Productivity Commission Enquiry

Review of Data Availability and Use

29 JULY 2016

Contents

Executive Summary 3

Credit is fundamental to Australia's economic well being 3

What is the stated objective of Australia's Credit Reporting system? 4

Potential Benefits of an effective Credit Reporting system – what's at risk? 4

1. Best practice principles for credit reporting 14

2. Wide array of potential benefits from effective credit reporting system ... 17

3. Immediate issues to be resolved 24

3.1 Constrained participation precluding of telcos and utilities from most effective data 24

3.1.1 Who is disadvantaged the most? 24

3.2 Telco and utility data precluded due to circumstances at a point in time: 24

3.2.1 Constrained inputs – limiting the value proposition – holding back benefits for all 25

3.3 Comprehensive data, from a broad range of sources, is considered fundamental 26

3.4 If supply of CCR data is achieved, will broad use follow? 28

3.5 Compliance uncertainty – a serious and immediate issue 29

3.5.1 How has it happened? 30

3.5.2 The consequences – the capacity to assess credit risk – vastly diminished 31

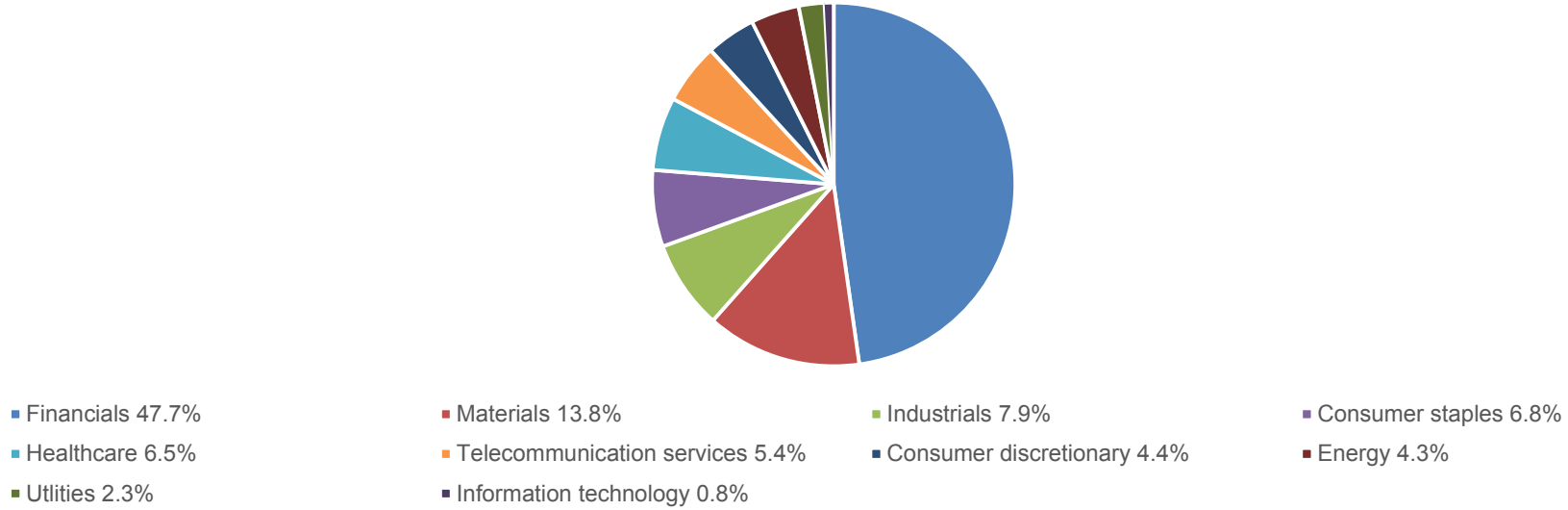
3.6 Alternative unregulated data being used increasingly to assess credit 32

4. Longer Term Structural Matters re: Data Access and Credit Reporting .. 33

4.1 Credit reporting - better regulated under Privacy or National Consumer Credit Protection Act? ... 33
4.2 An example of material regulatory delay due to a lack of cross jurisdictional coordination ... 33
4.3 Issues relating to how third parties gather personal information at the time of decisioning ... 34
4.4 Data ownership – is the right concept ownership or rights and obligations appropriate ... 34
4.5 Managing the costs of public data provision - best dealt with on a cost recovery basis ... 34
4.6 Coordinated public and private approach needed to meeting the demand for data science skills 35
4.7 Requesting personal information to be deleted – potentially problematic in a number of ways ... 35
4.8 Improving the management of data breaches includes prevention, detection and resolution. ... 36
5. Appendix 1: Addressing immediate compliance issues with RHI ... 36
6. Appendix 2: How credit risk models work; criticality of stable data ... 39
6.1 Overview of Credit Scoring ... 39
7. Appendix 3: Answers to Specific Issues Paper Questions ... 44
8. Appendix 4: Data Gathering in relation to Capacity to Repay ... 60

Executive Summary

Credit is fundamental to Australia's economic well being



Financial Services make up just under half of the ASX 200.

Currently, the total of Australian Consumer Credit stands at $ 1.7 Trillion and growing, larger than Australia's GDP of $ 1.6 Trillion.

At a household level, Australians have never owed more. On average they owe 180% of income, a level that is a full 20% higher than at the height of the Global Financial Crisis.

As a consequence it is more important than ever to ensure that Australia has the most effective means available of managing the credit risk associated with this debt.

Credit Reporting is a vital part of Australia's financial system infrastructure, providing wide array of potential benefits.

According to the World Bank's 2011 report General Principles for Credit Reporting:

> *"Credit reporting is a vital part of a country's financial infrastructure and is an activity of public interest.*
>
> *"In competitive markets, the benefits of credit reporting activities are passed on to borrowers in the form of a lower cost of capital, which has a positive influence on productive investment spending. Improved information flows also provide the basis for fact-based and quick credit assessments, thus facilitating access to credit and other financial products to a larger number of borrowers with a good credit history (i.e. good repayment prospects)."*

What is the stated objective of Australia's Credit Reporting system?

> *"One of the objects of the Privacy Act is to facilitate an efficient credit reporting system while ensuring that the privacy of individuals is respected. In recognition of that objective, the laws about credit reporting are intended to balance individuals' interest in protecting their personal information with the need to ensure that credit providers have sufficient information available to assist them to decide whether to provide an individual with credit.*
>
> *"The Australian credit reporting system also helps ensure that credit providers are able to comply with their* ***responsible lending obligations*** *under the* National Consumer Credit Protection Act 2009 *administered by the Australian Securities and Investment Commission (ASIC)."* [1]

The stated intention of the Australian Credit Reporting system is consistent with best practices, so that is not in question, but is the stated objective being effectively delivered?

Potential Benefits of an effective Credit Reporting system – what's at risk?

Important context is to consider what an effective credit reporting system can deliver in terms of benefits as these are what is at risk if that system is not working effectively.

Who are the potential beneficiaries?

Borrowers

- Those previously excluded from mainstream credit due to insufficient information to assess their credit worthiness
- Those seeking a 'better deal' or more innovative products not offered by their incumbent
- Those with good credit histories who have been relied on too much to cross subsidise the costs of bad debts
- Those at risk of credit trouble can also be identified earlier for treatment appropriate to their specific situation.

Credit Providers

- Incumbent Credit Providers who will have an even fuller perspective from which to make decisions and enable more efficient processes

[1] https://www.oaic.gov.au/privacy-law/privacy-act/credit-reporting

- Competitors, new market entrants and innovators who will have access to a threshold of data that will reduce the information disparity between them and a customer's incumbent credit provider – resulting in the choice to move or take up new products being put more firmly in the hands of the customer.

Government and Regulators:

- Provides an enhanced ability to analyse and model policy options, to simulate policy consequences relative to the credit market.
- Provides enhanced and efficient capability to observe broader industry or segment activities, for example, the use of a 'baseline' of information (CCR) in making credit assessment decisions and link that to resulting consequences, an important compliment to more traditional sampling of files.

From a data access perspective, D&B submission outlines how the current system stakes up against world's best practice, how its shortcomings are currently impeding the realisation of these benefits, suggests why this is the case and provides practical suggestions for improving the situation in the immediate and longer term.

Key Context: Types of data in Credit Reporting

CATEGORIES OF CREDIT REPORTING DATA	INCLUDES
NEGATIVE	Defaults, bankruptcy data, court judgements are all considered 'negative'. Also included in this category are enquiries – which are a records of someone having applied for a credit product. This was the extent of the allowable data pre the changes to the Privacy Act in 2014.
PARTIAL	Includes all of the negative data **plus four** additional elements: 1. The date an account was opened 2. The data an account was closed 3. The maximum amount of credit available (credit limit) 4. The 'type of credit' – limited to a set of elements defined in regulations.
COMPREHENSIVE (the incremental element also referred to by some as **'positive'** data)	Includes all of the Negative and all of the Partial elements **plus**: A code (from 0 to 7) to represent repayment history over a rolling 24 months. Roughly, each code translates to the number of months in arrears the account is that month.

How do these Categories (Tier Levels) interact?

Data Sets Included	Tier Level		
	Negative	Partial	Comprehensive (Restricted to Licensed Credit Providers – excludes Telco & Utility)
Coded 24 Month Payment History			Yes
Account Closure		Yes	Yes
Credit Limit		Yes	Yes
Credit Type		Yes	Yes
Account Open		Yes	Yes
"Negative" (Defaults, Enquiries, Public Records)	Yes	Yes	Yes

What do they look like in terms of decision making about an individual?

Current Negative Report

- Name
- Date of Birth
- Address
- Prior Address
- Drivers licence
- Directorships
- # and type of previous credit enquiries
- Bankruptcy
- Default
- Court Judgements

No default yet, but no idea of how much credit exists or how it is being conducted

Knowing this helps

Addition of Partial information

	Open Date	Exposure	Close Date
Credit Card	1/1/2001	$ 7k	-
Store Card	4/2/1995	$ 3k	-
Auto Loan	6/6/2009	$ 32k	31/5/2012
Home Loan	4/7/2001	$512k	30/6/2027
TOTAL		**$540k**	

But...

It is this that really identifies the risk

Further addition of Comprehensive data

Repayment History Information

(# of months in arrears)

	Credit Card	Store Card	Auto Loan	Home Loan
Jan	0	0	0	0
Feb	1	0	0	0
Mar	2	1	0	0
Apr	3	2	1	0
May	4	3	2	0
June	5	4	3	0

No default listing yet, but increasing delinquency

It is not until account behavior (repayment history information) is included that the 'right decision' begings to emerge.

Comprehensive Data, from a broad range of sources, is considered fundamental in achieving those benefits.

From the World Bank's recommended general principles for credit reporting:

> *General Principle #1*
> *Credit reporting systems should have relevant, accurate, timely and sufficient data—including positive—collected on a systematic basis from all reliable, appropriate and available sources, and should retain this information for a sufficient amount of time.*

What data makes up a typical credit score in a comprehensive credit reporting environment?

MAKE UP OF A CREDIT SCORE	IS THIS DATA ALLOWED IN AUSTRALIA?	IS THIS DATA CURRENTLY BEING SUPPLIED BROADLY IN AUSTRALIA?
30% Amounts Owed	**No**	**No**
30% Payment History	Limited Key segments (Telco/Utility)precluded	**No**
15% Length of Credit	Yes	**No**
10% New Credit	Yes	Limited Only requests for credit, not what has been granted
10% Type of Credit	Yes	
5% Defaults	Yes	Yes

Progress on implementation of comprehensive credit reporting (CCR) is slow and limited. The consequence of CCR data supply being voluntary is that Credit Providers (who represent only one of the beneficiary parties), must commercially justify the work involved.

The fact that the allowable data available is substantially less (from a predictive value perspective) than what the World Bank advocates as best practice makes such justification more difficult.

In contrast in New Zealand, where payment history data from telcos and utilities is allowed and the incremental predictive data is available, which increases the potential value of participation, they are nearing critical mass.

