users need to take to protect themselves.
- Additional law where risks are particularly high (eg specific use and disclosure limitations, criminal penalties, special measures to ensure review before critical changes are made;
- Technology, including design limits on information collected, what can be connected and who can see what;
- Governance, including transparency and accountability;
- Safety-net mechanisms for citizens when failure or mistakes.

3 DESCRIPTION OF THE PROPOSAL AND OTHER BACKGROUND

3.1 BACKGROUND

Australia has had anti-money laundering laws, including proof of identity requirements, since the late 1980s. The current law, the AML/CTF Act, sets out, amongst other things, reporting entities' obligations including in relation to customer identification. It adopts a risk-based approach (replacing the more prescriptive "100 points" approach of earlier anti-money laundering legislation). The AML/CTF Act leaves it more to reporting entities to decide how much checking is needed within the specified AML/CTF risk framework before being satisfied that the customer in the context of a product or transaction does not pose an unacceptable risk of money-laundering or other identified threats.

The approach is set out in Part 4.10 of the *Anti Money Laundering and Counter-Terrorism Financing Rules Instrument 2007* (the Rules) that allows for document-based and electronic verification or a mixture of both. The Rules specify the process for electronic verification, known as the "safe harbour" provisions, that can be used where the apparent risk of money laundering and/or terrorism financing is medium to low. The electronic "safe harbour" provisions allow reporting entities to verify a customer's identity by checking specified details against at least two independent data sources. The details to be checked at a minimum are:

- name and residential address; and either
- DOB; or
- that the customer has a transaction history for at least the past three years.

Reporting entities may decide to conduct additional checks if in their view the circumstances indicate there may be a greater risk of offences under the AML/CTF Act and so they need a greater level of assurance of identity.

EV may benefit both reporting entities and customers. IIS understands that experience to date shows it can significantly reduce AML/CTF compliance costs for reporting entities and customers. In addition, it reduces the need for customers to present physical records or provide certified copies of original records to reporting entities. However in practice take up is affected by the limited options for confirming details, in particular DOB, electronically. Credit reporting databases are one possible source of information for EV. The information they hold includes DOBs, in the case of the larger credit reporting agencies (CRAs), of most of the adult population.

3.2 ALRC CONSIDERATION OF USE OF CREDIT REPORTING INFORMATION FOR EV

The ALRC was asked to consider the use of credit reporting information for EV in its inquiry into the extent to which the Privacy Act and related laws continue to provide an effective framework for the protection of privacy in Australia. The Inquiry was completed in 2008. In its report, the ALRC noted that the "use and disclosure of credit reporting information for the purposes of satisfying obligations under the AML/CTF Act was an issue of significant concern to many stakeholders."[5]

[5] ALRC report Para 51.129 see note 1 above

The ALRC recognised the limited reliable sources of information currently available for EV and noted that CRAs are a regulated source, with comprehensive coverage and commercial electronic accessibility. It noted the views of reporting entities that EV is a faster, cost-effective way of streamlining credit and other applications that obviates the need for individuals to provide documents or undergo other identify verification processes. The ALRC was advised that EV is particularly important for the competitive position of credit providers that do not have a branch network and rely on the Internet or brokers to market and distribute their financial products.

The ALRC also noted the concerns raised by privacy and consumer advocates about the possible impact on the privacy of individuals. There was clear opposition to the proposals for reasons such as:

- Inconsistency with the current focus of the credit reporting system amounting to "function creep";
- The perception that the ALRC inquiry was a backdoor approach to overturning the Government's previous decision not to authorise the use of credit reporting information for EV;
- A better option would be to undertake a wider review of Australia's approach to identity management; and
- The difficulty in considering the risks without a detailed proposal as to what organisations and information would be involved and how issues such as secondary use, openness and accuracy would be handled.

Organisations offering alternative EV products also queried whether CRA data holdings were sufficiently accurate to use in EV processes.

In arguing the case for allowing the use of credit reporting information for EV reporting entities suggested privacy protections including:

- New restrictions on access to credit reporting information and new penalties for unauthorised access;
- A consent based approach, which would also ensure that the personal information comes directly from the individuals;
- Limiting disclosure to that needed to verify identity on a match/no match basis (one organisation suggested age of file would be relevant to confirming identity); and
- Access to CRA held credit information for AML/CTF purposes be logged

The ALRC recognised that the proposal amounted to significant function creep and it also recommended a wider review of identity checking and the sources of information available for EV. It also recognised that the Government had deferred its decision on the basis that the ALRC would consider the issues. It therefore concluded it needed to make a specific recommendation and concluded that the use of credit reporting data for EV should be permitted subject to further consideration of a wide range of issues including whether:

- the legislation should prohibit the secondary use or disclosure by reporting entities of credit reporting information obtained for identity verification purposes;

- reporting entities should have positive obligations to seek consent from individuals before using credit reporting information to verify identity; and
- reporting entities should have processes in place to resolve mismatches between the information individuals provide and credit reporting information. [6]

3.3 OVERVIEW OF CREDIT REPORTING AND ITS REGULATION

CRAs provide services to credit providers to assist them to manage credit risk, including by collating lists of loan defaulters. Part IIIA of the Privacy Act regulates the credit reporting sector, which includes CRAs, credit providers, mortgage insurers, debt collectors and some others. Part IIIA was enacted in recognition of the sensitivity of credit reporting information and the perceived risks to individual privacy including that credit reporting information was being used for unauthorised, non consumer credit related purposes. [7]

CRAs are permitted to collect and disclose quite detailed information about individuals including:

- full name, including any known aliases, sex and DOB;
- a maximum of three addresses consisting of a current and last known address and two immediately previous addresses;
- name of current or last known employer;
- driver's licence number;
- a record of a credit provider having sought a credit report to assess an application for consumer or commercial credit;
- default information (note that information may only be included here if a payment is at least sixty days overdue and the credit provider has taken steps to collect the amount outstanding); and
- certain items of publicly available information such as court judgments and bankruptcy orders.[8]

Part IIIA sets a prescriptive regime for the use and protection of credit reporting information. The provisions prevent non-credit providers, which would include some reporting entities, from accessing credit files or credit reports unless specifically authorised by another law. The provisions also limit the purposes for which CRAs may disclose credit reporting information. IIS understands Part III would not currently permit credit reporting agencies to disclose credit reporting information for the purpose of identity verification.

The provisions in Part IIIA include in summary:

- Rules about what information may be included in a credit file, in what circumstances;
- Limits on the use and disclosure of credit reporting information by CRAs;[9]

[6] ALRC Report on privacy laws, *For Your Information: Australian Privacy Law and Practice* Recommendation 57-4. The report is available at www.alrc.gov.au.

[7] See the Privacy Commissioner's website at www.privacy.gov.au/act/credit/index.html for information about the Part IIIA of the Privacy Act. Background to the credit reporting provisions is included in the Second Reading Speech, Privacy Amendment Bill, Hansard House of Representatives, 4 December 1990.

[8] Section 8E of Part III A of the Privacy Act Credit Reporting Determination 1991 No 2 concerning identifying particulars permitted to be included in a credit information file

- Limits on the use and disclosure of credit reporting information by credit providers; and
- Privacy protections for individuals including that they should have: prior notice of the possibility of a default listing; notice if a decision to refuse credit is based on a credit report; and, under the Privacy Commissioner's Credit Reporting Code of Conduct, an avenue for access to credit reports with no charge.

Part IIIA includes some significant penalties, for example "a credit provider that intentionally contravenes [section 18N(1)] is guilty of an offence punishable, on conviction, by a fine not exceeding $150,000".[10]

While generally the provisions, and the penalties, apply to players in the credit sector, some extend to any "person". These are:

- Prohibition on access, by any person, to credit information files or credit reports held by CRAs or credit providers unless authorised by the Privacy Act; and
- Prohibition on obtaining access to credit information files or credit reports held by CRAs or credit providers by false pretences.[11]

In addition, failure to comply with Part IIIA may amount to an inference with an individual's privacy meaning the individual concerned may, if not able to resolve the matter directly with the CRA or credit provider, complain to the Privacy Commissioner.

It is relevant to this PIA to note that ALRC review also considered Part IIIA. The ALRC recommended that the "existing credit reporting provisions of the Privacy Act be repealed. Instead, credit reporting should be regulated under the general provisions of the Act and new credit reporting regulations…".[12]

While the ALRC recommended some significant changes to the credit reporting regime, in particular permitting additional information to be included in credit information files, the limits on the organisations permitted to access the system, and on the use and disclosure of credit reporting information remain. In reaching this view the ALRC noted, amongst other things, that in "the light of stakeholder comments and after further consideration, the ALRC considers that the proposal made in DP 72 to permit use and disclosure of credit reporting information for any related secondary purpose within the reasonable expectations of the individual concerned is unjustifiably broad".[13] The ALRC recommendations include:

- Basing the proposed simplified rules about the purposes for which a CRA or credit reporting agency may use or disclose credit reporting information on the existing rules; and
- Replacing the current offence provisions with a civil penalty regime based on serious or repeated breaches. [14]

[9] CRAs use of credit reporting and other personal information is subject to section 18S which prohibits unauthorised access to a credit file and the NPPs which limit the use of personal information to the primary purpose for which it was collected unless exceptions apply

[10] Section 18N(2) of the Privacy Act

[11] Sections 18S and 18T of the Privacy Act

[12] Media Briefing Note 7 ALRC Privacy Inquiry 11 August 2008 http://www.alrc.gov.au/media/2008/mbn7.pdf

[13] ALRC report paragraph 57.36

[14] ALRC report Recommendations 57-1, 59-9 and 50-2 see note 1 above

The Government is currently considering the ALRC's recommendations and is expected to provide its response later in 2009.

3.4 THE PROPOSAL

The PIA is considering the AGD suggested response to the ALRC recommendation, which is to amend the AML/CTF Act to authorise reporting entities and CRAs to use and disclose credit reporting information for the purpose of electronic verification of customer details. Such an amendment would in turn provide an authorisation under section 18K(1)(m) of the Privacy Act that would otherwise prevent the use/disclosure of credit reporting information for EV.[15]

The AGD proposal is that credit reporting information held by CRAs could be used and disclosed for EV under tightly prescribed arrangements and with associated privacy protections. The proposal as put to IIS for assessment in this PIA is that:

- A reporting entity would be able to send identification information provided by a customer to a CRA for a data match. A CRA, in receipt of such a request from a reporting entity, will be limited to confirming the accuracy of the information provided to them. This may be done through either a 'yes/no' system or a scoring system. The score would depend on how closely the information provided by the reporting entity matches with the customer information held on the credit file.
- A reporting entity will not be able to obtain any information from the CRA's file. The reporting entity will also be required to keep a record of the process used to verify their customer's identity.
- The information that can be matched would be limited to what is necessary to achieve verification under the AML/CTF Act – the customer's name, address and DOB.
- A reporting entity would only be authorised to send a request for electronic verification to a CRA with the consent of the customer.
- This proposal would also require credit reporting agencies to note an electronic verification inquiry on the customer's credit file and the outcome of that inquiry.