Beyond the commercial dynamics – there are other issues delaying forward movement on Comprehensive Credit Reporting:

COMPLIANCE UNCERTAINTY – is undermining the stated intention of the credit reporting sections of the Privacy Act:

The stated objective of the credit reporting sections - per the Office of the Australian Information Commissioner's (OAIC) website:

> *"…the laws about credit reporting are intended to balance individuals' interest in protecting their personal information with the need to ensure that credit providers have sufficient information available to assist them to decide whether to provide an individual with credit."*

In order to achieve this outcome, it's fundamental we can clearly distinguish varying degrees of risk based on account behaviour in relation to the contractual terms which are relevant at the time and whether or not repayments are meeting those terms.

As a result of the how the Privacy Act's accompanying regulation and the Credit Reporting Code of Conduct (CR Code) were drafted and how they are being interpreted by the Financial Ombudsman's Service (FOS), assessing material differences in risk is critically impaired.

The following three groups that represent vastly different risk profiles would be represented as exactly the same – by Repayment History Information code value of '0':

1. Those making repayments in full as per the original contract
2. Those who have been granted a formal temporary hardship contract variation and are meeting those terms
3. Those who have promised to make a payment and the credit provider has chosen to work with the customer, though not agreed to a formal temporary hardship contract variation (either because there was no request for one, circumstances did not indicated that was appropriate or a requested for a hardship variation was declined).

It is important to note that most frequently the temporary hardship terms are highly concessionary. They frequently require no payment at all for a period that can extend for several months and even out to as long as a year or more.

Australian Prudential Regulation Authority (APRA) and the international accounting standards both recognised that those who are on concessional terms (or who have been within the last six months) are of greater risk. Under their rules such accounts must be tracked and reported separately, because they represent a materially higher level of risk. Yet increasingly the view is that they must remain indistinguishable in terms of credit reporting.

The result is that the very objective of the credit reporting is severely undermined.

To be clear, Dun & Bradstreet favours addressing the underlying cause of the uncertainty rather than cause a different issue by undermining the ombudsman's capacity to adjudicate complaints on the basis of the law. Simply 'telling FOS' they are wrong in their interpretation is not seen as an effective resolution to the issue at hand. The drafting needs to be sufficiently clear and complete as to enable the objective to be met.

Suggestions as to how dealing with the multiple types of temporary contract variations could be more effectively handled are provided in Appendix 1.

Addressing 'free rider' concerns, and other the broader desire to ensure a positive commercial return from participation

From the ACCC's Final Authorisation Decision:

> *"The ACCC accepts that there are free rider concerns that are likely to inhibit full and complete implementation of Comprehensive Reporting without some type of mechanism to ensure that other credit providers are not able to free ride on that information."*

The Principles of Reciprocity and Data Exchange having now been authorised, whilst addressing the 'free rider' concern appears to be insufficient motivation to achieve critical mass of data contribution.

Private versus Public Mode Data contribution

When a credit provider begins to supply data to a credit reporting body, for obvious reasons there is a need to test that the process is working correctly and that the data is correct. This is done under a 'private mode' setting where the data is barred from being returned in credit reports. The mechanism for this is a contract between each credit provider and the credit reporting business/s that they supply data to.

The largest two credit providers to begin supplying data remain in this 'private mode' – after more than 12 months.

The contract allows the decision to move into a 'public mode' to be made by the credit provider. Beyond achieving testing success, these mechanism can also be used to constrain the use of a credit provider's data – even by those also contributing as signatories to the Reciprocity and Data Exchange – until the data supplier believes there is sufficient commercial value in what they will get in return to allow their data to be moved into the 'public mode'.

Via this mechanism even those that undertake the work to supply data continue to exercise a commercial decision that extends beyond the potential of others to 'free ride' as that was prevented by the authorisation of the Principles of Reciprocity and Data Exchange.

Whilst commercially understandable, this has the consequence of continued delay of benefits to all other potential beneficiaries – in particular consumers.

Competition for Capital with other internal projects

As participation in credit reporting is voluntary, the decision as to when to participate (or indeed whether or not to participate at all) must compete with all other activities the credit provider has the option to undertake. The consequence of this is that only the benefits that would flow to the credit provider are considered in the value assessment. This means that there may be different competing priorities across the industry and until the decision to progress to public mode is made independently by a critical mass of data suppliers, every beneficiary's benefits are delayed. In the case of anyone other than those who make up the critical mass of data suppliers, they have no say in when (or even if) the benefits of the move to comprehensive credit reporting will eventuate.

Alternative unregulated data being used to assess credit

In the absence of full CCR implementation 'social media data', and 'web surfing meta data' are being increasingly used to augment. In some instances they are being used as a substitute for the available credit reporting data.

Such auxiliary/alternative data it is being collected and used outside of the credit reporting system and as a result does not have the protections afforded under Part IIIA of Privacy Act, including:

- Certainty over what data is being collected;
- Constraints on how it can be used;
- The more structured obligations for challenge of data accuracy and correction; or
- Required disclosure in relation to what contributed to the decline of a credit application.

Additionally, to the extent that this is being used as a substitute for the use of credit reporting, this has the consequence of undermining the credit reporting system further as there will be no record of the application for data or the creation of the account, or a record of its conduct. This further impacts the integrity of the system, unfairly impacting the capacity of others who do seek to use the system and those who derive benefits from it.

Finally, from a sustained reliability perspective, there are questions about the efficacy of certain alternative sources of data such as social media. Consider if MySpace data had been adopted as a 'replacement for' credit reporting. Similarly with Facebook, LinkedIn, Instagram, Snapchat; with great regularity social media trends come and go, and whilst such data may infer some insights re: credit risk, given that is it not observed credit risk behaviour, the strength of inference is subject to fluctuation. In short, such sources of data do not provide the sustainable underpinnings from which credit risk can be reliably assessed.

Results:

- Australian law precludes or substantially inhibits data that the World Bank recommends as necessary to achieve the potential benefits. Critically, it is the most predictive data that is precluded.
- Compliance uncertainty is also impacting even the limited comprehensive data that can be supplied in Australia, and is of critical concern to the early adopters who have already submitted data that is now in question.
- As a consequence, under the current voluntary credit reporting system, it is uncertain whether those credit providers that are key to achieving critical mass collectively have not made the commercial case to implement broader credit reporting.
- All beneficiary groups are being denied the benefits and corresponding protections of an effective credit reporting system, and the objective set for enabling the credit reporting system is not being achieved.

Recommendations:

- **ADDRESS THE COMPLIANCE UNCERTAINTY –** enable the reporting of the circumstances relevant to enable effective risk assessment based on account conduct. Detailed suggestions as to how this can be achieved are included in Appendix 1.

- **ADDRESS DATA CONSTRAINTS BY ENABLING DATA CRITICAL TO RISK ASSESSMENT –** as a minimum expand the data that can be supplied to include repayment history in relation to telco and utility accounts, as recommended by the World Bank. Consider expanding the scope of the data to enable a limited set of key additional elements (e.g. account balance, payments made and business related taxes payments which are materially overdue).

- **LOCK IN TIMING –** Seek to gain a clear understanding of where those central to achieving critical mass in the market are with regard to implementation.
    - What is their timeframe for implementation?
    - Are budget and resources allocated and activities scheduled?
    - Are the activities on track to deliver to the set timeframe?
    - Are there any foreseeable issues that would delay or stop achieving on time delivery?

- **IF COMMITMENT TO 'CRITICAL MASS' DATA SUPPLY WITHIN A REASONABLE TIMEFRAME IS NOT FORTHCOMING:**

  It may be necessary for Government intervention to achieve a 'critical mass' of participation.

  What constitutes critical mass?

  - Top two banks = 50.4% of total ADI held household debt
  - Top three banks = 66.6% of total ADI held household debt
  - Top four banks = 82.6% of total ADI held household debt
  - Top ten banks = 94.8% of total ADI held household debt

  A structured approach, which sees a critical mass of participation obtained quickly would create sufficient competitive tension. This would ensure the remainder of the market would have sufficient certainty of a viable system as to undertake the work required to participate.

- **BENEFITS OF EQUITABLE DATA ACROSS CREDIT REPORTING BUSINESSES:**

  Key to maintaining market competition will be to ensure supply of full CCR data – to those credit reporting bodies that each credit provider has an arrangement to obtain credit reporting information from – to allow comprehensive credit reporting to achieve its stated objective of enabling responsible lending decisions and allowing benefits to all stakeholders to be realised.

  In relation to the Australian Retail Credit Association's (ARCA) Principals of Reciprocity and Data Exchanges (PRDE), the ACCC in their authorisation indicated it was important that data be shared consistently with those credit reporting businesses with which the credit provider has a relationship. ASIC echoed in their submission to the ACCC authorisation a similar view, that there would be issues if sharing was not on this basis.

Additionally, such an approach to sharing will help to ensure that competitive forces remain to evolve and improve data management practices, in particular data management and matching.

1. Best practice principles for credit reporting

The World Bank outlines key elements of an effective credit reporting system, based on the findings from their extensive research. Outlined in the following pages is an assessment of the Australian model and current experience relative to that benchmark:

WORLD BANK GENERAL PRINCIPLES:	PRESENT IN AUSTRALIAN MODEL?
Data — Credit reporting systems should have relevant, accurate, timely and sufficient data—including positive — collected on a systematic basis from all reliable, appropriate and available sources, and should retain this information for a sufficient amount of time.	Limited
Data Processing Security and Efficiency — Credit reporting systems should have rigorous standards of security and reliability, and be efficient.	Yes
Governance and Risk Management — The governance arrangements of credit reporting service providers and data providers should ensure accountability, transparency and effectiveness in managing the risks associated with the business, along with fair access to the information by users.	Yes
Legal and Regulatory Environment — The overall legal and regulatory framework for credit reporting should be clear, predictable, non- discriminatory, proportionate and supportive of data subject and consumer rights. The legal and regulatory framework should include effective judicial or extrajudicial dispute resolution mechanisms.	Yes
Cross-border Data Flows — Cross-border credit data transfers should be facilitated, where appropriate, provided that adequate requirements are in place.	No

Those missing and limited elements are important considerations for credit providers in assessing the commercial business case for participation under a voluntary credit provider opt-in model.

WORLD BANK KEY PARTICIPANT ROLES	PRESENT IN AUSTRALIAN MODEL?
Data providers should report accurate, timely and complete data to credit reporting service providers, on an equitable basis.	Enabled, but not yet functioning
Other data sources, in particular public records agencies, should facilitate access to their databases to credit reporting service providers.	Limited[2]
Credit reporting service providers should ensure that data processing is secure and provide high quality and efficient services. All users have either a lending function or a supervisory role should be able to access these services under equitable conditions.	Materially Limited e.g. the exclusion of Telcos and Utilities
Users should make proper use of the information available from credit reporting service providers.	Broadly Yes
Data subjects should provide truthful and accurate information to data providers and other data sources.	Yes Data is not direct input by subjects
Authorities should promote a credit reporting system that is efficient and effective in satisfying the needs of the various participants, and supportive of data subject/consumer rights and of the development of a fair and competitive credit market.	Allowed, but not promoted

How these key roles are structured in Australia and the degree to which they are being engaged is thought to be driven primarily by a mix of three main reasons.

- Limited/excluded key predictive data
- Constrained participation by key segments in sharing the most predictive data that is allowed
- A potential lack of appreciation these consequences on the breadth and scale of potential beneficiaries and benefits.

[2] Improvements in the quality and availability of relevant Court Records are necessary.
Access to additional Public datasets, such as information about overdue self-employed and company tax records.

WORLD BANK RECOMMENDATION RE: OVERSIGHT	PRESENT IN AUSTRALIAN MODEL?
Credit reporting systems should be subject to appropriate and effective regulation and oversight by a central bank, a financial supervisor, or other relevant authorities. It is important that one or more authorities exercise the function as primary overseer.	**No** Oversight not by an agency with a commercial focus
Central banks, financial supervisors, and other relevant authorities should have the power and resources to effectively carry out their responsibilities in regulating and overseeing credit reporting systems.	**Partial** Powers seem sufficient. Enforcement resources limited
Central banks, financial supervisors, and other relevant authorities should clearly define and disclose their regulatory and oversight objectives and roles, as well as major regulations and policies with respect to credit reporting systems.	**Limited** Regulator very slow with provision of guidance relative to CCR
Central banks, financial supervisors, and other relevant authorities should adopt, where relevant, the general principles for credit reporting systems and related roles, and apply them consistently.	**No**
Central banks, financial supervisors, and other relevant authorities, both domestic and international, should cooperate with each other, as appropriate, in promoting the safety and efficiency of credit reporting systems.	**No (E.g. no cooperation between AUS and NZ)**

From an oversight perspective the Australian model is not well aligned, both structurally and operationally, to the best practice oversight elements outlined by the World Bank. This further contributes to the failure to embrace CCR in Australia, to date.

2. Wide array of potential benefits from effective credit reporting system

Benefits from CCR are available to a wide variety of stakeholders including borrowers, new market entrants, product innovators, current credit providers with and without existing relationships and those who rely on credit in part to facilitate the purchase of their goods and services, as well as the general population.

Though primarily these benefits are derived using the incremental CCR data to provide more accurate credit assessment decisions, there are other benefits that can be achieved.

Borrower Benefits:

		POTENTIALLY - WHO BENEFITS FROM WHAT RE: USE OF CCR?						
		Better new credit assessment			Better existing credit monitoring	Process efficiency and protection		Improved financial Literacy
	BENEFICIARIES	More credit	Less credit	Cheaper credit (relative to current)	Help sooner	Lower cost	Less hassle / Greater protection	
BORROWERS	Financially (mainstream) excluded - Currently Under Lent	1		2			3	4
	Financially exposed - Currently Over Lent		5		6			
	Now at risk due to changed circumstances							
	Those with good credit histories			7				

EXPLANATION:

1. **Financial inclusion:**
   Those who are currently financial excluded *from mainstream credit* due to insufficient information to adequately assess their risk will be able to get credit – a key part of financial inclusion.

2. **Cheaper and fairer credit:**
   The resulting credit that previously excluded people would be able to get, will almost certainly be less expensive and on fairer terms than any 'non mainstream' (unregulated) credit they may currently have access to.

3. **Less Hassle and greater protection:**
   CCR enables processes to be more efficient and effective in gathering the data required. This is in part due to the fact that CCR data, being obtained independently is already verified. CCR data, being specifically regulated also carries a higher level of consumer protection than if that data were sourced via other means. For example, there are mandated corrections and complaints mechanisms in place including access to External Dispute Resolution (EDR) schemes.

4. **Improved financial literacy (via greater awareness):**
   The vast majority of Australians have historically had little if any interaction with the content of their credit report. Many have no idea what it contains or how it is used. This is primarily due to two factors:

   a. Negative credit reporting has largely been limited in its use of assessing new applications for credit, an activity that on average happens less than once per year

   b. In the vast majority of instances only when credit is declined based on a 'default listing' does the consumer take any interest in what data is on their credit report. Given less than 15% of the population have had a default during the past five years or other negative item (e.g. court judgement or bankruptcy), being declined 'for credit bureau related reasons' is rare.

In contrast, under CCR (assuming full implementation) every account held will be listed as existing at a minimum, and accounts with licensed credit providers will have a repayment history update made monthly. This more objective and directly conduct-related data will be used for risk assessment and most likely data that is less objective and more inferential will be will be substituted out. The increase in decisions related to credit bureau information will increase individuals' awareness of what is on their credit report and how to positively influence that data – both key elements of increased financial literacy.

Furthermore, the resulting vast increase in predictive power from the additional information will mean that credit providers will be more likely to use the data in other areas of the credit life cycle:

	BASIC CREDIT LIFECYCLE		
TYPICALLY…	Application Assessment	Account Management	Collection of Overdue Debt
WHEN ARE NEGATIVE FILES USED?	Yes		
WHEN ARE CCR FILES EXPECTED TO BE USED?	Yes	Yes, *but restricted under Privacy Act*	Yes

Even in a fast growing credit environment new accounts only account for about 10% of the total in any one year; whereas on any one day there are nearly the same proportion of accounts that are overdue and or at risk due to a life changing event. This means that there are many times more decisions likely to be influenced by CCR data assuming wide spread adoption.

5. **Reduction in over lending:**
CCR enables a vastly greater awareness of the individual's current level of indebtedness when they apply for new credit. Further, the data is independently supplied and more accurate than data supplied when the credit provider was dependent on the consumer to fully disclose their debts.

   Prior to the Privacy Act changes an information study undertaken by ten credit providers, which looked at the extent to which consumers under reported their debts. The study found that a substantial proportion of borrowers understated their debts. Approximately 40% understated their debts by more than 25% (of the value of debt that was later manually discovered by contacting the other study participants, which is time intensive). This assessment was undertake after the credit decision was made so did not alter who did and didn't get approved for credit. Those who did under disclose were more likelihood to end up in bankruptcy within a 12 month period (4 times as likely).

6. **Identification of credit issues sooner:**
At the time of application:

   Those seeking new credit that are already over indebted will be identified sooner, preventing them from getting into even greater debt.

   When there is evidence that a 'life event' has impacted their capacity to repay existing debt:

   Such instances will be identification sooner enabling credit providers to work with the borrower earlier to find the most effective way forward.

   Important to note:

Whilst 'defaults' can 'in theory' be listed at 60 days past due (subject to notification and other prerequisites) in reality they are almost exclusively NOT listed until far later, generally 180 days past due or more. This is in part because of the exceptionally complex consequences involved in listing a debt before the debt has been accelerated to the full balance owing.

Repayment history information (RHI) will enable detection of building financial difficulty (such as increasing delinquency at another institution) potentially months earlier. To the extent that early detection enables increased opportunity to remedy the situation before it reaches the 'default listing stage'

7. **Much quicker recovery from a credit issue is possible with CCR fully implemented:**
   RHI is updated monthly, so once debts begin to be repaid on time, this will be reflected. Further, the retention period for RHI is just two years, whereas defaults have a retention period of five years. It should also be noted that defaults are only updated once they are fully resolved, interim payment updates are in fact prohibited.

   Combined with the earlier detection and potential to prevent a more severe situation from developing in the first place, RHI will enable the consumer to demonstrate a rehabilitated credit record in less than half the time.

8. **Potentially lower levels of cross subsidisation:**
   The diminished predictive power of negative only information results in those with good credit history being unable to extract value in the form of better pricing, because the ability to assess the degree of risk can't be as effectively calibrated.

   NOTE:
   On the understanding that 'penalty interest' is not legally allowed in Australia, those whose circumstances change and their level of risk increases will not experience 'dynamic repricing'[3]. This is an important difference between the Australian and American markets, a difference that seems to be missed in discussions about the likely consequences of Australia's migration to a more comprehensive credit reporting system.

[3] 'Dynamic Repricing' is the resetting of the interest rate charged on a debt being linked to changes in their credit bureau score.

Lender Benefits:

		POTENTIALLY - WHO BENEFITS FROM WHAT RE: USE OF CCR?						
		Better new credit assessment			Better existing credit monitoring	Process efficiency and protection		Improved financial Literacy
	BENEFICIARIES	More credit	Less credit	Cheaper credit (relative to current)	Help sooner	Lower cost	Less hassle / Greater protection	
BORROWERS	Large incumbent credit providers	8	9		10	11		
	Small incumbent credit providers							
	New market entrants							
	Innovators							

EXPLANATION:

For renders re: 8,9,10 and 11:

Fully implemented CCR ensures that at least a baseline threshold of predictive data across an individual's credit exposure is available for decision making. This benefits all credit providers, though to varying degrees and in different ways.

Large incumbents – May already hold some of this information to the extent that the customer has a credit relationship with them. The broader the credit relationship the more data they have, however that does not assure they are always in a better position to assess risk.

The real determinant of the incumbent's benefit is not the extent of the data they hold, but rather the extent of the data they don't.

It is very clear from bankruptcy studies over time that the degree of 'financial promiscuity' (i.e. the number of institutions one has debt with) is highly correlated with risk.

Small incumbents – The benefit of CCR is similar to that for large incumbents but is tempered by the breadth and depth of use they enable, which may be influenced by resource constraints.

Extracting benefits from the more predictive data requires the capacity to use that data to calibrate risk and use the calibration to segment processes tailor decisions, and execute actions. Full value is extracted by being able to identify when automation can be most appropriately used (both the achieved cost efficiency, but more to achieve decision consistency). Adding to that is the cost of the staff needed for the data science, analytic, and technical resources needed to implement and run these systems.

New market entrants – Will have access to a threshold of data that will reduce the information disparity between them and a customer's incumbent credit provider – resulting in the choice to move or take up new products being put more firmly in the hands of the customer (not constrained by their incumbent credit provider).

Innovators – CCR data being 'new information' enables identifying improvement opportunities that were previously hidden to tailor actions more effectively to the underlying risk.

There are also benefits from increased competition between credit reporting businesses including constructive pressure to:

- Continually improve data matching capabilities
- Extract greater predicative accuracy from the data available – refining scoring models
- Evolution of tools to utilise credit assessments into more appropriate actions – better tailored to the circumstances of the individual's situation.

Another dimension to consider in relation to benefits for lenders is where they accrue and from what sort of decisions:

Based on the analysis Dun & Bradstreet has done on the New Zealand market (thought to be a relatively good proxy for Australia), following is the estimated proportional breakdown.

	POTENTIALLY - WHO BENEFITS FROM WHAT RE: USE OF CCR?						
	Better new credit assessment			Better existing credit monitoring	Process efficiency and protection		Improved financial Literacy
BENEFICIARIES	More credit	Less credit	Cheaper credit (relative to current)	Help sooner	Lower cost	Less hassle / Greater protection	
Where do the lenders' economic benefits come from (estimate)	33%	30%		30%	6%		

Based on in-house analysis of the New Zealand CCR experience thus far, roughly a third comes from identifying opportunities to responsibly lend to those miss-assessed as too high risk. Nearly two thirds comes from lending less or taking action sooner where the new data indicates changed circumstances that suggest the individual needs assistance. The smallest of the benefits relates to cost cutting efficiencies.

94% of the benefit to lenders relates to improved risk assessment and the taking of actions that are more appropriate under the circumstances.

The suggestion that CCR is likely to lead to an explosion of additional credit is simply not substantiated; given the commercial benefits for implementing CCR would not stack up purely on incremental lending, as the bulk of benefit comes from more effectively mitigating risk, not just taking more on.

Beyond the obvious borrowers and lenders stakeholders, there are potentially material benefits available for others – some direct benefits others more indirect.

	BENEFICIARIES	BENEFIT
OTHERS	The wider population	Better distribution of capital and economic growth
	ASIC	Access to new information that will be helpful in assessing compliance with prudential and conduct obligations
	APRA	
	Government (Treasure and others)	Access to new information available for objective policy analysis and development

Well beyond theoretical, these benefits are being achieved by others based on a vast body of evidence internationally and is thought to be highly likely based on Australian simulations.

3. Immediate issues to be resolved

3.1 Constrained participation precluding of telcos and utilities from most effective data

3.1.1 WHO IS DISADVANTAGED THE MOST?

Based on international experience, excluding the provision of account behaviour (performance earlier than at the point of default) from Telcos and Utilities has been shown to be disproportionally detrimental to:

- Those with lower incomes;
- Minorities;
- Both ends of the age spectrum (young and old); and
- Immigrants[4]

Such data has also been shown to be helpful in enabling credit assessment for these same groups, where without it credit assessment is substantially inhibited resulting in greater financial exclusion.

3.2 Telco and utility data precluded due to circumstances at a point in time:

The current Privacy Act restricts access to repayment history information (which alone constitutes approximately 60% of the predictive power of available credit reporting information) to only those who hold an Australian Credit License (ACL), a consequence of which is being subject to the National Consumer Credit Protections Act and its responsible lending obligations. It is well documented that this pre-requisite condition was based on a view at the time of development that having to be subject to 'responsible lending' obligations was an appropriate trade-off for enabling credit providers to have access to the limited (and prescribed) new data sets of personal information.