AGD has also noted that as reporting entities under the AML/CTF Act are subject to the Privacy Act a customer of a reporting entity that has released personal information to a CRA without proper consent would be able to access remedies under the Privacy Act. Part IIIA of the Privacy Act also creates a number of credit reporting offences, which include offences relating to:

- persons intentionally obtaining unauthorised access to credit information files or credit reports, and
- persons obtaining access to credit information files or credit reports by false pretences.

AGD considers that these offences should apply to reporting entities accessing credit reporting information for AML/CTF purposes.

[15] Section 18K(1)(m) of the Privacy Act sets out the circumstances in which CRAs may disclose credit reporting information. re is currently no authorisation for credit reporting information to be disclosed for the purpose of verifying identity under the AML/CTF Act

3.5 CURRENT EV SERVICES

Reporting entities are currently using EV to satisfy AML/CTF requirements to confirm "safe harbour" details against two independent data sources. They will normally use an EV service provider to undertake the checks rather than do this themselves.

There are a number of such service providers including Dun and Bradstreet, Veda Advantage and greenID. The former two are also CRAs. Each of these organisations briefed IIS as part of the consultations for this PIA. The three services are also described in detail in the May 2009 AML Magazine, Anti-*Money Laundering - Combating Money Laundering In Financial Services*.[16] According to the AML Magazine, each of the services uses a variety of public and propriety data sources in making their checks. The data sources mentioned include:

- the Australian Electoral Roll;
- Sensis White Pages;
- the Department of Immigration;
- the Department of Foreign Affairs and Trade watch lists;
- the Australia Post Postal Address File; and
- propriety databases such as the historical white pages, FCS OnLine Public Number Directory: derived from the Integrated Phone Number Directory (IPND), the Veda Advantage Identity Bureau Data, Veda Advantage Credit Bureau Data and Insurance Reference Service.

IIS understands that EV services use propriety algorithms to decide if the specified identity elements – name, address and DOB or three year transaction history – can be confirmed against at least two other data sources. As noted earlier, the ability to confirm DOB is currently limited.

The service offered by greenID also involves an element of "dynamic" matching in which individuals self-check their details by a process in which they are invited to logon to agencies and organisation with which they have an existing relationship. The greenID process allows it to confirm that the individual has been authenticated; it then feeds this information into its results. GreenID selects agencies and organisations that it considers have a strong legislative obligation to protect personal information and therefore are likely to have reliable data and to authenticate individuals to a high standard, for example Medicare. GreenID considers that its services offers privacy advantages, for example, in that the self-checking element is under the individual's control to the extent that they choose which organisations to approach and the authentication process is private.

The following brief extracts from the AML Magazine give a flavour of the matching processes, as described by the organisations themselves.

[16] www.amlmagazine.com.au

EV Service Provider	Matching process
Dun & Bradstreet	The methodology uses a scoring system and a set of conditional rules to corroborate the supplied customer information against, at minimum, two reliable and independent data sources. The D&B Identi-Check solution comprises numerous and varied data sources. To ensure that all datasets are considered in conjunction (rather than in isolation) for customer verification purposes, D&B applies scorecard methodology and creates compliance algorithms and business rules tailored for each individual risk situation.
Veda Advantage	Each record retrieved is assessed using a matching algorithm to evaluate how similar that record is to the identity data provided on input. This layer of logic ensures that the phonetically similar records retrieved during the search phase are reassessed in terms of actual similarity while making allowance for phonetic closeness. VeriCheck AML utilises comparison matching algorithms to assess the similarity between two given strings of data. It then returns a value that indicates the degree of similarity between these two strings. The matching and result calculation commences at data element level and concludes with the return of a number of high level summary match indicators. Each level is utilised to calculate the match result level above it.
greenID	Matching against the static databases is done within greenID using a matching algorithm to a standard set by the reporting entity as required under their AML/CTF program and risk appetite. Matching against dynamic databases is done by the government agency or department under their legislation and to their own standard (sufficient to safeguard the interests of the government, the taxpayers and the true owner of the identity that is seeking to be verified).

4 PERSONAL INFORMATION COLLECTION AND INFORMATION FLOWS

The following table sets out the potential information flows should the AML/CTF Act authorise the use of credit information (CRI) for EV. The table reflects IIS's understanding of the potential personal information collected, used, disclosed and retained by the participants in an EV process. It describes the process that may occur should the person consent to an EV process using CRI.

<table>
<tr><th colspan="4">Personal Information flows in hypothetical EV process under the AML/CTF Act both with and without use of credit reporting information</th></tr>
<tr><th>Person</th><th>Reporting Entity</th><th colspan="2">CRA as EV service provider</th></tr>
<tr><td rowspan="6">Person applies online – Asked to provides details
• Name
• DOB
• Residential address
• Others details ➔

Asked to consent to ➔
• EV involving CR information or
• Other EV
• Advised about off-line physical process</td><td>Reporting entity collects:
• Name,
• DOB
• Residential address
• Others details
• Person's preference re EV</td><td>CRA collects
• name, date of birth, residential address
• Reporting entity details
• Details of the EV request, time, date etc</td><td>CRA disclosures (other than to reporting entity in response to request) ➔</td></tr>
<tr><td rowspan="5">If consumer consents to use of credit information reporting entity discloses to CRA/EV Service Provider

• name, DOB, residential address ➔</td><td>EV process logs details above – retained for audit purposes, used for monitoring, improving scoring algorithm, matching sequences ➔</td><td>• to individual concerned
• to reporting entity, AUSTRAC or as otherwise authorised</td></tr>
<tr><td>Uses details collected to verify information against at least two independent data sources including credit information, using matching algorithm</td><td></td></tr>
<tr><td>➔response (y/n or score)</td><td></td></tr>
<tr><td>Records details of request and response in person's EV file, which can be accessed by individual, and disclosed for AML/CTF purposes</td><td>• to individual concerned
• to reporting entity, AUSTRAC or as otherwise authorised</td></tr>
<tr><td>If consumer consents to EV without the use of credit reporting information</td><td>EV process logs details</td><td>• to individual concerned
• to reporting entity, AUSTRAC or as</td></tr>
</table>

	reporting entity discloses to EV service provider • name, DOB, residential address ➔		otherwise authorised
		EV check excluding CRI	
		← response (y/n or score))	
		Record of check and response,	• to individual concerned • to reporting entity, AUSTRAC or as otherwise authorised
Individual considers response decides: • Not to proceed; • To provide additional information requested • To proceed with application by presenting physical documents	← advises applicant if EV successful or if further ID needed (could be further information for EV eg passport number) or if hard copy documents need to be presented		

5 PRIVACY ISSUES AND RISKS

5.1 APPROACH TO ANALYSIS

The ALRC inquiry process canvassed the possible privacy impacts of the proposal. IIS drew on this work to focus the PIA. It developed a brief consultation paper that outlined the AGD proposal and listed an initial set of issues including those canvassed by the ALRC. The consultation paper was then discussed with a range of stakeholders. The questions raised in the issues paper are included at Appendix 3.

The analysis below assesses the proposal taking account of:

- the views expressed in stakeholder consultations, as provided in meetings and submissions, including on the draft report which was circulated for comment;
- the requirements of the NPPs and Part IIIA of the Privacy Act;
- and broader privacy issues.

It focuses on the key issues raised by the policy proposal rather than a provision-by-provision examination of the privacy principles. The intention in the analysis is to identify the nature and extent of possible privacy issues and to make an assessment of the impact and possible mitigation options.

5.2 FUNCTION CREEP – EXTENSION IN USE OF CREDIT REPORTING INFORMATION

"Function creep" occurs when organisations, or governments, expand the purposes or functions for which personal information is used beyond those stated to be the purpose when personal information was first collected. Whether or not the expansions will be welcome or accepted by the community or seen as unwelcome "function creep" will depend on their nature and how they are made.

Submissions to the ALRC inquiry, including from the OPC identified the use of credit reporting information for EV as function creep and the ALRC report accepted this view. The next section considers a range of perspectives on this issue.

5.2.1 CASE FOR THE USE OF CREDIT REPORTING INFORMATION

The ALRC considered that an argument in favour of credit reporting information was that it was a regulated source that could be controlled. The Australian Privacy Foundation (APF) in its submission to this PIA process asked to what extent does access to credit reporting information solve the problem and what consideration of alternatives had been undertaken. It argued that the better approach would be to conduct a wider review of ID management. Stakeholders raised issues that could be part of a wider review. GreenID for example argued that government databases in general would be a more accurate and secure source of identity information.

5.2.1.1 ALTERNATIVES SOURCES OF DATA FOR EV

The ALRC considered this question in the course if its inquiry particularly in relation to DOB. ING provided a comprehensive survey of possible alternative sources including:

- Australian Government, for example, held by the Australian Electoral Commission (electoral roll); the Department of Foreign Affairs and Trade (relating to resident non-citizens) and Australian Securities and Investment Commission (ASIC);

- State and Territory Government, for example, registries of births, deaths and marriages and motor vehicle registries; and
- the private sector, for example, the Telstra Integrated Public Number Database.

ING considered that there were inadequacies with each of these data sources. It advised that it was unable to identify any comprehensive data sources of DOB that are able to support high volume, real-time electronic response.

In consultations with IIS the electoral roll was often mentioned as desirable source of DOB. The *Commonwealth Electoral Act 1918* currently authorises the use of the electoral roll to confirm name and address in specified circumstances including for EV under the AML/CTF Act. The Joint Select Committee on Electoral matters recently considered again whether the authorisation should extend to DOB. It decided against this noting that

> …the committee places a very high value in ensuring that, wherever possible, elector information should remain private and that there be no wider secondary use of such information. Such an approach is required to ensure that potential electors are not dissuaded from enrolling because they hold a perception that their information will be shared across a number of spheres for non-electoral related purposes.[17]

Another option raised was the Federal Government's proposed document verification service (DVS). IIS understands that the DVS will be a secure, national, real time, on-line system accessible to all authorised Australian Government, State and Territory agencies, and potentially by the private sector. It is intended that the DVS will allow participating agencies to verify that:

- a document was in fact issued by the document issuing agency claimed on its face
- the details recorded on the document correspond to those held in the document issuing agency's register
- the document is still valid (i.e. has not been cancelled or superseded), and
- the document has not been lost or stolen[18]

The DVS is not yet available for private sector use and IIS is not aware of any timeframe for this. In any event, the DVS is premised on individuals first presenting physical documents and so would not appear to support a fully online process. Some stakeholders, for example Abacus, did consider that the DVS could be a useful adjunct to an EV process.

Submitters to the ALRC inquiry also advised that DOB can be confirmed against state based Certificate Validation Services. However, the Australian Finance Conference is reported as considering this service "unreliable", in part because customers are less likely to have a birth certificate number readily available. Abacus also raised concerns about these services including that they are slow and expensive and less relevant given that the people now rarely use a birth certificate as identity.