Times have changed:

Since the requirement to have an ACL as a pre-requisite to be able to provide or receive repayment history information was developed during the drafting of the Privacy Act amendments, both the telecommunications and utilities industries have revised their codes of practice. Whilst they do not mirror the NCCP responsible lending requirements and ASIC guidelines, there are clear parallels to a number of the NCCPs key protections. Additionally, service providers in both of these industries are required to participate in an External Dispute Resolution scheme.

Improved telco conduct:

[4] The Credit Impacts on Low-Income Americans from Reporting Moderately Late Utility Payments by Michael Turner, Ph.D., Patrick Walker, M.A., and Robin Varghese, Ph.D., Sukanya Chaudhuri, Ph.D. August 2012

At the time that the Privacy Act amendments were being drafted the telco industry was experiencing high numbers of complaints about billing, and in particular 'roaming charges'. Additionally, there were previous issues with failed telephony service providers that went out of business and defaults they previously listed not being open to challenge with regard to data accuracy.

These matters have been subsequently addressed and measures put in place with regard to correction request processes that means these issues have been addressed, and no longer pose the risk they did at the time.

Complaints about mobile services dropped 23%, with a ratio of 18.3 per 10,000 SIO, compared to 23.7 in 2013-14. The TIO's 2014-15 annual report commented that complaints about mobile services decreased as a result of improvements in key areas such as coverage and excess data charges. [5]

Improved utility conduct:
Similar to the Telco industry complaints in relation to utilities have dropped dramatically. As an example, complaints relating to billing and credit practices to the Energy and Water Ombudsmen service covering NSW (EWON) were down 14% and 12% respectively since drafting of the Privacy Act.[6]

At EWOV (the Energy and Water Ombudsmen service covering Victoria) "cases fell across all industries and issues categories. But in an indication of the changing nature of our work, while billing cases fell 47%, credit cases fell only 25%."[7]

Dun & Bradstreet believes given the consequences of excluding this data and the improvements made by these industries it is time to reconsider this decision.

3.2.1 CONSTRAINED INPUTS – LIMITING THE VALUE PROPOSITION – HOLDING BACK BENEFITS FOR ALL

In Australia, RHI data from telcos and utilities can be provided.

In contrast in New Zealand, where the move to comprehensive credit reporting started at least a year later, such data is allowed. In New Zealand they have has achieved substantial levels of participation; however their largest bank has yet to supply full CCR data.

To date only one of Australia's major banks has begun sharing the newly allowable data (in a testing mode) – well short of what is needed to reach critical mass.

Whether or not this is the primary reason – failure to get to a point where the majority of the data available is being supplied means that all stakeholders other than those who control that decision must wait for them.

[5] http://www.tio.com.au/publications/news/whole-of-industry-complaints-drop-in-2014-15
[6] http://www.ewon.com.au/index.cfm/publications/annual-reports/annual-report-2014-2015/complaints-issue/
[7] https://www.ewov.com.au/__data/assets/pdf_file/0014/15404/EWOV_2015_Annual_Report.pdf

BENEFICIARIES	WHO CAN BENEFIT	WHOSE DATA PARTICIPATION IS CENTRAL TO ACHIEVEING THESE BENFITS?
Borrowers who are:		
Financially (mainstream) excluded – Currently under lent	Yes	[redacted]
Financial exposed – Currently over lent	Yes	
Now at risk due to changed circumstances	Yes	
Those with good credit histories	Yes	
Credit providers who are:		
Large incumbents – Credit providers and CRBs	Yes	Yes
Small incumbents – Credit providers and CRBs	Yes	[redacted]
New market entrants – Credit providers and CRBs	Yes	
Innovators – Credit providers and CR data management services	Yes	

Dun & Bradstreet believes achieving sufficient CCR data supply in the near term to enable an effective system is critical, and central to ensuring that the proposition to voluntarily participate is sufficiently compelling.

Clearly supply of data alone is insufficient to achieve some of the benefits – there must be use of the data.

3.3 Comprehensive data, from a broad range of sources, is considered fundamental

Other categories of highly predictive data that remain excluded:

> Current legislation in relation to CCR precludes the sharing of any data that is not specifically listed for the purpose of assessing credit worthiness.

Three key elements that are currently NOT allowed:

- Actual account balance – the actual debt that is outstanding – an objective measure of behaviour. This information is different to the credit limit (the maximum possible exposure which in the vast majority of cases is not reflective of behaviour and so can only be used to infer conduct – a much weaker means of predicting future repayment risk.
- Actual payment data – another objective measure of behaviour that is predictive of repayment risk, and without must be inferred from other data, resulting in far less risk assessment accuracy.

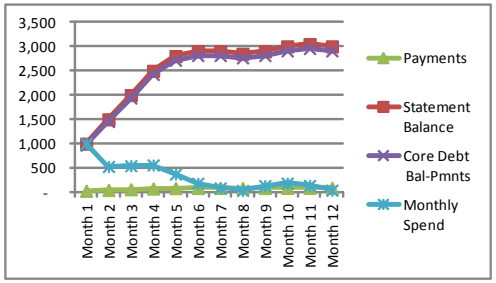
Examples of what data matters when differentiating risk:

- Both have the same credit limit – currently allowed to be shared
- Both have the same balance – currently NOT allowed to be shared
- However, there are very different payment levels – currently NOT allowed to be shared.

Following is an example of how these elements work and why such data is important to the effective assessment of credit risk – the underlying purpose of credit reporting.

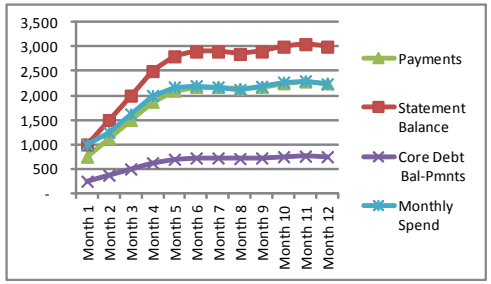
Core Debtor

	Limit	Statement Balance	Payments	Core Debt Bal-Pmnts	Monthly Spend
Month 1	3500	1000	30	970	1000
Month 2	3500	1500	45	1,455	530
Month 3	3500	2000	60	1,940	545
Month 4	3500	2500	75	2,425	560
Month 5	3500	2800	84	2,716	375
Month 6	3500	2900	87	2,813	184
Month 7	3500	2900	87	2,813	87
Month 8	3500	2850	86	2,765	37
Month 9	3500	2900	87	2,813	136
Month 10	3500	3000	90	2,910	187
Month 11	3500	3050	92	2,959	140
Month 12	3500	3000	90	2,910	42



Active User

Limit	Statement Balance	Payments	Core Debt Bal-Pmnts	Monthly Spend
3500	1000	750	250	1000
3500	1500	1,125	375	1,250
3500	2000	1,500	500	1,625
3500	2500	1,875	625	2,000
3500	2800	2,100	700	2,175
3500	2900	2,175	725	2,200
3500	2900	2,175	725	2,175
3500	2850	2,138	713	2,125
3500	2900	2,175	725	2,188
3500	3000	2,250	750	2,275
3500	3050	2,288	763	2,300
3500	3000	2,250	750	2,238



Without both balance and payment data these profiles are indistinguishable even though they are vastly different in terms of credit risk

These two elements of information are additionally and uniquely valuable given their potential to be checked against a credit report as they form part of periodic account statements – unlike many of the other allowed data elements.

- **Overdue company debts** – (e.g. BAS and quarterly payment of taxes) are vitally important elements of information that if available would materially improve decisions relating to the provision and management of credit for those who are self-employed.

The ATO is one of the largest lenders in Australia owned billions of dollars in overdue tax at any one time, yet no information is readily available about these debt at an individual 'borrower' level (be that an individual or a business) for use in making credit decisions. Given that tax debt ranks above other debt types (including secured credit), this creates a 'blind spot' that results in credit losses that are higher than they might otherwise be. The cost of those losses is perversely being borne ultimately only by those who in fact do re-pay their debts. New Zealand has already adopted legislation that will allow this content to be added to their credit reporting system.

3.4 If supply of CCR data is achieved, will broad use follow?

ASIC in their Responsible Lending Guide RG 209 indicated an expectation that when CCR data was available that they expected it would be included as part of what was 'reasonable' to consider in credit assessment.

> *"Credit providers, which are subject to the Act's responsible lending obligations, must "take reasonable steps to verify" a consumer's financial situation. As noted in ASIC Regulatory Guide 209 Credit licensing: Responsible lending conduct, what constitutes "reasonable steps" may change as additional tools, such as the comprehensive credit reporting system, become available.*

ASIC further in their submission to the ACCC authorisation of the industry developed Principles of Reciprocity and Data Exchange (PRDE) expanded on that view by saying:

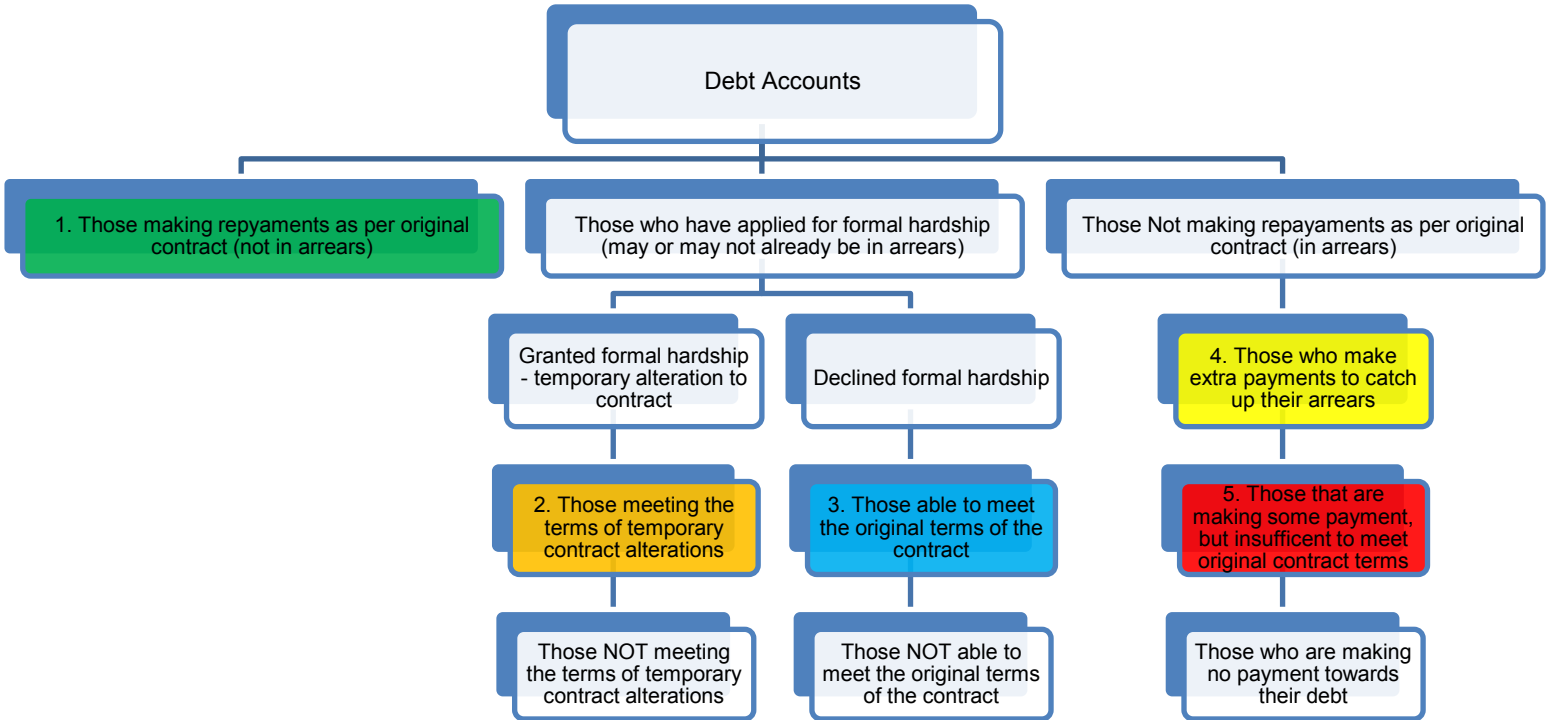
> *"If a credit provider chooses not to use such a tool, ASIC would expect the credit provider to be able to explain why the use of the tool was not appropriate or what other steps the credit provider has taken to verify the consumer's financial situation. This factor would need to be considered by a credit provider when deciding whether to become a signatory and, if they become a signatory, at what tier (comprehensive or negative) to participate."* [8]

Recalling that RG 209 was written prior to the Privacy Act changes enabling CCR data and the PRDE sets of rules that governing the 'supply' of CCR data, it would seem plausible that ASIC could have been flagging that Supply (now 'available') is linked to meeting their expectation in regards to 'use'.

[8] http://registers.accc.gov.au/content/trimFile.phtml?trimFileTitle=D15+69467.pdf&trimFileFromVersionId=1191221&trimFileName=D15+69467.pdf

3.5 Compliance uncertainty – a serious and immediate issue

Below is an illustration of the interplay between making or not making payments relative to the original contract or a formal temporary hardship variation to the contract. Each of the coloured boxes represent very different risk profiles, however, there is an issue with distinguishing them given the drafting and interpretation of the credit reporting provisions of the Privacy Act, related regulations and Credit Reporting Code of Conduct.



CRITICAL ISSUE REQUIRING ACTION:

A situation where these scenarios are made indistinguishable due to limitations of what information can be reported will result in material inaccuracy in credit risk assessment and as a consequence inappropriate credit decisions – undermining the primary stated objective of credit reporting. D&B believes that addressing this uncertainty and dealing with stakeholder concerns effectively may require government assistance in the very near term.

3.5.1 HOW HAS IT HAPPENED?

The following section outlines a brief description of the cumulative effect of drafting of the regulations, the CR Code and most recently determination by the Financial Ombudsman Service (FOS) and how this may be undermining the ability to achieve that stated purpose of the legislation re: credit reporting.

- **First** –The Act allows for information about the terms of the credit to be exchanged, but limits the data to what is specifically listed in the regulations that accompany the Privacy Act. Those regulations were drafted such that a seemingly vital aspect of information – i.e. whether the terms of a contract have been formally varied to more concessional terms for a temporary amount of time – is not specifically listed as 'allowed'. Therefore, based on how the mechanism works it is 'not allowed'.
- **Second** –The 'assumption' by industry was that they could address this matter within the drafting of the Credit Reporting Code of Conduct, which was specifically intended to enable industry to deal with technical and nuanced matters relating to the precise data to be exchanged.
  Industry is understood to have expected to be able to address 'temporary variations' by simply flagging such instances in the 24 month rolling history of repayment; called repayment history information. As this is an element that is updated monthly this would offer a practical means of ensuring that it remains up to date.
- **Third** –The OAIC's refused to allow such 'flagging' in the 24 month profile, at the request of consumer advocates. It is understood that the advocates were concerned about how the data would be used and that potentially its inclusion might result in fewer borrowers seeking to avail themselves of the hardship provisions in the National Credit Act. It was also thought to obtain credit in the future would be negatively impacted by a 'black mark' or any existing, but unused credit would immediately be withdrawn. These consequences were viewed by the advocates as potentially detrimental.
- **Fourth** – Based on the limited provision of full CCR data thus far, from the perspective of repayment history information, industry participants given the inability to flag 'temporary variations', or to 'ignore' such arrangements (as that would create issues with data being incomplete) are choosing to simply report the conduct of the account relative to the original terms of the credit. This decision is entirely consistent with the APRA requirements to treat such credit as impaired, given that is demonstrably of higher risk of future default.
- **And finally** – The determination by FOS in case 422745:
  In the case before FOS, there was no hardship application involved. However, the lender agreed to postpone their rights under the contract (which would have included calling up the full debt) up to the full debt, whilst the individual was making up the arrears in addition to make additional payments as they fell due.

FOS's view is that "the Applicant met her contractual obligations to make all payments that were due and payable under [the] loan contract, as varied" and "It was therefore inappropriate for the FSP to record the applicant as having missed payments…[in her credit report]".
The sum total result – informal temporary concessional contracts, as in the specific case before FOS, cannot be reported as having missed payments during the period whilst the arrears are being caught up.

It is also understood that FOS intended to take the same view relative to instances of formal temporary concessions (Hardship arrangements under the NCCP Act).

3.5.2 THE CONSEQUENCES – THE CAPACITY TO ASSESS CREDIT RISK – VASTLY DIMINISHED

Such an interpretation would see credit providers having to report the same value of 'zero' defined under the CR Code as meaning 'Current up to and including the grace period' – irrespective of whether the payments they are making are what the original contract calls for, what a formal temporary contract variation calls for or what a credit provider deems to be sufficient to informally agree to not immediately exercise their contract rights.

As a consequence – what is expected to be reported is the same (technically a value of 'zero') irrespective of whether the borrower repaid the debt in accordance with the full terms of the contract, or only in relation to concessional terms (which frequently include making no payment at all for a period of time).

These scenarios represent very different levels of risk. Therefore not being able to distinguish them effectively, materially inhibits the ability **to "assist credit providers to determine whether to provide an individual with credit"** and to **"ensure that credit providers are able to comply with their responsible lending obligations"**, which are core elements of the currently stated objective of the credit reporting system.

D&B recommends that the government needs to initiate action urgently to address the matters impeding effective reporting of account conduct (RHI). Further, D&B believes that a change to the regulations could achieve a practical solution and be implemented quickly.

A more detailed description of our recommendation is included in Appendix 1 and involves making a single addition to the Regulations.

The reason that we advocate utilising the regulations is twofold:

1. **They are thought to be the simplest of the 3 elements (Act, Regulations or CR Code) to change.**
2. **To avoid further 'black letter' definition of data – an approach that quickly dates.**

3.6 Alternative unregulated data being used increasingly to assess credit

There is a dangerous myth in circulation that suggests the need for credit reporting can be totally met by modelling of ‘social media data’, and ‘web surfing meta data’.

Whilst ‘social media data’ can add incrementally to processes involved in credit assessment, its ability to be manipulated and the speed by which sources have historically come and gone creates a substantial systemic risk.

Consider if the source of data had been social media when MySpace was in vogue. Very quickly that platform was replaced by Facebook, and today segments of Facebook have been replaced by Twitter, Snapchat and others.

In addition, the use of these data sources is difficult for consumers to readily link to credit performance and difficult to identify a path to an improved credit profile. This contrasts with the credit reporting system that provides transparency, access to the data used in the decision and a clear path to improving the consumer’s credit standing.

An underlying baseline of stable ‘always’ fit-for-purpose data to enable credit risk assessment, is soundly delivered by a fully implemented CCR system. This is a critical part of Australia’s financial and economic infrastructure.

Refer to Appendix 2 for additional detail on how credit scores are developed, how they are managed and their fundamental need for underlying data stability.

4. Longer Term Structural Matters re: Data Access and Credit Reporting

4.1 Credit reporting - better regulated under Privacy or National Consumer Credit Protection Act?

This situation creates a misalignment between the stated policy intentions regarding credit reporting and the obligations the legislation imposes for responsible lending. Credit reporting is considered primarily a credit conduct matter – as most of the obligations in the Privacy Act, associated regulations and CR Code are conduct matters and not matters of information protection.

The objectives set out for credit reporting, in addition to enabling credit assessment, seek to create a balance between that and what the OAIC refers to as the need to 'balance individuals' interest in protecting their personal information. The vast majority of Part IIIA deals with matters well beyond 'protecting personal information'. In fact largely only Sections 20Q and 21S deal with matters of protecting personal information. The remainder of Part IIIA deals primarily with matters of credit risk assessment and fairness with regard to credit practices – which are much more closely aligned with the objectives of the National Consumer Credit Protection Act.

Dun & Bradstreet believes that it would be more effective for matters other than 'data protection' – identified under these two sections as 'data security' to be dealt with as matters under the National Consumer Credit Protection Act. The benefits of consolidation of these areas under the National Consumer Credit Protection Act would be greater integration, simplified implementation and more effective oversight. Leaving them under separate jurisdictions perpetuates multiple issues, including the ongoing difficulty with coordination of legislative changes and striking/maintaining the appropriate balance between the outcomes and enabling the means to do so.

Today if ASIC increases or adds an expectation in relation to meeting NCCP obligations there is no mechanism that automatically seeks to consider corresponding changes as to achieve that outcome.

4.2 An example of material regulatory delay due to a lack of cross jurisdictional coordination

In 2001, ASIC highlighted issues with third party data gathering services, including that the Privacy Act did not deal with such matters effectively. Today, more than 15 years later these same issues remain unresolved. It seems likely that part of the reason for this is that solving these matters cuts across jurisdictions – jurisdictions that do not have a regular forum by which they interact.

As the use of data intensifies this issue is likely to become increasingly problematic.

4.3 Issues relating to how third parties gather personal information at the time of decisioning

There are two basic approaches which can be classified as either 'impersonation' or a 'secure courier' approach.

Dun & Bradstreet does not support the use of impersonation as a means of gathering data, and seeks instead to see the regulatory and legal issues in this area clearly rule out such practices by ensuring that the process is consumer driven, effectively transparent to all parties involved, and issues of liability are clearly and fairly addressed.

The most prevalently used approach today is 'impersonation'. These services via various technical means obtain an individual's internet banking ID and password, and then pretend to be that person and use those details to extract data to be used for, amongst other things, income and expense assessment and verification as well as creditworthiness assessments. As ASIC identified in 2001, such services raise issues and questions of legality that cut across multiple regulatory jurisdictions.

A detailed assessment and explanation developed externally of the current situation, the issues involved and suggestions as to effectively deal with this issue are provided in Appendix 1 with permission of the author.

4.4 Data ownership – is the right concept ownership or rights and obligations appropriate

Typically 'ownership' can be transferred (sold) and so is not perpetual. Whereas 'rights (and obligations)' can be perpetual and shared. Given data that is about someone remains about them even in the hands of others, ownership does not seem to be the appropriate principle to apply.

Dun & Bradstreet sees itself as a 'steward of personal information' responsible for respecting the rights of those to whom the data refers and meeting its obligations under the law.

However, to the extent that Dun & Bradstreet derives information from data about a person (such as in the case of a 'credit score') Dun & Bradstreet should have an ownership right to the precise means by which this is done (i.e. as a 'trade secret'). However, Dun & Bradstreet would not consider itself to own the information just as it would not seek to 'own' someone's name or other personal information. The Privacy Act deals with derived data under the Credit Reporting sections in a way that attaches obligations and responsibilities, but does not define ownership – a principle that Dun & Bradstreet supports.

4.5 Managing the costs of public data provision - best dealt with on a cost recovery basis

Dun & Bradstreet is of the view that funding for data provision should be on a cost recovery basis and linked to those that utilise the data for commercial gain. The pricing should be set such that it would allow the government to recoup the development and running costs involved in the provision of the data, including the cost of work to continually improve accuracy and maintain process evolution consistent with a standard (to be developed) for data exchange.

4.6 Coordinated public and private approach needed to meeting the demand for data science skills

Such skills are highly technical and take considerable time to develop. Currently they are in relatively short supply. Additionally, there is a growing need to ensure that oversight authorities have sufficient skills to discharge their duties.

These elements combine to create the need for a robust and coordinated effort to develop an increased supply of such skills. This is likely to evolve for more effective incentives to encourage those capable of developing the skills to seek the necessary education and training, for the education and training to be made effectively available and for those who can do the work to be able to readily choose to undertake such work in either the public or private sector. Currently there are substantial wage inequities between private and public sector positions requiring such skills, and this is thought to be causing issues with enabling regulatory development and enforcement to keep pace with industry development.