[17] Joint Standing Committee on Electoral Matters *Report on the conduct of the 2007 federal election and matters related thereto* paragraph 11.91 available at http://www.aph.gov.au/house/committee/em/elect07/report2/Chapter%2011.pdf

[18] Report to the Council of Australian Governments on the elements of the National Identity Security Strategy - April 2007 available at http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_ReporttotheCouncilofAustralianGovernmentsontheelementsoftheNationalIdentitySecurityStrategy-April2007

In consultations for this PIA, Abacus also noted that if the government would make more of its databases available there would be less need to seek access to credit reporting information.

For the purposes of this PIA the conclusion seems to be that while there may be alternative sources of DOB information, none have so far been identified that are likely to be available or efficacious in the short term.

5.2.1.2 EV SUCCESS RATES

A question for this PIA is how the addition of credit reporting information to confirm identity details including DOB will affect the efficacy of EV services. Stakeholders consulted about the current rates of success for EV services gave quite varied responses. The variations appear to arise from a range of factors including reporting entities appetite for risk, the product the reporting entity is offering and the nature of the EV service. One organisation advised that in the case of a particular product it would not consider relying on EV unless it could directly confirm DOB. Others reported EV success rates from 30% - 80%, with a clustering in the 30% - 50% range.[19]

Dun and Bradstreet advised "the uplift could be significant, particularly for those in the younger age groups and / or newly arrived citizens. This situation will occur because new entrants to the country may not yet be on the electoral roll or the IPND however they may have applied for a mobile phone thereby creating a credit file. For this group in particular, the uplift could be up to ten percent."

While the basis for estimation and the estimates varied, most reporting entities and EV service providers anticipated that access to information held by CRAs would result in significant increases in success in confirming identity with the average success rates ranging from 60% - 80% again depending on the products and organisations concerned. Dun and Bradstreet, for example, advised in its further submission on the draft PIA report that its analysis indicated that the details of "an additional 36 percent of customers" could be verified using credit reporting information.

5.2.2 EXTENT OF FUNCTION CREEP

While the proposal does involve a new use of credit reporting information, it only affects a part of the information in credit files. The proposal does not directly involve the most sensitive elements of the information held by CRAs, that is, information about loan defaults or the detail of credit enquiries. However, in some cases CRAs may also use artefacts of individuals' credit history, for example, the age of a credit file would give an indication of "transaction history". The OPC noted in consultation meetings that it was less concerned if the checking process was limited to the three parameters noted in the proposal.

The ALRC put the view in its report that confirming identity details is an existing part of the credit system. While accepting that Part IIIA is not framed in this way, the ALRC considered that conducting a credit check as part of a risk assessment could be seen in part as an identify verification process.

It is the case that the proposal would permit a wider range of organisations to interact with CRAs. Reporting entities may also be credit providers, which are currently permitted access to credit

[19] The tables in the AML Magazine report EV service providers as indicating greater success rates of up to 98%. However, IIS understands these figures also depend on reporting entity products and risk appetite.

information, but extend beyond that to organisations offering services such as debit or stored value cards, money transfer or bullion dealers, payment services and on-line gambling.

However, the proposal would only permit these additional organisations to ask question of CRAs and to receive a response. The process would not reveal substantive information about an individual and non-credit providers would continue to be prevented from accessing the content of credit information files.

5.2.3 IMPACT OF THE FUNCTION CREEP AND WHETHER WELCOME

These are relevant consideration and are discussed in detail in the next part of the PIA.

5.2.4 POTENTIAL FOR FURTHER FUNCTION CREEP

The OPC raised one of the more difficult issues in considering function creep – that is, would taking the step proposed open the floodgate for other purposes. The APF and Liberty Victoria expressed similar concerns. The APF argued that should the proposal be adopted, the use of any further database for EV should be subject to a same level of scrutiny. IIS agrees that the potential for further extensions will be a risk.

IIS considers that the potential for further function creep in this case might be managed in two ways. The first is by minimising the amount of discretionary increment possible by administrative action, which IIS considers has been largely achieved by the carefully defined and narrow proposal that is the subject of this PIA. The OPC in its further submission notes this as an important plank in managing function creep.

The second approach is to ensure arrangements are in place, in this instance preferably in legislation that ensure the impact of any further change is properly considered including by PIAs and public consultation.

5.3 CONSIDERATION OF PRIVACY PRINCIPLES

This section considers the proposal taking account of the NPPs in the Privacy Act. In particular it addresses issues such as those that, for example, the OPC in its submission to the ALRC argued should be explored further before the use of credit reporting information was extended to include EV. The matters identified included: who has access; what information can be used and disclosed; what secondary uses would be permitted; and what safeguards, including individual access and notice/consent, would be needed.

5.3.1 COLLECTION OF PERSONAL INFORMATION

NPP 1 governs the collection of personal information by organisations and includes provisions aimed at limiting the collection of personal information to that necessary to fulfil lawful functions or activities and ensuring fair and lawful means of collection and that individuals have sufficient information to make informed choices about whether to proceed with the transaction. Part IIIA applies to the collection of credit reporting information and sets more specific rules including about what information may be collected in what circumstances. Part IIIA also provides that individuals should be told if a decision to deny credit on the basis of credit report.

5.3.1.1 EXTENT OF PERSONAL INFORMATION COLLECTED

The AGD proposal, as set out in section 3.4, limits the information that reporting entities provide to CRAs to name, address and DOB. While this gives comfort to some stakeholders including the OPC,

it raised questions for the industry stakeholders including the Australian Bankers Association (ABA) and Veda Advantage.

Veda Advantage noted that the ALRC recommendation referred to "credit reporting information" which, as set out at section 3.3 above, includes considerably more information than that listed in the AML/CTF Act.

Veda Advantage considers that the addition of a person's sex and previous addresses would "significantly help improve the quality of the matches". It also observes that if a match is weak or indeterminate then supplementary matching could result in a successful match. It advises that in overseas jurisdictions "a series of 'dynamic' questions can be asked directly and in a secure session between a CRA and a consumer ensuring that the CRA does not disclose information, and the consumer is simply responding to questions that the CRA already holds on them".

Veda Advantage proposes rather than specifying particular data items an outcomes based approach be adopted. For example it suggests outcomes such as the statement in the consultation paper "that the credit reporting information that can be used for matching is no more than directly required to achieve verification under AML/CTF Act" or that the verification process should not disclose information that is not already in the hands of the reporting entity or the consumer.

Veda Advantage also commented on this issue in its further submission on the draft PIA report. It suggested that an alternative would be to include a mechanism, for example a regulation under the AML/CTF Act made in consultation with the OPC, which would permit CRAs to receive and confirm additional information about an individual that may then lead to a successful match. The ABA also argued for flexibility in the information that could be checked in an EV process using credit reporting information; it suggested that individual consent would be an appropriate authorising mechanism.

IIS appreciates that the propositions by Veda Advantage and the ABA could have the potential to give EV systems more flexibility with greater matching success. However, they also appear to involve more extensive use (if not necessarily not disclosure) of credit reporting information than would be the case if the proposal is limited to confirming specified details. They may have other privacy impacts so far not identified and may impact on the EV market overall. Given the scope of this PIA and as the consultation to date has been based on the specific AGD proposal IIS is not in a position to make a finding about the privacy impact of these suggestions. It considers that further privacy assessment of a specific proposal would be needed before taking this approach.

5.3.1.2 Potential for organisations (including CRAs) to gain access to new information that they would not otherwise have had

IIS asked in the consultation process if the proposal could be characterised as allowing individuals to have their identity confirmed without *"any organisation gaining more information about a person than they would have had from current methods of identity verification".*

Reporting entities were inclined to say that from their perspective there would be no new collection of personal information. The APF considered that even reporting entities would be gaining some new information, for example, at a minimum whether or not the individual had a credit information file.

Bankwest noted that in the normal course of a credit check it would submit ID information (name address and DOB) as well as credit related data, to a CRA as part of a standard credit check. In this sense, a CRA is not getting information that it would not otherwise get. Part IIIA would also permit CRAs to add to and update credit information files using information provided as part of a credit check (or a default listing).

However, IIS agrees that as identified by the APF, CRAs could collect additional information in some circumstances. For example:

- The EV process will result in an electronic footprint or audit log which IIS understands would include the reporting entities' details and the ID details to be confirmed and which will also over time build a history of an individual's EV history;
- If the person does not currently have a credit information file, the person's name address and DOB and the fact that they are dealing with a particular organisation;
- Where the person does have a credit information file, and reporting entities are not credit providers, or do not use the CRA for credit checks, the fact that a person has a relationship with a particular organisation and possibly that the person's address details have changed or they are presenting a variation on their name.

Some stakeholders considered that updating records, for example adding a street number to a credit information file if the CRA did not hold this, should be prohibited. IIS understands that Part IIIA would prevent CRAs from creating or directly updating credit files as a result of an EV process. If is this is not the case, IIS considers that it would be an important protection.

As noted, the EV process could automatically generate an electronic footprint of the process. There is also the question about whether the CRA should make a record of the check, either as part of a credit information file or separately. While some stakeholders considered that it could be safer for there to be no record of any sort of an EV check, others considered that it would be important for CRAs to record the fact that a check had been conducted and details and results of the check. However, there was concern that if this sort of information was included in the person's credit information file that credit providers may draw inferences, for example from the number of EV checks undergone, or the nature of the reporting entity making the request. For example, the APF would be concerned if the use of credit reporting information for EV in anyway affected a person's ability to gain credit. It considered that where and how a CRAs records requests and results and these would be available to credit providers in context of credit reporting activities would affect the likelihood of harms. The OPC considered that it would be good privacy practice to keep a separate record that was not part of a credit information file but which would allow an individual to gain a clear view of the use and disclosure of personal information for EV.

IIS agrees with OPC that in the interests of transparency and accountability a CRA should be required to make a record of the facts associated with an EV check. Such a record would also assist an individual know what EV checks had been undertaken using their credit information file and to follow up any problems. IIS considers that this record should be available to the individual concerned. It considers that in line with the purpose of collection (to confirm ID) this information should not also be used in credit assessment processes. IIS understands that currently a record of an EV check would be excluded from the permitted contents of a credit information file – see section

3.3 – and so could not be made available as part of a credit check. However, if this is not the case, IIS considers this should be addressed in any legislative amendment.

IIS understands that CRAs would anticipate using the information collected and used in the context of EV checks, for example in audit logs, to monitor and improve the scoring algorithm and matching sequences. IIS considers that uses of this sort in the context of EV under the AML/CTF Act seem consistent with privacy principles. The risks in secondary uses arise where the use is for a different purpose or context that the individual would not expect and cannot control.

In its draft report, IIS suggested that a record of an EV check should include the result or outcome of the process; that is whether or not a match had been achieved. There was reasonable agreement on the industry side that this should not be done. Dun and Bradstreet, for example, noted that the fact that EV processes are risk based, and tied to each organisations' approach to risk, rather than having standard criteria for all reporting entities, means that it would be difficult for individuals to interpret the result. The OPC also took this view. It considered that the inclusion of the outcome of an EV check in the record might be prejudicial to the individual concerned.

IIS has taken account of these views. It considers that that it is on the whole reasonable to exclude the result from the record of an EV process. In particular, IIS notes that while the CRA conducts the EV process it does this on the basis of the parameters agreed with each reporting entity and it is the reporting entity that it responsible for deciding whether it is, or is not satisfied with the result and what it will advise the individual concerned. IIS therefore agrees that the EV record held by a CRA should not include the match results.

5.3.1.3 CONSENT

The consultation paper outlined the AGD proposal that "a reporting entity would only be authorised to send a request for electronic verification to a credit reporting agency with the consent of the customer".

Industry stakeholders were generally in favour of a consent element to EV, considering it would promote individual control and hence privacy. However, Abacus raised some concerns about an obligation to obtain consent. It noted that "this would raise procedural and record-keeping obligations and regulatory risk in cases where a request is accidently sent without consent" and suggested that this may deter reporting entities from using EV. Abacus put this position again strongly in its further submission on the draft PIA report. While noting Abacus's position, IIS considers that given general level of support from reporting entities and CRAs, and the general context including the sensitivity of credit reporting information, it is desirable for the proposal to proceed on the basis of freely given and informed consent.

The APF challenged the notion that consent would automatically increase individual control; it considered that this issue had not been sufficiently canvassed in the IIS consultation paper. The APF observed amongst the other things that seeking consent would be meaningless if a reporting entity did not offer an alternative online or offline means for an individual to authenticate their identity. The APF argued for an honest process so that if real consent were not possible it would be "more appropriate to require specific notice of the proposed e-verification (involving both disclosure and collection of personal information), and perhaps express acknowledgement of this by the customer." In its further submission on the draft PIA, Liberty Victoria again expressed scepticism about the

ability for a free and informed consent process, particularly if non-EV processes were withdrawn. As far as the question about alternatives to EV, IIS considers that these are likely to be available for at least a number of years. It considers that the potential for off-line identify verification to become less available should be reviewed in the context of the required review of the AML/CTF Act.

A number of other submissions on the draft PIA addressed consent. The ABA noted that reporting entities would need to develop new procedures to gain consent and that they may wish to seek consent for use (in identity verification) of all information disclosed by customers. GreenID argues that explicit, opt-in consent should be required.

IIS considers that if the choices available to individuals are easy to take up and supported by reasonably detailed information about the use and disclosure of the information and the alternatives available the consent process is more likely to be effective. It also considers that if individuals are to be able to exercise real choice the question of use of credit reporting information would need to be put separately from other consent requests. Preferably individuals should be advised that the EV process is risk based, that the process may not be successful for a number of reasons, given an indication of the databases involved, and advised how to find out more. IIS considers that it should be reasonably easy to design a simple process offering, for example, three choices with an explanation of the consequences of each. This might mean offering EV using credit reporting information with potential for higher success rates, EV without credit reporting information with less potential for success and an off-line alternative. IIS suggests that reporting entities test the process with consumers with the aim of designing a simple process that is as transparent as possible.

5.3.1.4 NOTICE ABOUT EV FAILURE OR REQUIREMENT TO UNDERGO FURTHER IDENTITY VERIFICATION

Stakeholders in the consultation process also discussed the possible safeguard of advising individuals if they "failed" EV. For example, the OPC considers that individuals should be told there has been a mismatch, although not necessarily the basis for the mismatch. There was some question about whether this would be contrary to the prohibition on "tipping" off in the AML/CTF Act; the OPC considers it would not be.

While there was general support for the notion that individuals should be aware they had "failed" a check so that they could take action, such as seeking a copy of their credit file to check the details, there were varying views about how much feedback would be needed or would be appropriate.

The discussions explored the option of giving detailed feedback, including about which databases, and which elements of the check had failed. There was some support for this but also downsides, including that this may add to the risk of ID fraud (by giving a fraudster leads on what elements of stolen identity needed work), that the process would be costly and that there was no similar requirement in relation to check conducted against other databases.

IIS appreciates that the approach to providing post-check notice in the EV context is complex. For example, where a person has met the EV check against the reporting entities own criteria, they may still be asked to provide documents or attend a site in person because of other risk factors. It also understands that the matching algorithms used are complex and may involve elements on more than one database. However, IIS considers that feedback advising of the EV failure, and some indication as to what follow up was needed or possible, would be in line with the obligation in Part

IIIA to tell people when making decisions based on a credit report and would also meet privacy better practice in relation to transparency and openness.

In its draft report, IIS suggested that, in addition to information provided to support requests for consent (see section 5.3.1.3 above), individuals should be given specific information about any significant mismatch, including which datasets are involved. It suggested that this sort of information could assist individuals to resolve problems, which in some cases may arise from serious inaccuracies or identity theft. The ABA in its further submission noted that deciding on the level of information to provide would be complex. For example, there will be a difference between a mismatch, for example where an address provided by the reporting entity does not match that held by a CRA, and a partial match, where there may be no address. In addition, providing detailed about the nature of the EV failure may facilitate identity fraud by pointing to records that needed to be altered.

While recognising the complexities IIS considers it should be possible to provide individuals with sufficient information about an EV failure to alert them to potential inaccuracies in records held about them. It considers that, if the proposal proceeds, further work, including testing options with individuals, should be undertaken to develop an appropriate response.

5.3.2 USE AND DISCLOSURE OF PERSONAL INFORMATION

NPP 2 governs the use and disclosure of personal information. The NPPs permit the use or disclose of personal information for the purpose for which it was collected unless a specified exception, including that the individual would reasonably expect the use or disclosure or has consented, applies. As noted in section 3.3, Part IIIA sets out specific rules about the use and disclosure of credit reports by credit providers and CRAs.

5.3.2.1 CRA USE OF CREDIT REPORTING INFORMATION TO CONDUCT EV CHECKS

A question for consideration is the nature of information CRAs would use to confirm and individual's identity. IIS understands that CRAs would propose to use the parameters of a credit information file, such as its age, on the basis that this would equate to "transaction history", if it is not able to obtain an acceptable match based on name, residential address and DOB alone. ING considers that this would add considerably to the efficacy of the EV process.

IIS understand that using the age of a credit information file would be consistent with the AML/CTF provisions and would be unlikely to raise additional privacy risks. The OPC in its further submission noted that it did not disagree with this position provided that there was would be no reference to the more sensitive information, for example as defined by section 18E that sets out the permitted contents of a credit information file.

5.3.2.2 POTENTIAL FOR SECONDARY USE OF PERSONAL INFORMATION BY REPORTING ENTITIES OR CRAS

The ALRC recommended that consideration be given to limitations on secondary uses of information obtained as a result of an EV process by reporting entities. In its consultation IIS asked the question as well in relation to CRAs.

The OPC submitted that that there should be secondary use restrictions particularly in relation to CRAs. It noted that CRA could be expected to seek new ways to add value to the information it holds that could fall outside of regulatory framework under the proposal.

Veda Advantage favoured permitting CRAs to work within the current NPP framework. It argued that a more restrictive regulatory response would be disproportionate, leading to regulatory arbitrage and preventing innovation and flexibility to respond. It also argued that a very strict secondary use limit would prevent it from using log data for monitoring and improving the scoring algorithm for its EV services.

IIS considers that there is a range of factors suggesting specific secondary use limitation for CRAs are warranted. These include the involvement of credit reporting information that historically has been subject to very specific protection and the difficulty, in the absence of a wider review of ID management, of assessing whether there are better alternatives from a privacy perspective. It considers that information obtained as a result of an EV process relying on credit reporting should only be used for secondary purposes directly related to EV processes under the AML/CTF Act.

Abacus raised the issue from the perspective of the reporting entities. It argued that it would be undesirable to include specific limitations from a reporting entity perspective because of the potential unintended consequences. There was also a general sense in the consultations that people currently fail EV for all sorts of reasons, and that a failure would simply trigger the reporting more questions or to go to a physical process. The ABA advised that banks do not attach risk ratings to the ID process and that they have little interest in blacklisting customers unless there is a real concern. They would therefore be unlikely to use EV results in risk assessment processes, or in creating blacklist.

However, IIS considers that it is reasonable to limit secondary uses of personal information collected or generated in the EV process, which in the case of reporting entities is likely to be a yes/no response or a matching score, to those directly related to EV processes under the AML/CTF Act.

5.3.2.3 Whether the use of a scoring system rather than a 'match/no match' response provides a more viable option for electronic verification.

IIS asked stakeholders to consider the privacy and other implications of a point scoring system rather than a yes/no response from the CRA. In this approach in response to a request for EV, the CRA would provide a score based on how closely the information provided to it matches information held on the credit file. The reporting entity would then determine whether the score was acceptable for the verification of identity.

The APF was interested in what discretion reporting entities/CRAs have to set tolerance levels, and whether this was specified in the AML/CTF Act.

Section 3.5 gives some information about how EV services conduct the matching process. In consultations Abacus, Veda Advantage and bankwest confirmed that the EV matching process is tailored to the risk appetite and other business needs of individual reporting entities in response to their compliance obligations under the AML/CTF Act. Reporting entities advised that without a graded score it is not possible for them to understand the extent of the mismatch and therefore to meet their obligations under the AML/CTF Act to make decisions about customer risk.

Industry stakeholders argued strongly for a scoring system. The ABA and banks that participated in the consultation advised that a yes/no response is not supported as it implies an exact match. The National Australia Bank advised in its submission that a yes/no approach would rule out more people. A subtle difference in information could result in a failed match, for example on a yes/no

system variations such as Bill/ William or Street /Road may be rejected when the reporting entity may deem it to be a satisfactory risk based match.

The OPC noted it had previously argued for yes/no on the grounds that reporting entities would draw the wrong inference; in consultation it indicated it would reserve its view on scoring until understanding more of the scoring process. The OPC notes that the scoring process (including algorithms) is likely to be commercial-in-confidence and appreciates that the detail of score would not be accessible to an individual. In its further submission on the PIA draft report the OPC indicated that if a scoring model was adopted, it should not mean that individuals would be prevented from identifying that inaccurate information had been used in an EV process and seeking to correct it.

IIS considers that on balance it is reasonable to support the proposal on the basis of a scoring approach provided that this does not prevent individuals from becoming aware of inaccuracies in information held about them.

5.3.3 Accuracy completeness and currency of credit reporting information

Accuracy of information, and the ability to seek correction to information that is not accurate are important aspects in ensuring that the handling of personal information is privacy protective. NPP 3 requires organisations to take reasonable steps to make sure personal information is accurate, up-to-date and complete. There are similar requirements in Part IIIA.