In addition to the pure technical skills, there is an equal if not greater shortage of skills in the 'soft side' of data science – the knowledge and skills needed to develop and implement the appropriate frameworks to ensure the intent in using data science and the actual outcome are well aligned and appropriately balanced from a compliance and culture perspective. The need here is 'continuous' – developing new legislation alone will not deliver the outcome, there needs to be effective ongoing oversight and enforcement – internally at organisations, as well as externally by government.

4.7 Requesting personal information to be deleted – potentially problematic in a number of ways

For example, in cases where the data has been shared in ways that are untraceable it could be highly impractical if not impossible to execute a request to delete such data. Similarly, if the request is limited to only that data which is currently held by the organisation, it may not address the underlying concern. Additionally, problems would arise if data that is legally allowed to be held in order to meet other societal objectives – such as credit reporting or birth, marriage and death records were required to be deleted at the request of the individual.

Further in relation to CCR data:
The answer here assumes that this question does not relate to correcting or deleting information that is in error, i.e. it is factually incorrect or precluded from being held by law.

Allowing an individual to request that data that is correct and allowed to be held, be deleted, would be highly unlikely to have a true benefit to the individual to whom it relates. In many instances it could have a detrimental effect, other than in instances where the data held cannot be reasonably be relied upon to accurately assess credit worthiness. Such might be the case if the individual's credit reporting data was negatively impacted by a natural disaster or some other event that was both clearly out of their control and likely to cause an error in the assessment of their level of credit worthiness in the future. The Credit Reporting Code of Conduct already caters for such instances and in fact requires that they be considered.

In relation to broader personal information:
There are already many mechanisms that enable access to data to be restricted – certain types of court data, for example.

There are already provisions that require data to be destroyed when there remains no further allowable use for the data. Rather than seek to develop further obligations, Dun

& Bradstreet recommends that more be done to ensure compliance with existing obligations.

4.8 Improving the management of data breaches includes prevention, detection and resolution.

In many instances where privacy has been breached (in relation to any of the six aspects defined under the Privacy Act) frequently there was not sufficient care taken to protect data in the first instance. Things like failing to encrypt data or allowing weak data access controls are frequently identified as the points of compromise or root cause of the data security breaches.

Whilst it is unlikely that 'perfect security' can be achieved, it is possible to ensure that reasonably effective preventive measures are taken and that an evolutionary program of maintaining what constitutes reasonably effective measures can be implemented.

Currently, the Privacy Act does not focus on effective detection or resolution of data breaches. It is understood that draft legislation was developed previously, but have yet to be enacted.

Whilst expansion of obligations may be useful in some areas, improved assurance (i.e. enforcement) of obligations is thought to be central to more effectively protecting personal information.

5. Appendix 1: Addressing immediate compliance issues with RHI

Given the fundamental objective of credit reporting is to enable effective risk assessment; key to achieving that outcome is being able to differentiate levels of risk based on account behaviour.

One means of enabling that is to enable the recording of 2 key items of information:

1. What is the conduct of the accounts, relative to the obligations for repayment; and
2. What are the obligations for repayment

The rolling 24 month RHI information enables the 1st of these items to be addressed.

Currently there is no mechanism that enables the 2nd matter to be reflected.

How might this be fixed - one simple solution could be:

Amend the regulations that feed into the definition of consumer credit liability information by adding just one more element:

(f) “change history in relation to items (a) through (e) and the nature of the terms and conditions that the RHI (if reported) reflects relative to whether those terms and conditions have been varied”.

This in conjunction with the existing obligation to keep credit reporting information complete, accurate and up-to-date would enable the development of refinements to the exchange of data enable the recording of the 2 key pieces of information and better achieve the intentions of both Part IIIA of the Privacy Act and the NCCP responsible lending legislation.

The data standards used to record this information could then be updated to include classification values of the nature of the terms, such as:

- Full Commercial Original terms;
- Formal Temporary Hardship Varied terms;
- Permanent Concessional terms.

For those situations where the credit provider had not granted a formal hardship variation (as defined under the NCCP Act), but has never the less chosen to delay exercising their original contractual rights, the account would be reported as operating under its “full commercial original terms”, so long as any correspondence with the consumer makes reasonable clear that this is the case.

Following is further context in relation to those elements of the legislation (Act and Regulations) thought to be relevant to giving effect to this outcome.

Relevant sections of ASICs Regulatory Guide 209 and the Privacy Act and Regulations

From RG 209 Credit licensing: Responsible lending conduct

RG 209.18

To determine whether a credit contract or consumer lease is unsuitable, the legislation states that you must make reasonable inquiries about the consumer. The legislation requires credit assistance providers, credit providers and lessors to:

(b) make reasonable inquiries about the consumer’s financial situation (i.e. to determine whether the consumer has the capacity to meet their payment obligations under the credit contract or consumer lease being considered); and (c) take reasonable steps to verify the consumer’s financial situation.

RG 209.30

The obligation to make reasonable inquiries about the consumer's financial situation requires you to find out about the particular consumer's current situation. This involves obtaining information about the consumer's actual income, expenses and other circumstances that are likely to affect their ability to meet the financial obligations of the proposed credit contract or consumer lease.

RG 209.33
Depending on the circumstances of the particular consumer, and the kind of credit contract or consumer lease they may acquire, reasonable inquiries could also include:

(c) the consumer's credit history (including the number of small amount credit contracts the consumer has been a debtor under within the previous 90-day period, and whether the consumer has defaulted on payments under those contracts);

From section 6 of the Privacy Act:

consumer credit liability information: if a credit provider provides consumer credit to an individual, the following information about the consumer credit is ***consumer credit liability information*** about the individual:
(a) the name of the provider;
(b) whether the provider is a licensee;
(c) the type of consumer credit;
(d) the day on which the consumer credit is entered into;
(e) the terms or conditions of the consumer credit:
(i) that relate to the repayment of the amount of credit; and
(ii) that are prescribed by the regulations;
(f) the maximum amount of credit available under the consumer credit;
(g) the day on which the consumer credit is terminated or otherwise ceases to be in force.

Referenced Privacy Regulation:

6 Consumer credit liability information
For paragraph (e) of the definition of consumer credit liability information in subsection 6(1) of the Act, the terms or conditions of the consumer credit are the following:
(a) how the principal and interest on the consumer credit are to be paid, namely whether:
(i) the principal and interest are to be paid in full; or
(ii) the principal and interest are to be paid, leaving a residual unpaid amount of principal and interest at the end of the term of the consumer credit; or
(iii) only the interest is to be paid;
(b) whether the term of the consumer credit is fixed or revolving;
(c) if the term of the consumer credit is fixed—the length of the term;
(d) whether the individual is a guarantor to another individual in relation to the other individual's credit;
(e) whether the consumer credit is secured or unsecured**; and**

(f) change history in relation to items (a) through (e) and the nature of the terms and conditions that the RHI (if reported) reflects relative to whether those terms and conditions have been varied.

6. Appendix 2: How credit risk models work; criticality of stable data

6.1 Overview of Credit Scoring

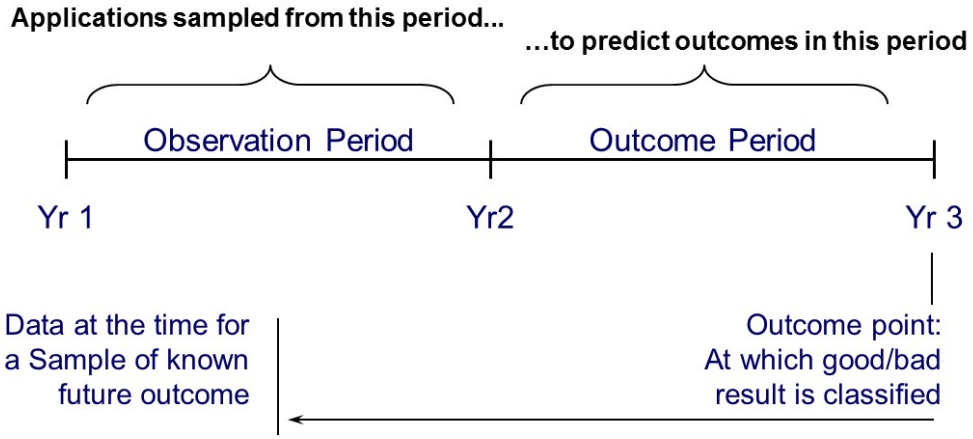
Credit scoring has been in continuous use since the 1940's to predict whether or not credit extended to an applicant is likely to be repaid. Credit scoring is widely used to determine who will get credit, how much credit they should get, and what operational strategies will be employed to manage the credit risk over time. It is part of a dependable assessment of a person's credit worthiness since it is based on actual data.

The Fundamental Principle in Credit Scoring:

"Past Experience will be predictive of future performance"

The correlation between data available at the time of making the decision and a known outcome at a point in the future is determined.

An illustrative example of a credit score used to assess credit applications is developed.



Each item of information known at the point of decision is analysed to determine if it is predictive of the future outcome.

Characteristic analysis of residential status

Attribute	# good	% good	# bad	% bad	odds	index
Owners	4356	27	157	11	28	249G
Buyers	6578	40	365	25	18	162G
Renters	4569	28	876	59	5	213B
LWP	876	5	76	5	12	103G
TOTAL	**16379**	**100**	**1474**	**100**	**11**	**100**

Odds - The ratio of goods to bads
5:1 = 5 goods for every 1 bad

Statistical techniques are then used to assign points to each characteristic are then assigned.

Predictive characteristics	Points
Residential status	
owner	+40
buyer	+30
renter	-25
LWP	0
Time & Address	
< 1 year	-80
1-2 years	-60
2 years +	+20
Home phone # provided	
yes	0
no	-70
Time in job	
<2 years	-55
2-5 years	-40
5 years +	+80
CR defaults	
yes	-285
no	0
Plus up to 20 others	

The scorecard can then be used to make an objective assessment of the level of credit risk associated with an application.
It is important to note this is only 1 aspect to be considered; an assessment of capacity to repay must also be conducted to see if the additional credit is affordable.

Most Critical:
The time it takes for the outcome to be known is frequently 18 months. Given that the decision made can only relate to information available at the time, it is necessary for the use of a credit score for that same sort of data to be available in the future to make decisions based on the scores prediction of the outcome.

This means that the sort of data available – including its underlying meaning needs to be ‘stable’ over a reasonably long period. Sudden shifts in the available decision data cause issues with the application of traditional credit scoring, as it violates the underlying assumption that:

“Past Experience will be predictive of future performance”

7. Appendix 3: Answers to Specific Issues Paper Questions

QUESTIONS ON HIGH VALUE PUBLIC SECTOR DATA

What public sector datasets should be considered high value data to the: business sector; research sector; academics; or the broader community?

Tax debt data

Overdue company debts are one source of data that would be substantially important for the provision and management of credit. The ATO is arguably one of the largest lenders in Australia owned billions and billions of dollars in overdue tax at any one time, yet no information is readily available about these debt at an individual 'borrower' level (be that an individual or a business) for use in making credit decisions. Given that tax debt ranks above all other (including secured debt) this creates a 'blind spot' that results in credit losses that are higher than they might otherwise be…and those credit losses are borne by all those who borrow in the firm of higher rates for all those who do pay their debts.

Additionally – if such data were shared, it would likely lead to improved collection of overdue taxes, and reduce the very material costs of collecting these overdue amounts.

What characteristics define high value datasets?

1. Data that the highly relevant to a specific types of decision. In the case of overdue tax (a form of debt) in relation to credit decisions as an example.
2. Data that is identifiable i.e. includes sufficient data to enable matching to the individual or entity to which it relates.

What benefits would the community derive from increasing the availability and use of public sector data?

1. Better credit decisions for small business owners – reducing the risk of them over borrowing and other financial difficulties.
2. Increased tax collection…as the consequence of non-payment would be greater due to increased consequences that would arise…such as reduced capacity to borrow.

QUESTIONS ON COLLECTION AND RELEASE OF PUBLIC SECTOR DATA

What are the main factors currently stopping government agencies from making their data available?