IIS asked stakeholders for their views about the accuracy of credit reporting information for EV purposes and the potential for this to mean that individuals unfairly fail EV. Stakeholders did consider the question of database accuracy, and options such as notice of failure. Participants in the both industry meetings noted that if a match fails at an EV service provider, the issue may be with credit reporting information or with another data source; the problem exists independently of credit reporting. The question about the accuracy of CRA information is a narrow segment of a wider EV question, the present quality of EV means that people find it hard to verify ID via EV.

IIS notes that stakeholders indicate that successful EV rates are fairly low and reporting entities expect that permitting use of credit reporting information will increase matches significantly.

CRAs consulted are confident that their data are increasingly accurate. Dun and Bradstreet report difficulties in an EV process that require a manual correction affect about 2% of matches.

The APF, Liberty Victoria and OPC are wary about the accuracy of CRA records. The OPC noted even a low percentage of record will mean very many individuals are affected. Anecdotally IIS understands that the Consumer Action Law Centre considers that there are fewer problems with CRA information than there have been in the past and that in any event inaccuracies tended to be in the content of credit information files rather than in identifying information. GreenID is also wary. Its view is that government databases more likely to be accurate than those held in the private sector.

Reporting entities and CRAs also noted that given that Australians are relatively mobile, there would often be discrepancies in address information and to a lesser extent in name. DOB is static (and some organisations would only accept a 100% match here). Abacus reported mixed views amongst

members as to the accuracy of CRA information. However, it considers CRAs will have a "powerful incentive to ensure their data is accurate and reliable".

Participants in the Gambling Industry meeting consider that CRA information is sufficiently accurate to be useful in the mix and that in fact CRA information would add to accuracy. This meeting noted that currently some data sets are better than others, for example drivers licence sets produce more accurate address information.

The finance industry meeting noted that a fairly in-depth review Veda database had been conducted and it is not perfect but reasonable. Bankwest notes that the AML/CTF rules require reporting entities to assess reliability of data sources, taking into account accuracy, security and methods of keeping the data up to date. It has performed extensive due diligence and is satisfied that the data its chosen EV service provider uses is of sufficient standard for use in EV.

Taking account of discussion in relation to other aspects of this PIA, IIS considers that the credit information held by CRAs is likely to be sufficiently accurate to include in EV processes.

5.3.4 Security of personal information

NPP 4 requires organisations to take reasonable steps to protect personal information from misuse and loss and from unauthorised access, modification or disclosure. Part IIIA contains similar requirements.

A few stakeholders raised the question of the security, particularly in the course of transmission of customer records for EV. The concern was reporting entities might be transmitting information via insecure channels. IIS considers that this is an area of risk but it does not appear that permitting the use of credit reporting information would add significantly to the risk. However, it considers that both CRAs and reporting entities would need to consider security when setting up EV arrangements.

5.4 Consequences of rejection/failure including blacklists or other EV harms

IIS asked stakeholders to consider if a failure to successfully verify an identity electronically using credit reporting information could have other consequences besides being directed to other means of identity verification. For example, it asked if it could result in an individual being "black listed" or put on a watch list or in other harms.

APF and Liberty Victoria were concerned about the possibility of blacklisting individuals – that is denying them a service only on the basis of a fail on an EV process. They saw a need for active measure to prevent this, for example a requirement to offer an alternative process should EV fail, or a legislative prohibition against such a practice.

Industry stakeholders were unanimous in asserting that this sort of blacklisting would not happen. They advised that there are many reasons for an EV fail and that no inferences are drawn, rather people are simply referred to another process. A number of stakeholders, including ING and PayPal indicated that if people fail EV, they tend to drop out of the process rather than pursing a physical ID authentication process. Abacus is comfortable with a requirement to offer an alternative process but considers there is no evidence of blacklisting. Veda Advantage advised that it had looked at the UK experience and noted that there had been very few complaints and no prosecutions or civil actions. It considered this indicated the likelihood of harms is low.

Liberty Victoria observed that while alternatives may be offered now, people may have fewer options, for example if reporting entities charge more for off-line process or only offer EV.

The APF also considered that EV processes, which carry the connotation of passing or failing, might start to constrain how individuals present their identity. The APF considers these processes could start to assume there is only one correct combination of name and address for a person and they have to use this in all circumstances. IIS considers this is certainly an issue that deserves consideration. At present there appears to be a tolerances for variations in how ID is presented in an EV context. For example, the use of "fuzzy" matching and scores rather than yes/no approaches accommodates at least some variation, and, as discussed earlier, the main consequence of an EV failure is the offer of an alternative process. There are also options, such as the greenID process, which allow individuals in part to self-authenticate, using whatever form of their details is appropriate to the agency concerned.

However, IIS considers that this could be an issue as use of EV processes expands and depending on how the market expands; the issue could be considered as a part of a wider review of ID management.

IIS considers that at present there appears to be a low risk of blacklisting. It also appears that there would be a high likelihood that individuals would have an alternative processes at least in the short term. However, IIS considers that these settings could change quickly as EV becomes more widespread and if it becomes so reliable that few people need to use an alternative process. It considers these matters should be reconsidered, possibly in the context of the required review of the AML/CTF Act in 2013.

5.5 IMPACT ON INDIVIDUAL CONTROL OVER THEIR PERSONAL INFORMATION

The consultation paper asked stakeholders to consider the proposition that the proposal will not reduce the control an individual has over their personal information and may increase protections around it for the following reasons:

- The proposal requires a reporting entity to gain the individual's consent before using credit reporting information to verify identity for AML/CTF purposes.
- An individual can choose to use off-line means of identity verification if they do not wish to give their consent.
- Access to and use of credit reporting information is regulated by Part IIIA of the Privacy Act, and this includes offences for unauthorised access to credit reporting information;
- Current online identity verification schemes may not seek individual consent before accessing databases containing identity details about them;
- Current online identity verification schemes are only regulated by the more general provisions of the Privacy Act, and these do not include offences for unauthorised access.

Industry stakeholders were inclined to conclude that individuals would have the same or increased levels of control under the proposal. They noted factors including: the emphasis on consent; benefits including convenience, cost savings and viable on-line alternatives for rural and remote communities; and the potential for greater feedback to consumers about EV failures. The finance industry meeting considered that effective EV would mean individuals would have less need to

provide identity documents to an agent or mortgage broker; again positively affecting individual control. These stakeholders also saw that EV may be a useful addition to paper based processes where additional checks are needed for high risk people or products and could provide another option to KYC, to get the person over the line.

Veda Advantage also considers that the proposal would not affect individual control. Its view, as put to the ALRC, is that EV using credit reporting information is likely to be within an individual's "reasonable expectations". Veda Advantage also emphasised that the ALRC concluded that EV processes are less harmful and intrusive than document based processes. Liberty Victoria also considered that EV processes might be less intrusive in some respects.

On the other hand, greenID considered that its processes that rely on Government 2.0 technology allow for greater privacy and control for individuals.

Privacy advocates and the OPC were less sanguine about the impact on individual control. As noted earlier, the APF queried aspects of the EV process including whether consent could be informed and freely given and the impact on the wider ID management approaches. The APF, Liberty Victoria and the OPC also queried the extent to which Part IIIA provisions would apply where reporting entities are not also credit providers (discussed in section 5.7 below). The OPC also identified possible gaps in coverage in the Privacy Act (discussed in section 5.7 below) as affecting individual control. Liberty Victoria reiterated its concern in its further submission on the draft PIA that it considered that the points noted above could be inaccurate or misleading, for example, if the consent processes were inadequate or if in the future there are no viable alternatives to EV.

Taking account of the issues canvassed here and elsewhere in this PIA, IIS considers that the proposal if implemented appropriately could enhance the control particular individuals have in relation to EV processes. However, again considering the range of issued identified in this PIA, IIS considers there are potential risks at the overall system level. This view is reflected in the section 6 on findings and recommendations.

5.6 Dispute resolution and other safeguards

5.6.1 Dispute resolution

IIS asked stakeholders to consider the ALRC recommendation that reporting entities should have processes in place to resolve mismatches between the information individuals provide and credit reporting information.

In general, stakeholders agreed that individual access to appropriate dispute resolution was an important safeguard. There was a general view particularly amongst industry stakeholders that existing channels were likely to be sufficient; Abacus in particular argued against a prescriptive approach. Veda Advantage noted that in the UK only a handful of matters have gone to dispute resolution.

IIS understands that the most likely dispute resolution channels would be the OPC, or industry dispute resolution bodies such as the Banking and Financial Services Ombudsman. It notes that the ALRC has recommended as part of its review of credit reporting arrangements that CRAs should be required to join industry dispute resolution schemes. The OPC also noted these channels.

IIS considers that key factors in effective dispute resolution in relation to individual concerns about an EV process involving credit information are:

- The likelihood that individuals will be aware that there may be problem;
- The likelihood that individuals will know which organisation to approach and how to contact them; and
- That is an appropriate independent channel available if they are not able to resolve the issue with the organisation.

The discussion at section 5.3.1.4 above identifies that individuals should be given feedback where they fail an EV process. In its draft PIA report, IIS also recommended that where individuals who failed an EV process are not offered an alternative process to verify their identity that they should be referred to a dispute resolution body.

Industry stakeholders including the ABA, Abacus and Veda Advantage were not in favour of this proposition. They considered that it would be onerous and moreover may be inconsistent with the AML/CTF Act objectives.

IIS remains of the view that referral to a dispute resolution body should be included as a safety net option. It understands that reporting entities would offer alternatives ID processes in most cases, and in any event, the option for an individual to raise an issue with a dispute resolution body would already be available.

5.6.2 Other issues

5.6.2.1 Access to file by an individual

The OPC's submission recommends that the individual should be able to obtain a copy of their "EV" file so that they can verify who has accessed it and whether there are any errors. It also suggests that CRAs should be required to take reasonable steps to correct the file so that it is accurate, up-to-date, complete and not misleading, and in specified circumstances, attaching a statement to the EV file at the request of the individual. IIS agrees that these would be important privacy protections. It understands that individual access and correction rights would be available under NPP 6.

The OPC also suggests that access to an EV file should be reasonably free of charge as is currently the case for credit reporting purposes.[20] IIS agrees that this would be a reasonable approach given that the EV process relies on credit reporting information.

5.6.2.2 Retention of EV information

The OPC has recommended that the retention periods for information in an "EV" file (other than name, address and DOB) follow the approach in Part IIIA, rather than in the AML/CTF Act. In particular it suggests that the retention of the following types of information should be limited to five years on the file in line with the general credit reporting provisions:

- e-verification inquiry on the customer's file (including date of inquiry and name of reporting entity); and
- Date of disclosure by the CRA and to whom disclosed;
- Legislative protections and other safeguards.

[20] *Credit Reporting Code of Conduct*, clauses 1.7 and 1.8 see http://www.privacy.gov.au/materials/types/download/9254/6787

IIS considers that unless there are policy reasons arising from the AML/CTF regime to keep EV records held by CRAs for longer than five years, this should be the applicable retention period. AUSTRAC in its further submission indicated a preference for the seven year retention period to apply and observed that as there were already some variance in retention periods in Part IIIA this would not impose new or unreasonably onerous requirements on CRAs.

5.6.2.3 Application of the Privacy Act to reporting entities

The OPC considers the proposal to permit reporting entities to verity identity should be accompanied by assurances that individuals will be able to access remedies under the Privacy Act if as a result their personal information is mishandled. The OPC notes that the provisions deeming reporting entities as organisations under section 6E(1A) of the Privacy Act is in relation to the activities carried on by a small business operator for the purpose of complying with the AML/CTF legislation. However, it is unclear if personal information collected, used or disclosed by a reporting entity (not otherwise subject to the Privacy Act) for AML/CTF purposes would continue to be protected by the Privacy Act if the reporting entity later used, or misused it for non AML/CTF purposes. The OPC is seeking a broadening of coverage of reporting entities that are small business operators to ensure that individuals will have a remedy if personal information collected for the purposes of the AML/CTF Act is mishandled whether or not the mishandling relates to compliance with the AML/CTF Act.

IIS considers that this is an important issue and that should the provisions deeming reporting entities not act to protect personal information collected for the purposes of EV under the AML/CTF Act in all circumstances then there should be an amendment to the Privacy Act to address this.

5.6.2.4 Part IIIA coverage

The consultation paper indicated that an additional protection in relation to the use and disclosure of credit reporting information for EV would be the provisions in Part IIIA that prevent unauthorised access to credit information whether held by a CRA or a credit provider with strong penalties applying.

These prohibitions apply to any "person" and so apply to all reporting entities, whether or not they are also credit providers. However, as indentified by the OPC, these provisions will not apply to personal information that is derived from credit information but which is held outside the credit reporting system. This appears to be the case in relation to the information generated as result of an EV process (including the reporting entity, information matched, and result of the match) held by a CRA, and the result of a match held by a reporting entity.

The OPC suggests that the solution here is to introduce civil penalty provisions in the AML/CTF Act to support prohibitions on:

- Accessing a file held by a credit reporting agency containing information relating to AML/CTF e-verification; and
- Using and disclosing information for all secondary purposes obtained from electronic verification (which should also cover a credit reporting agency).

IIS understands that the intention here is to ensure that individuals do not loose privacy protections because of the extension in the use of privacy protections and to protect against further "function creep".

IIS notes that the information held in an EV context, presuming as discussed elsewhere that it is held separately from credit information files, will not include any information about loan defaults or a person's ability to manage credit. However, there are still sensitivities to consider.

The main additional personal information held by reporting entities as a result of an EV process using credit reporting information will be whether or not the match was successful. Reporting entities would also hold this information where EV does not use credit reporting information. IIS does not consider this information in the hands of reporting entities needs additional protection other than to limit secondary uses.

CRAs are likely to hold more detailed information including the reporting entities seeking the check, the matching algorithm used, and the result. Over time this could start to build up a detailed picture of an individual's activities. IIS notes that where CRAs provide EV services not involving credit reporting information they may be hold similar information about an individual.

IIS considers limitation on further uses of this information would be one response to managing the risks, given that the information derives from credit reporting information.

IIS notes that the ALRC has recommended the removal of the Part IIIA offence provisions and relying instead on increased powers for the Privacy Commissioner, including seeking civil penalties. IIS considers that the question of the need for offences be considered taking account of any changes to Part IIIA and the alternative enforcement options under the AML/CTF Act.

5.7 BALANCING BENEFITS/COSTS TO THE INDIVIDUAL AND THE COMMUNITY FROM THE PROPOSAL

IIS asked stakeholders to consider if:

- the proposal was likely to result in economic and privacy gain for both individuals and the community, for example though greater convenience and cost reductions and or by encouraging innovation in online service provision; or
- there could be some undesirable consequences including focussing EV on credit reporting information or economically marginalising people without credit histories.

Reporting entities considered that there was likely to be clear benefits for both individuals and business. Abacus suggested that the ALRC had already answered the question. Particular factors mentioned included the lower cost of EV compared to document based verification, the benefits to people living in remote communities without access to a bank branch and the benefit to business that do not have a physical presence. Industry stakeholders also noted that people who fail EV regularly drop out of the process leading to loss of business. AUSTRAC considered that if privacy can be properly protected there seem to be more benefits over costs. Treasury had a similar view.

Liberty Victoria acknowledged that an electronic process may be less intrusive than a paper based process. However, in its further submission is notes that there is dispute about the extent to which the use of credit reporting information for EV processes will helpful and it queries whether there is sufficient benefit to proceed. Veda Advantage noted that the ALRC had considered EV less harmful from a privacy perspective than a document based process.

However, Veda Advantage also flagged its concerns with the approach proposed that may mitigate benefits. For example it consider that a detailed and limited proposal would be disproportionate to the privacy risks, would lead to regulatory arbitrage and would undermine competitive neutrality.

The APF noted there might be advantages in replacing unregulated EV processes with regulated processes.

The OPC noted that the Government agreed in principle with amendments subject to strong privacy protections being in place.

Taking account of the range of views expressed and its own analysis IIS is inclined to consider that there are potentially considerable benefits from the proposal. IIS considers there are privacy risks and that these are largely manageable. The question that is more difficult to assess is the longer implications for identity management process including EV.

6 FINDINGS AND RECOMMENDATIONS

The issue that drives this PIA is the need to find a reasonably trustworthy, reasonably technologically accessible source of information about DOB to add to existing sources of information used by EV services or processes, in order to meet electronic identity verification requirements under the AML/CTF Act.

The policy development process, including the ALRC's review of the Privacy Act, has led to the conclusion that in the current environment DOB held by credit reporting databases would add considerably to the utility of EV systems. In the AML/CTF context this cannot be ignored.

IIS also notes that there is currently one EV service provider, and potentially others, offering alternative approaches to identity verification. However, it was beyond the scope of this PIA to consider the privacy risks in other EV models. IIS has also briefly considered other sources of DOB information that could be included in an online EV system including:

- State and Territory registers of births, deaths and marriages;
- The Australian Government's DVS;
- State and Territory registers of drivers' licence and motor vehicle registrations;
- The Electoral Roll; and
- Australian agency databases of information about citizens including the ATO, Medicare and the Passports Office.

For a range of reasons these data sources are not currently available or are not viable for EV services. These reasons are discussed in section 5.2.1.1 above.

In the course of this PIA IIS has identified a number of areas of privacy risks that may arise should identity information held by credit reporting databases be made available for AML/CTF EV. These are:

- "function creep" meaning that the proposal extends the use of credit reporting data beyond that currently permitted by the law and expected by the community, potentially undermining community trust in credit reporting and, for example, willingness to consider other changes to the credit reporting system;

- the potential for the identity confirmation process to create new data about individuals that could then be used for new purposes, which may or may not be with the knowledge of the individual concerned and may or may not be to the advantage of the individual concerned;

- the potential for individuals to be disadvantaged if they "fail" the EV process should it involve the use of credit reporting information, for example because of inaccuracies in the information held by CRAs or because of the nature of the checking process, without inadequate advice or recourse;

- the extent of choice that individuals have in the process, for example about whether to provide paper documents in a face-to-face identity verification process or to proceed with electronic verification and if the latter to choose whether or not to have credit reporting information included as part of an EV check; and

- the extent to which CRAs or reporting entities might either incidentally or otherwise gain access to personal information beyond what is necessary for the purposes of identity verification for AML/CTF purposes and who bears the risk when problems or mistakes with electronic verification system arise.

IIS recognises that the proposal as given to it for conducting PIA has been crafted with considerable effort to minimise privacy impact including by minimising changes to the credit reporting system. The measures to minimise impact include:

- only allowing access to identifying information held by CRAs for the purpose of verifying name, residential address and DOB to proceed with the consent of the individual concerned;
- only allowing the EV process to return a yes/no response or matching score and no other information; and
- not permitting secondary use of information obtained as a result of a matching process.

IIS notes that some industry stakeholders consider the proposal as framed is quite restrictive and as such is not a proportional response to the privacy risks identified. However IIS considers that a more open approach would raise possibly different privacy and policy issues and would need to be subject of a further review and consultation process.

IIS considers that the proposal as circulated raises some significant privacy issues and that these need to be addressed. However, IIS considers that if the proposal is introduced in the limited way set out in the AGD proposal, and subject to the recommendations it makes in this PIA, then on balance the proposal is likely to have reasonably significant benefits, including privacy benefits, to individuals and the community.

6.1 FINDINGS

Finding 1 – use of credit reporting information for EV

IIS finds that the proposed expansion in the permitted uses of credit reporting information to allow it to be used for EV is likely have practical benefits for individuals needing to establish identity so that they can transact online. IIS finds that the proposal does involve the use of the credit reporting system beyond its current parameters albeit in a limited way and in this sense is a significant departure from the legal "promises" made in relation to the disclosures of information from the credit reporting system. Rightly or wrongly, personal information collected in the context of the credit reporting system traditionally has been considered particularly sensitive and has been afforded special protections.

IIS concludes that the proposal could therefore be considered to be "function creep". Amongst the possible consequences of the proposal are that:

- it could be seen as opening up the system to pressure for further uses; and
- it has the potential to start to change the nature of CRAs by increasing their view of aspects of an individual's life beyond their use of credit.

However, on balance, IIS finds that it is that it is reasonable to proceed with the limited proposal that is the subject of this PIA so long as some additional measures are instituted to address the impact on individuals and to limit any possible systemic impact of the changes.

Finding 2 – EV processes involve new collection of personal information

IIS finds the proposal would result in reporting entities gaining some new information about individuals; for example, the reporting entity will know whether or not the individual has had previous dealings with a CRA.

IIS also finds that, should CRAs retain any record of the EV matches they have conducted, the proposal would result in CRAs holding new information about individuals. Depending on the way the checking process is undertaken and the nature of records kept this could result in quite a detailed set of information about an individual's activities, for example the frequency and nature of interactions with reporting entities.

Finding 3 – information to be disclosed to CRAs for an EV match using credit reporting information

The proposal under consideration in this PIA reporting entities would be limited to disclosing to a CRA only the minimum information necessary to achieve verification under the AML/CTF Act – the customer's name, address and DOB.

IIS has conducted its assessment on this basis and finds that limiting the amount of information to that necessary to achieve verification is consistent with privacy principles.

IIS notes that some industry stakeholders consider that the current proposal is too limited in that the identity elements mentioned, which are the minimum requirements under the AML/CTF Act, will not be able to be matched with sufficient certainty in many cases. They argue that permitting reporting entities to disclose more details about an individual, for example, their gender, their employers name, and/or previous addresses, would result in more successful EV processes and so would benefit the individuals concerned. The industry stakeholders suggest two mechanisms to authorise reporting entities to disclose additional information to CRAs for the purposes of EV matches using credit reporting information as follows:

- disclosures could be consent based and this consent would not override other prohibitions on the use or disclosure of the information; or
- a regulation under the AML/CTF Act made in consultation with the OPC, which would specify additional information that reporting entities could disclose to CRAs for the purposes of an EV process using credit reporting information.