In many cases doing so is not within the scope of their responsibilities. As a consequence no economic mechanism is in place that would facilitate the required development and ongoing activities required.

How could governments use their own data collections more efficiently and effectively?

1. By developing a common data management framework – that sets out clear accountability, policies, processes and procedures, monitoring of activity and outcomes, and reporting to ensure visibility of performance.
2. Developing standards for data storage, access control and exchange.
3. Ensuring sufficient resources (funding and skills) are available to undertake the work to effectively manage the collection, storage, and provision of the data.

Should the collection, sharing and release of public sector data be standardised?
Yes.

What would be the benefits and costs of standardising?
Standardisation benefits a broad group of parties by ensuring consistency of data meaning and enabling efficient development of the means of acquiring, consuming and utilising the data in research, analysis and decision making.

Assuming that standardisation is undertaken effectively, the costs are inherently lower than non-standardisation when the full lifecycle of data is considered. This is due to the benefits of consistency in both development of acquiring, consuming and utilising the data, but also the ongoing maintenance of those means.
Additionally, without standardisation, many activities that could be undertaken would simply be too difficult and costly – meaning their associated benefits could never be realised.

What would standards that are 'fit for purpose' look like?
Characteristics of 'fit for purpose' standards include them being competitively neutral, being publically available, being easily evolved as changes inevitably bring matters not previously considered into play, or better options are identified. ISO standards are a clear example of how standards work well.

What criteria and decision making tools do government agencies use to decide which public sector data to make publicly available and how much processing to undertake before it is released?

Principles based criteria – likely achievement of a balanced set of benefits – and a consistent framework/process for making decisions about whether or not to release data and what data processing is required prior to that release, are thought vital to effectiveness. These two elements will help establish consistency, fairness, predictability, and efficiency in relation to how decisions about data release are to be made. A common framework across government would be far more helpful than allowing each area within government to determine how this process will work.

What specific government initiatives (whether Australian Government, state, territory or local government, or overseas jurisdictions) have been particularly effective in improving data access and use?

The Document Verification Service[9] (DVS) is a national online system that allows organisations to compare a customer's identifying information with a government record.

The DVS is a secure system that operates 24/7 and matches key details contained on Australian-issued identifying credentials, providing a 'yes' or 'no' answer within seconds.

The DVS helps organisations build greater confidence in the identities of their clients. This helps protect governments, businesses and Australians from identity crime.

[9] http://www.dvs.gov.au/Pages/default.aspx

QUESTIONS ON DATA LINKAGE

Which datasets, if linked or coordinated across public sector agencies, would be of high value to the community, and how would they be used?

Bankruptcy, overdue tax data, federal and state court records (relevant to credit and debt matters only).

Which rules, regulations or policies create unnecessary or excessive barriers to linking datasets?

A lack of coordination across regulatory jurisdictions (e.g. ASIC, OAIC, and APRA in the case of credit provided by banks). Obligations imposed related to one jurisdiction are not coordinated with obligations relating to enablement. One clear example is the increased expectations of both ASIC (in relation to Responsible lending and in particular income and expense verification) and APRA (re sound risk management practices) and the constraints in relation to Privacy re: data access and other matters. These issues were identified in 2001 by ASIC[10] as needing to be addressed across jurisdiction, however this has not yet happened. It is understood that there is no regular form for ASIC, OAIC, and APRA along with perhaps Treasury) to consider cross jurisdictional matters.

Refer to Section 5.2 above.

How can Australia's government agencies improve their sharing and linking of public sector data?

Establish forums that incorporate the OAIC with other regulatory agencies where access to (and protections of) personal information are involved and may enable improvements to practices. E.G. a forum that includes ASIC, OAIC, APRA, and Treasury in the case of consumer credit matters impacting Australian Deposit Taking Institutions (Banks).

QUESTIONS ON HIGH VALUE PRIVATE SECTOR DATA

What private sector datasets should be considered high value data to: public policy; researchers and academics; other private sector entities; or the broader community?

First and foremost personal information that the individual is willing to have shared – so long at the process for sharing is based on ensuring several fundamental principles:

A. That the individual controls access.
B. That the process is transparent to all involved: the individual, those that hold the date that the individual seeks to have released, the recipient who the individual seeks to provide the data to.

[10] http://download.asic.gov.au/media/1933166/what-do-you-want-to-do-with-acctaggreg_issues.pdf

C. The process is secure, and includes effective authentication.

D. That the data that is exchanged can be reviewed and challenged by the individual to whom it relates in relation to accuracy.

Second, access to de-identified datasets should be readily available for analysis. However, there should be a means of restricting the results of analysis being inked back to the individual.

The means to do that are technical, but can be explained as enabling 'association of data' but without identification to who the information relates. More detail can be provided on this if there is interest from the Productivity Commission.

In each case cited, what characteristics define such datasets?

Rather than a list of criteria with regard to each data set, there should be a mechanism established that is used to objectively determine 'potential public value' and evaluates effectiveness of achieving sufficient privacy protection. In both of the above listed examples – people seeking to share data that others hold about them, and data de-identified for the purposes of analysis and research.

What would be the public policy rationale for any associated government intervention?

Though there are instances where data about someone need not have their specific consent at the time to release (e.g. criminal records between relevant law enforcement agencies) the bias should be shifted to enabling an individual to more effectively control of their rights re: the access and sharing of data about them, rather than the current approach which can see such efforts thwarted either as an intention or as a consequence of impracticalities that make informed data sharing difficult.

What benefits would the community derive from increasing the availability and use of private sector data?

Re: People seeking to share data that others hold about them

Individuals would be in better control of the data about them, better enabled to exercise their right of access and better protected by processes to help to ensure that the obligations to protect the data about them are clearly established and enforced.

Re: Data de-identified for the purposes of analysis and research

Allowing access to data for research enables questions to be asked (and answered) that would not have been thought of to ask in the first instance. Measuring the consequences of decisions and actions taken is fundamental to evolution. This is how people's knowledge grows and can be used to improve many elements of life.

QUESTIONS ON ACCESS TO PRIVATE SECTOR DATA

Are there any legislative or other impediments that may be unnecessarily restricting the availability and use of private sector data?

Answer specifically relates to credit reporting.

Yes.

Current legislation in relation to CCR content is highly prescriptive and precludes the sharing of any data that is not specifically listed for the purpose of assessing credit worthiness. Key elements that are current NOT allowed:

- Current balance
  The actual debt that is outstanding at any point in time. This information is different to the credit limit (the maximum possible exposure which in the vast majority of cases is not reflective of behaviour and so can only be used to infer conduct – a much weaker means of prediction future repayment risk.

- Actual payment data
  Another objective measure of behaviour that is predictive of repayment risk. Without this information, inferences from other data must be made which results in reduced risk assessment accuracy.

Refer to section 4.3 above.

Should these impediments be reduced or removed?

Yes.

Refer to section 4.3 above.

What are the reasonable concerns that businesses have about increasing the availability of their data?

From a commercial perspective some, such as those who already hold majority or substantial market share positions, might argue that is it 'reasonable' to seek to hoard data to protect against competition. It is Dun & Bradstreet's view that such a reason for impeding supply of data is not justified.

Allowing such restriction to the exchange of data by institutions that hold such positions comes at the cost of smaller competitors and most importantly consumers – who ultimately have less choice as a consequence. This is thought to be a significant factor in the slow uptake of CCR in Australia and corresponding delay in achievement of its potential benefits.

New Zealand has 1 large bank with <50 % market share. In contract Australia has 4 Major Banks 70%+ market share. Another market difference is that full CCR participation is allowed for Telcos and Utilities, unlike Australia where it is restricted. Additionally, there is compliance uncertainty with regard to RHI at present in Australia does not exist in NZ.

Participation is nearly at critical mass in NZ. However, it should be noted that NZ's largest bank is yet to begin contributing full CCR data.

What principles, protocols or legislative requirements could manage the concerns of private sector data owners about increasing the availability of their data?
RE: Credit Reporting:

As per this submission, enhance the potential value of credit reporting by aligning the Australian model more to that of the World Bank's recommendations. If that is not deemed acceptable, or if that is still not sufficient to generate firm commitment to critical mass participation in the near term then consider the following:

- Mandating CCR data supply; and
- Removing the complexity of the current 3 tiered credit reporting system – those that share only the historic negative information, those that are restricted (by the legislation) to sharing only 4 of the 5 new data sets, and those that opt in to sharing all of the new data. A single tiered widely adopted system will be enables the greatest level of benefits and be far less complex for all parties to implement, oversee and use.

RE: Data beyond the scope of Credit Reporting

- Requiring consistency of access to personal data that the individual chooses to share

Should the collection, sharing and release of private sector data be standardised in some way?
Yes. By establishing principles-based legislative limits, but leaving the practical delivery detail to the industry. Not taking this approach and seeking instead to be highly prescriptive within legislation; such as in the case of CCR within the CR Code, which while industry drafted the OAIC required substantial editing. This combined with the very normal need to continually evolve standards as new situations previously not considered arise and they inevitably do. This is how ISO standards are managed. The inability to do so in the case of credit reporting, has contributed to the delay in adoption of CCR and corresponding delay in achievement of its potential benefits.

How could this be done and what would be the benefits and costs?
Refer to suggestions in relation to moving most of the credit reporting legislation out of the Privacy Act and placing it under the relevant credit conduct legislation (NCCP)….so that as consumer credit protection obligations evolve so to can the means of enabling them under Section: 5.1 above.

What would standards that are 'fit for purpose' look like?
There are 2 levels of standards to consider:

1. Consistent legislative principles about data; and
2. Technical data management standards.

For the first, such standards focus on the outcomes that have to be achieved and or avoided – rather than on the means. This will increase dramatically the useful life of the standards. Today, the Credit Reporting legislation does not follow this approach and some parts of which are already problematic as they focused at an inappropriate level of detail. Specification of individual field level values is not appropriate.

For the technical standards, examples such as XML protocols work effectively as do the mechanisms that manage their ongoing evolution.

To what extent can voluntary data sharing arrangements — between businesses / between businesses and consumers / involving third party intermediaries — improve outcomes for the availability and use of private data?

To be clear, the issue here is not data sharing but rather a common form of access, so that data beyond the scope of credit reporting can be shared easily at the request of the individual.

To date, an Open API approach to access such data whilst an available technical option has not been widely adopted. As a consequence alternative methods that rely on impersonation of the individual have been developed. To date, these too have not been widely adopted presumably due to data security, reputational risk issues as well as commercial concerns. Those taking up such approaches are typically smaller credit providers and market innovators who are attempting to overcome the consequence of highly limited credit reporting data (limited content actually available as well as potentially available even if there were wide CCR participation due to the constraints on what data can be included.

For more, detail on the differences between an Impersonation versus a Secure Courier model for enabling access to an individual's internet banking data held by another financial institution, please refer Appendix 4.

How could participation levels be increased?
With regard to non-credit reporting financial data such as a consumer has access to via their internet banking – it is recommended that the use of Open APIs be mandated.

For more, detail on the differences between an Impersonation versus a Secure Courier model for enabling access to an individual's internet banking data held by another financial institution, please refer Appendix 4.

Would such voluntary arrangements raise competition issues?
Most likely, yes. Similar to the credit reporting Principles of Reciprocity and Data Exchange (the competition relevant bits of which were ACCC Authorised), a scheme that is voluntary but seeks to establish a common market approach may require similar ACCC authorisation.

However, from a practical perspective it is thought that rather than reduce competition, allowing standardisation, (once it is widely adopted) or mandating the principle of reciprocity is most likely to facility and encourage increased competition and innovation.

How might this change if private sector information sharing were mandated?
Mandating Open APIs would ensure that access to data was made simpler and facilitates a material change from incumbent credit providers having primary control over what data is available for decision making to place the consumer in control.

Is authorisation (under the Competition and Consumer Act 2010 (Cth)) relevant?
If the government were to mandate reciprocity of data exchange, then a large aspect of anti-competitive risk would be addressed. This assumes that the process for developing data exchange standards was not allowed to be abused, so as to make standards so hard to achieve that they end up being exclusionary.