IIS considers these proposals may have merit but would need to be the subject of a further review and consultation process.

Finding 4 – Use of credit reporting information for EV subject to consent

While IIS agrees that individuals should have choice about whether or not an EV process should include a check against data held by a CRA, it finds that in practice there is likely to be a risk that "consent" could become token if individuals do not have genuine alternatives available to them and if the consent process is not constructed so as to give individuals the opportunity to exercise free

and informed choice. This could happen, for example if the consent to a CRA check is combined with a consent to check other data sources, or if individuals are not well informed about the checking process. IIS considers that measures will be needed to ensure that the consent process operates to give individuals real choice. These measures could include:

- ensuring that individuals have the opportunity to agree or disagree to the use of credit reporting information for EV separately from any other consent they may be asked to give, and that the choice process is clear and easy to exercise; and
- providing reasonably detailed information about the EV process, including that it is risk based, the possible outcomes, the EV service provider used and the alternatives available.

Finding 5 – EV results can be reported as a matching score rather than only on a yes/no basis

In the course of the PIA IIS considered the option of reporting a match as score rather than on a yes/no basis.

IIS finds that the use of a scoring system is likely to increase the efficacy of the use of CRAs for EV in that individuals may be more likely to pass a reporting entity's EV requirements, which are based on its own assessment of what is appropriate, for example given the nature of the product and client profile, to meet its obligations under the AML/CTF Act. A possible benefit to individuals and reporting entities is that this would reduce the need for a document verification process (which requires documents to be presented by mail or in person).

IIS finds that the use of a scoring system will not add significantly to individuals' privacy risks provided that:

- the recommendations in this PIA report are adopted; and
- CRAs are required to provide the result as one score rather than a line by line score which would reveal details of the elements of ID that failed the matching algorithm;

Finding 6 – Secondary use of information obtained during an EV process using credit reporting information

IIS finds that CRAs should be prevented from using either the factual details associated with a match or the results of the match for any purposes that is not directly related to EV matching under the AML/CTF Act.

Finding 7 – CRA to retain a record of EV checks separate to credit information files

IIS finds that there are arguments both for and against permitting CRAs to retain any record of information it collects as part of an EV verification process. Depending on what is kept and what is then made available to the individual concerned, the record may provide useful insights in identifying where there may be a record accuracy issue. Some record may also be needed as part of appropriate transparency and accountability protections for individuals, reporting entities, and the AML/CTF system. On the other hand the richer the data trail the more attractive for other uses by CRAs or others. It has also been suggested that including the outcome of a match in an EV record may also be prejudicial and/or misleading to the individuals concerned. Elsewhere IIS has found that the responsibility for advising the outcome of an EV process lies with the reporting entity.

IIS finds that CRAs should keep a record of the use of credit reporting information for EV purposes. It considers that potential privacy risks will be minimised if the EV record is not included as part of a credit information file or report, and is not used or disclosed for any credit reporting purposes including to up date credit information held by CRAs.

IIS finds that on balance the EV should contain sufficient information to ensure the individual can correct any inaccurate information but should not contain the results of a match.

Finding 8 – Alternative processes need to be available

IIS observes that under current EV arrangements significant numbers of individuals are not able to have their identity confirmed via an EV process and therefore needs to be invited to provide further information or be directed to an alternative, document based, ID verification process. The EV failure may be for a range of reasons including that:

- the individual is not listed on a database;
- there are legitimate variations in details provided to the reporting entity and those held on a database because the individuals uses different details in different circumstances, has changed some details etc;
- there are errors in the data sources or in the matching process; or
- the reporting entity considers that there are factors about the product it is offering, or the particular transaction that may raise risks in terms of the AML/CTF Act and it therefore requires further identity checks whether or not the EV process was successful.

IIS finds that the privacy risks in the use of credit reporting information for EV purpose will increase if there is not an alternative method of ID verification readily available.

Finding 9 – reporting entities to advise individuals about the outcome of an EV process

IIS finds the addition of CRAs to EV processes could make it more difficult for individuals who chose to do so to track down the reason for an EV "failure". It considers that measures that may assist in the mitigation of this risk include giving individuals to detailed information about the EV process at the point of entry to the process and about the outcome of EV matching processes where there has been an EV failure, in particular in relation to credit reporting information.

IIS acknowledges that there are difficulties in establishing an appropriate form of advice for individuals about EV failure. For example, there may be a range of reasons for the failure including that there are variations in the information presented, that no information is held to match against, or that, given the particular risk circumstances considering AML/CTF requirements, the reporting entity considers it needs additional information to assure it of a person's identity. In addition, providing detailed about the nature of the EV failure may facilitate identity fraud by pointing to records that needed to be altered.

Nevertheless IIS considers it should be possible to provide individuals with sufficient information about an EV failure to alert them to potential inaccuracies in records held about them or to possible identity fraud or other problems. It considers that, if the proposal proceeds, further work, including testing options with individuals, should be undertaken to developed an appropriate response. This work should be undertaken by AGD in conjunction with reporting entities and will need to balance

the concerns of reporting entities and the need to alert individuals to the possible need to follow up possible inaccuracies in source records or other difficulties.

Finding 10 – Credit reporting information sufficiently accurate for use in EV processes

It goes without saying that all data holdings contain inaccuracies. IIS finds that inaccuracies in credit reporting information held by CRAs should not prevent this information being used in EV processes, provided that processes are in place to ensure transparency, accountability and resolution of disputes.

Finding 11 – Coverage of the Privacy Act

IIS understands that there is some uncertainty about whether the provisions deeming reporting entities as organisations under section 6E(1A) of the Privacy Act in relation to the activities carried on by a small business operator for the purpose of complying with the AML/CTF legislation are broad enough to protect personal information collected for AML/CTF purposes in all circumstances. In particular, there may be a gap if a reporting entity (which is not otherwise subject to the Privacy Act) uses, or misuses, this personal information for non- AML/CTF purposes.

IIS finds that if this is the case there would be a privacy risk unless individuals can be assured of their ability to access remedies under the Privacy Act if their personal information is mishandled in these circumstances.

Finding 12

IIS finds that there are a number of issues raised in the course of this PIA that point to the need for a wider review of ID management. These include:

- that the addition of credit reporting information to the EV process will not solve all problems and so there may be additional call for access to more databases, or for additional use of credit reporting information;
- that this PIA was not based on a detailed examination of the privacy impact and utility of alternative ID processes, or data sources including those held by government; and
- the potential for the narrow nature of the proposal being considered in this PIA, if implemented, to limit other innovations in EV processes.

6.2 RECOMMENDATIONS

IIS has considered the issues in this PIA through the lens of its "layered" defence framework. At this early stage, the emphasis in the recommendations is on establishing the legal and governance framework that will build in strong and sustainable privacy protection from the start. The recommendations below are grouped by the relevant layer in the IIS framework.

6.2.1 RECOMMENDATIONS RELATING TO THE LAW

Recommendation 1 - Consent

IIS recommends that, if the proposal proceeds, the enabling legislation must provide that an EV process using credit reporting information should only proceed with the consent of the individual concerned and that a request for consent should be made separately from requests for consent for

any other activities, should be easy to exercise and should be informed by detailed information about the EV process including that:

- an EV process may not succeed, or may not be sufficient, for a number of reasons because of the nature of risk bases processes allowed under the AML/CTF Act;
- the likely databases involved;
- how to find out more about the databases; and
- the alternative identity verification mechanisms available.

Recommendation 2 – Details to be checked in an EV process using credit reporting information

IIS recommends that, if the proposal proceed, the enabling legislation permit reporting entities in seeking EV using credit reporting information to provide only an individual's name, residential address and DOB to a CRA and that the CRA be permitted to use credit reporting information only to confirm the accuracy of these details on the basis agreed between the reporting entity and the CRA.

Recommendation 3 – Results reported on a yes/no basis or as a score

IIS recommends that if the proposal proceeds that it should be on the basis of a legislative amendment specifying the information that CRAs would be permitted to provide to reporting entities. This should be limited to the results of a match, which could be reported on a yes/no basis or as a score as agreed between the reporting entity and the CRA.

Recommendation 4 – Separate individual EV record

IIS recommends that if the proposal proceeds, the enabling legislation should require a CRA to keep a separate record of EV attempts it has processed in relation to an individual and that the record should include the date of inquiry and the name of reporting entity, the details matched and a note of disclosures of the contents of the EV record. IIS further recommends that the EV record should be held separately from a credit information file and not be included as "permitted contents" of a credit information file, included in a credit report under Part IIIA of the Privacy Act.

Recommendation 5 – Limits on secondary use of EV process information

IIS recommends that the enabling legislation should specify that information obtained or generated as part of EV using credit reporting information must not be used or disclosed for any secondary purpose not related to EV under the AML/CTF Act, other obligations under the AML/CTF act or as otherwise authorised by law. In particular, the law should provide that CRAs are not permitted to use information obtained in the course of an EV request to create or update credit information files as defined by Part IIIA of the Privacy Act.

Recommendation 6 – Notice of EV failure

IIS recommends that if the proposal proceeds, AGD should undertake further work, in conjunction with reporting entities and including testing options with individuals, to develop an approach to advising individuals about an EV failure. The approach will need to balance the concerns of reporting entities and the need to alert individuals to the possible need to follow up possible inaccuracies in source records or other difficulties.

Recommendation 7 – Alternative to be available

IIS recommends that if the proposal proceeds, the enabling legislation should provide that should an individual fail an EV process offered by a reporting entity, the reporting entity must either offer an alternative means by which the individual may choose to attempt to verify their identity or must refer the person to an existing dispute resolution process such as the Privacy Commissioner, or the Banking and Financial Services Ombudsman.

Recommendation 8 – Individuals to be given reasonable access to EV files about them

IIS recommends that if the proposal proceeds the enabling legislation should specify that where an EV process involves the use of credit reporting information an individual should be entitled to access to their EV record held by a CRA on the same basis that access would be provided to credit reporting information under the access provisions in Part IIIA of the Privacy Act and the Credit Reporting Code of Conduct.

Recommendation 9 – Penalties for unauthorised access or use

IIS recommends that if the proposal proceeds, consideration should be given to the need for offence provisions for unauthorised access to EV records whether held by a CRA or a reporting entity taking account of any changes to Part IIIA following the Government's consideration of the recommendations in the ALRC report.

Recommendation 10 – Privacy Act coverage

IIS recommends that if the proposal proceeds, consideration should be given as to whether the Privacy Act protects personal information collected by reporting entities for the purposes of EV under the AML/CTF Act in all circumstances, including where a reporting entity (which is deemed by section 6E(1A) of the Privacy Act to be an organisation for the purposes of complying with the AML/CTF Act) uses, or misuses, this personal information for non- AML/CTF purposes. If any gap in coverage is identified the Privacy Act should be appropriately amended.

Recommendation 11 - Retention of EV information

IIS recommends that if the proposal proceeds the applicable retention period for EV information be five years unless there are policy reasons arising from the AML/CTF regime to keep EV records held by CRAs for longer than five years.

Recommendation 12 – EV using credit reporting information included in AML/CTF Act review

IIS recommends that any amendments to give effect to the proposal be subject to review as part of the required review of the AML/CTF Act in 2013. IIS recommends that this review should include consideration of alternative sources of information available for identity verification, the privacy implications arising from both alternative information sources and alternative EV process, and that it should include a wider review of Australia's ID management systems. IIS recommends that a review of EV using credit reporting information should be informed by detailed statistical information collected by the relevant regulation on EV including on the extent to which EV is successful and where it is not successful, the reasons.

6.2.2 Recommendations relating to Governance, including transparency and accountability

Recommendation 13 – Monitoring

IIS recommends that the proposal should not proceed unless it is clear that the relevant regulators and dispute resolution bodies are properly resourced to carry out appropriate monitoring of the use credit reporting information in EV processes in particular in relation to whether:

- the consent processes used by reporting entities mean that individuals are provided with appropriate information before deciding to proceed;
- reporting entities are providing appropriate advice to individuals about EV failure;
- failure in relation EV is not being taken into account in substantive decisions about an individual.

IIS notes that the Office of the Privacy Commissioner, AUSTRAC and relevant dispute resolution bodies may need to liaise to clarify their respective roles in implementing this recommendation.

Recommendation 14 – No further use of credit reporting information without review

IIS recommends that there should be no further use of information held by CRAs for any new purposes without a wide-ranging review that is:

- independent;
- includes wide ranging public consultation; and
- follows PIA good practice.

IIS also recommends that the Government consider undertaking an investigation into Australia's online identity verification practices so as to identity processes and information sources and regulatory frameworks that are effective and which minimise privacy impact.

7 APPENDIX 1 REFERENCE DOCUMENTS

7.1 ALRC SUBMISSIONS REVIEWED

Author	Title
Dun & Bradstreet	Inquiry into Privacy Act, 13 April 2006
Dun & Bradstreet	Review of Privacy – Credit Reporting Provisions, Issues Paper, 9 March 2007
Dun & Bradstreet	Review of Australian Privacy Law – Vol 3, Discussion Paper 72, 7 December 2007
FCS Online	Review of Australian Privacy Law, Part 53, Use and Disclosure of Credit Reporting Information- Identity Verification Purposes, 7 December 2007
Australian Bankers' Association	Review of Australian Privacy Law, Discussion Paper 72, February 2008
Australian Bankers' Association	Review of Privacy Issues Paper 31, 19 March 2007
Global Data Company Pty Ltd	Review of the Privacy Act 1988, 7 December 2007
Galexia	Credit Reporting Framework, December 2007
Veda Advantage	Review of the Privacy, Issues Paper 31, January 2007
Australian Privacy Foundation	Review of Australian Privacy Law Discussion Paper 72, 2 January 2008
Australian Privacy Foundation	Review of Privacy – Credit Reporting Provisions Issues Paper 32, 2 April 2007
Office of the Privacy Commissioner	Submission to the Australian Law Reform Commission's Review of Privacy - Issues Paper 32 Credit Reporting Provisions, April 2007
Office of the Privacy Commissioner	Submission to the Australian Law Reform Commission's Review of Privacy - Discussion Paper 72, December 2007
Cyberspace Law and Policy Centre UNSW	Submission to the Australian Law Reform Commission on the Review of Privacy Issues Paper 32: Credit Reporting Provisions, 19 December 2007
Consumer Action Law Centre	Discussion Paper 72: Review of Australian Privacy Law, 21 December 2007

8 APPENDIX 2 – PARTIES CONSULTED FOR THIS PIA

Meetings held with Stakeholders	
5 August	Veda Advantage
	Dun and Bradstreet and FCS Online
	ING Direct
6 August	greenID (Deloitte and Global Database Company)
	AUSTRAC Gambling Industry Forum - Australian Casino Association, Betfair Ltd, Centrebet, Crown Melbourne, ClubsNSW
7 August	AUSTRAC Finance Industry Forum – Australian Bankers' Association, Australian Finance Conference (via teleconference), Investment and Financial Services Association Limited, Colonial First State, Securities & Derivatives Industry Association, Abacus, PayPal
	Office of the Privacy Commissioner
	AUSTRAC Privacy Forum – Australian Consumer's Association
10 August	Government Stakeholders – AUSTRAC, Treasury, Department of Prime Minister and Cabinet, Department of Finance and Deregulation, CrimTrac
10 August	Australian Bankers' Association, National Australia Bank, bankwest, Commonwealth Bank, ANZ
Additional submissions during consultation phase	
1	Association of Building Societies and Credit Unions (Abacus)
2	Australian Privacy Foundation
3	Bank of Western Australia (bankwest)
4	ING Direct
5	Liberty Victoria
6	National Australia Bank (NAB)
7	Office of the Privacy Commissioner
8	Australian Government The Treasury

Submissions on Draft Privacy Impact Assessment Report	
1	Association of Building Societies and Credit Unions (Abacus)
2	AUSTRAC
3	Australian Bankers Association
4	Australian Privacy Foundation
5	Dun and Bradstreet
6	greenID
7	Liberty Victoria
8	Office of the Privacy Commissioner
9	Australian Government The Treasury
10	Veda Advantage Limited

9 APPENDIX 3 – CONSULTATION QUESTIONS

CONSULTATION

The Australian Law Reform Commission recommended that the use and disclosure of credit reporting information for electronic identity verification purposes to satisfy obligations under the AML/CTF Act should be expressly authorised under the AML/CTF Act. However, it also noted that this amounted to significant function creep and that before the recommendation can be implemented there are a wide range of issues that require further consideration. The issues it identified include whether:

- the legislation should prohibit the secondary use or disclosure by reporting entities of credit reporting information obtained for identity verification purposes;
- reporting entities should have positive obligations to seek consent from individuals before using credit reporting information to verify identity; and
- reporting entities should have processes in place to resolve mismatches between the information individuals provide and credit reporting information.

The Australian Law Reform Commissioner received submissions in favour of using credit reporting information for electronic identity verification and also submissions that were concerned about the privacy implications.

This document seeks to draw out these issues further for the purposes of more fully assessing the privacy impact of this proposal. In determining the privacy impacts of this proposal there are a number of considerations. Some of these are set out below followed by questions designed to elicit views and evidence about them.

ISSUES

Whether the proposal will result in organisations (including credit reporting agencies) gaining access to new information that they would not otherwise have had.

One way of characterising this proposal is that it is simply another way of people providing identity information about themselves and does not result in any organisation gaining more information about a person than they would have had from current methods of identity verification.

What argument or evidence is there that might corroborate this view, or might contradict this view?

Whether the proposal will result in individuals having the same, or more or less control over their personal information.

It could be argued that the proposal will not reduce the control an individual has over their personal information and may increase protections around it for the following reasons:

- The proposal requires a reporting entity to gain the individual's consent before using credit reporting information to verify identity for AML/CTF purposes.
- An individual can choose to use off line means of identity verification if they do not wish to give their consent.
- Access to and use of credit reporting information is regulated by Part IIIA of the Privacy Act, and this includes offences for unauthorised access to credit reporting information;
- Current online identity verification schemes may not seek individual consent before accessing databases containing identity details about them;
- Current online identity verification schemes are only regulated by the more general provisions of the Privacy Act, and these do not include offences for unauthorised access.

What argument or evidence is there that might corroborate this view, or might contradict this view?

Whether credit reporting information is sufficiently accurate, complete and up-to-date to be a reliable source of identity verification.

It could be argued that credit reporting information is not sufficiently accurate or up-to-date to be a reliable means of identity verification. It could result in a significant number of individuals finding their application is rejected unfairly because there was a false rejection from the credit reporting information.

What argument or evidence is there that might corroborate this view, or might contradict this view?

Whether there are other existing means of electronic identity verification that are adequate for verifying identity for AML/CTF purposes.

It could be argued that there are already electronic identity verification services that are adequate for verifying identity for AML/CTF purposes and that there is therefore no need for this proposal that may have privacy intrusive consequences.

What argument or evidence is there that might corroborate this view, or might contradict this view?

What the consequences of rejection might be.

It could be argued that a failure to successfully verify an identity electronically using credit reporting information could have other consequences besides being directed to other means of identity verification. For example, it could result in an individual being "black listed" or put on a watch list.

What argument or evidence is there that might corroborate this view, or might contradict this view?

Whether the use of a scoring system rather than a 'match/no match' response provides a more viable option for electronic verification.

Implementation of this proposal may involve the use of a point scoring system rather than a yes/no response from the credit reporting agency. In a response to a request for electronic verification, the credit reporting agency would provide a score based how closely the information provided to it matches that information held on the credit file. The reporting entity would then determine whether the score was acceptable for the verification of identity.

It could be argued that this would provide a more practical and viable business system for reporting entities as it would overcomes mistakes, such as spelling errors, to ensure a higher match rate.

What argument or evidence is there that might corroborate this view, or might contradict this view?

Whether the scoring or matching process could enable the parties to the proposal, and in particular credit report agencies, to draw inferences about a customer, and to use this information for purposes unrelated to identity verification for AML CTF purposes.

It could be argued that the outcome of a matching process could be used by a credit reporting agency or other party to the matching to draw an inference about the person whose identity is being verified and to use this inference for purposes unrelated to verifying the person's identity for AML/CTF purposes and that this should not be allowed.

What argument or evidence is there that might corroborate this view, or might contradict this view?

Whether or not there is, on balance, benefit to the individual and the community from the proposal.

It could be argued that there will be economic and privacy gain for both individuals and the community, including business by:

- Making identity verification much more convenient for individuals and reducing the circumstances in which they must provide primary identity documents to organisations;
- Reducing costs for business seeking to conduct their business online;
- Encouraging innovation in online service provision.

On the other hand, it could be argued that there could be some undesirable consequences including:

- Individuals who do not have credit reporting histories are unable to have the benefit of receiving online financial or other services that require identity verification for AML/CTF purposes, and so become economically marginalised;
- Electronic identity verification could become focussed only on credit reporting information when other more effective mechanisms that do not involve use of credit reporting information are not explored.

What argument or evidence is there that might corroborate these views, or might contradict these views?

Whether there are harms or benefits to individuals or the community that have not been so far identified.

What are the harms that could result from use of credit reporting information to electronically identify a person for AML/CTF purposes?

What evidence is there to support this view?

If the proposal does not adequately address these harms, how might the harms be addressed?

What are the benefits that could result from the use of credit reporting information to electronically identify a person for AML/CTF purposes?

What evidence is there to support this view?