What role can governments usefully play in promoting the wider availability of private datasets that have the potential to deliver substantial spill over benefits?
In terms of data beyond the scope of credit reporting (such as access to for verification of income and expenses etc.):

By adopting a policy requiring Open API that addresses the key factors of:

1. That the individual controls access.
2. That the process is transparent to all involved: the individual, those that hold the date that the individual seeks to have released, the recipient who the individual seeks to provide the data to.
3. The process is secure, and includes effective authentication.
4. That the data that is exchanged can be reviewed and challenged by the individual to whom it relates in relation to accuracy.

This will ensure that the individual's right of access is effectively enabled in a modern way that improves awareness, safety and operational efficiency as well as innovation.

Who should have the ownership rights to data that is generated by individuals but collected by businesses?
D&B believes there is a question of whether ownership of personal information is the right question in the first instance.
"Ownership" can be transferred (sold)…and so is not perpetual…where as "rights (and obligations)" can be perpetual and shared.
Given that data that is about someone remains about them even in the hands of others.
D&B sees itself as a "steward of personal information" responsible for respecting the rights of those to whom the data refers and meeting its obligations.

To the extent that D&B derives information from data about a person…such as in the case of a "credit score" D&B should have an ownership right to the precise means by which this is done (as a 'trade secret'), but the individual about whom the data derived data relates (so long at that data remains reasonably identifiable as relating to them) should hold rights to that data as they would in relation to the data upon which the derivation was based.
This is how the Privacy Act deals with derived data under the Credit Reporting Sections – a principle that D&B supports.

Ground floor, 479 St Kilda Road | 13 23 33
Melbourne, VIC 3004 | dnb.com.au

For which data does unclear ownership inhibit its availability and use?

This applies most particularly to personal information.

QUESTIONS ON CONSUMER ACCESS TO, AND CONTROL OVER, DATA

What impediments currently restrict consumers' access to and use of public and private sector data about themselves?
Based on comparisons with other markets, the 'restriction of access' is thought to be largely self-imposed resulting from a limited or lack of awareness and understanding of their rights of access and of what data exists and is being collected about them, as well as how it is being used.

One example of note:

The use of various elements of 'meta data' captured as part of many processes the individual undertakes is searching and applying for credit.
Some credit providers determined there to be a correlation between certain metadata elements and the risk of future non-repayment of credit and are using such information in their assessments of repayment risk. For example:

- How certain questions are answered relative to choices they are given – e.g. if allowed to select their desired loan amount, how close is their choice to the maximum choice option and if the choice is presented in the form of a 'slider' how quickly they move the slider 'up the scale';
- How long an applicant's mouse 'hovers' over certain questions or sections of a web page;
- The number of spelling mistakes, or back space strokes.

Whilst there may be a correlation between these data elements and the risk of non-repayment, there is clearly no 'causal' effect. Additionally and more importantly many of these elements can easily be manipulated so that their capacity to accurately predict future non-repayment is a risk of becoming unstable over time as people learn about such elements and seek to manipulate their 'web behaviour'.

Is there scope to streamline individuals' access to such data and, if there is, how should this be achieved?
Yes, by increasing transparency about what information is being used to make a decision and making this available at the point of decision.

Are regulatory solutions of value in giving consumers more access to and control over their own data?
Potentially yes.
Clarifying the obligations to be more specific and timely – relative to the decision being made – is likely to assist consumers to understand the consequence of the data that is being used in context, and is seen as likely to drive an increased awareness of consumer's rights of access and other rights and the use of them.

Are there other ways to encourage greater cultural acceptance amongst businesses of consumer access to data about them?

There seems to be something of a slow progression toward businesses seeing benefit in greater openness about what they are doing. Some examples are clear in the peer-to-peer lending industry, where both investors and borrowers are actively being made more aware of the process and data used in those processes. It is however, expected to be a slow migration from the historic paradigm of control of information and secrecy equating to power (and profits) and the new paradigm of businesses seeking to a realising incremental value from greater transparency.

What role do third party intermediaries currently play in assisting consumers to access and use data about themselves?
Refer to appendix 4

What barriers impede the availability (and take up) of services offered by third party intermediaries?
Refer to appendix 4.

What datasets, including datasets of aggregated data on consumer outcomes at the product or provider level, would provide high value to consumers in helping them make informed decisions?
Refer to appendix 4.

Relative to obtaining credit:
Data about income and expenses (not just debt payments).

Given most Australians do not maintain a detailed budget (so don't personally have this data to hand) and even if they did the data would need to be independently verified to a reasonable degree so as to ensure it was accurate.
Consumers would benefit greatly by processes that:

1. Gather the data about them directly from its source (with the party who holds the data being aware of this happening (but not able to interfere assuming appropriate authentication)
2. Present the retrieved data in an understandable form to the consumer in the context of the decision the data will be used to make
3. Enabling the consumer to challenge (but not directly change) the accuracy of the data; and then
4. Release it for use in making the decision.

What criteria should be used to identify such datasets?
A mechanism that is focused on assessing public interest of access to data could be established with a clear mandate and process to be followed. As the use of data in decision making continues to grow (likely to be at an exponential rate), a mechanism that is dedicated to continual consideration is thought to be a far better approach than awaiting legislative review and update to things like the privacy Act – where the history of change has been one material review in 24 years.

What, if any, barriers are impeding consumers' access to, and use of, such data?
The matter of data rights and priority of those rights is thought to be fundamentally what is delaying the move to a greater level of customer control over personal information.

Additionally, enabling an effective means of consumer driven access is thought to be key to enabling consumers to exercise their rights more effectively.
Refer to appendix ## with regard to how

RE: Private Sector Data:
The greatest barrier is the current capacity of the data holder to choose not provide ready and effective access to the data – such as via an Open API. Without such some obligation to do so currently 3rd parties involved in gathering private sector data are primarily utilising some means of impersonation to obtain the data by pretending to be the consumer.

RE Public Sector Data:
There is the example of the government's Data Verification Service (DVS). Prior to the establishment of the DVS the government was the subject of the impersonation method – with third parties obtaining the data by pretending to be the consumer. It was a conscious choice by the government agencies that hold the data used in the DVS to stop the impersonation method (seeing the inherent risks it presents) and to enable via an Open API a means of data verification.

NOTE: the DVS model which does not supply raw data in return but rather an indication of whether or not data provided is verified works where the question is only one of verification and a 'yes' or 'no' answer to a question is sufficient to proceed. That is not the case with regard to gathering income and expense data where greater detail than a simply yes or know is required and where small differences may result in a 'no match' when there is not material difference. In short, processes need to cater for the degree of precision needed in the decision.

QUESTIONS ON RESOURCE COSTS OF ACCESS

How should the costs associated with making more public sector data widely available be funded?
D&B advocates a market based approach as is currently done with some elements of public data. For example, credit reporting businesses pay for access to court judgement data, and bankruptcy information. This would allow the government to recoup the development and running costs involved in the provision of the data, including the cost of work to continually improve accuracy and maintain process evolution consistent with a standard for data exchange.

To what extent are data related resources in agencies being directed towards dealing with data management and access issues versus data analysis and use?

The answer to the question is largely unknown, which in itself is an issue. It would be useful to have a central point or easily accessible common mechanisms for gaining an understanding of what data is available, how and under what conditions it can be accessed and at what if any cost.

What pricing principles should be applied to different datasets?
Refer the previous answer:

D&B advocates a market based approach as is currently done with some elements of public data. For example, credit reporting businesses pay for access to court judgement data, and bankruptcy information. This would allow the government to recoup the development and running costs involved in the provision of the data, including the cost of work to continually improve accuracy and maintain process evolution consistent with a standard for data exchange.

What role should price signals play in the provision of public sector data?
It is not expected that the sale of public sector data would be undertaken on a 'for profit basis'; but would rather be undertake on a cost recovery basis. This would ensure that the government recoups the development and running costs involved in the provision of the data, including the cost of work to continually improve accuracy and maintain process evolution consistent with a standard for data exchange

Is availability of skilled labour an issue in areas such as data science or other data specific occupations?
Yes.

Such skills are highly technical, and are in relatively short supply. There is also the need to ensure that oversight authorities have sufficient skills to discharge their duties. The current shortage, the highly technical nature of the skills and the effort and time it takes to develop them, as well as the need for more by both industry and government suggests that more needs to be done to meet this demand. There needs to be effective incentives to encourage those capable of developing the skills to seek the necessary education and training, for the education and training to be made available and for those who are able to do the work to readily choose to undertake such work in industry or government. Currently there are substantial wage inequities between private and public sector positions requiring such skills and this is causing issues with enabling regulatory development and enforcement to keep pace with industry development.

In addition to the pure technical skills, there is an equal if not greater shortage of skills in the 'soft side' of data science – the knowledge and skills needed to develop and implement the appropriate frameworks needed to ensure the intent in using data science and the actual outcome are well aligned and appropriately balanced from a compliance and culture perspective. The need here is 'continuous' – developing new legislation alone will not deliver the outcome, there needs to be effective ongoing oversight and enforcement – internally at organisations as well as externally by government.

Is there a role for government in improving the skills base in this area?
Yes.
There needs to be effective incentives to encourage those capable of developing the skills to seek the necessary education and training, for the education and training to be made available and for those who are able to do the work to readily choose to undertake such work in industry or government. Given the expectation that demand for such skills will be increasing for the foreseeable future, it is thought to be vital that we implement a coordinated approach to ensure this demand is met be developed and effectively implemented.

QUESTIONS ON PRIVACY PROTECTION

Context taken from the PCs issues paper:
Trust - For the economic benefits of data to be fully realised, it will be essential to maintain individuals' and businesses' confidence and trust in how data is collected, stored and used.
Privacy - A considerable proportion of data being collected, stored and transmitted, increasingly electronically, consists of personal data about individuals, some of it potentially sensitive and which the individuals concerned may, legitimately, not wish to have distributed widely. Globally there is growing debate over how societies should consider privacy against the economic benefits associated with the rapidly growing volume of data being generated and used.

What types of data and data applications (public sector and private sector) pose the greatest concerns for privacy protection?
The greatest privacy concerns parallel the types of data and data its application (uses) that it can influence relative to the potential consequences to the individual. Areas of high potential consequence would include: safety, health, areas thought to be 'sensitive information' as defined under the Privacy Act and finance.
Rather than seek to list the data and its current applications, it may prove to be more effective to begin with list the outcomes or areas of highest potential consequence, as it is expected that over time these will remain more stable. Following this we recommend developing a process for evolving the list of data or data applications that may influence these outcomes, as this is likely to evolve more quickly (in particular as it is one of the objectives of data science to in fact identify such new items and uses of data.)

How can individuals' and businesses' confidence and trust in the way data is used be maintained and enhanced?
'Clear rules and a fair referee' – Legislation that is clear with regard to intended outcomes, transparency and sufficient awareness by all parties involved (including those charged with oversight) of what is happening, this includes what is being done and the consequences, rights of redress that include efficient practices to achieve resolution and consequences (and remedies) that are fair and proportionate so as to support and encourage the intended outcomes and discourage behaviour that is inconsistent with those outcomes.

What weight should be given to privacy protection relative to the benefits of greater data availability and use, particularly given the rate of change in the capabilities of technology?
It is unlikely that the tide of ever more data and increasing capacity to link, analyse, and take action in relation to and individual can be reversed. Protections are likely to be more effective if describe clearly the outcomes to be either achieved or avoided and not seek to prescribe (either by enabling or preventing specific means). Industry will continue to evolve means – causing legislation that is specific about means to become dated ever more quickly.

Are further changes to the privacy related policy framework needed?
Yes. The current structure is overly focused on restricting specific means of data use in a number of areas. Instead it should be clear on the objective it's aiming to achieve. Ensuring that outcome clarity is achieved also helps to discourage seeking to find ways of circumventing the intention of the law via finding alternative means to achieve the outcome intended to be prevented.

Refer to the sections relating to RHI and contract variation issues as a clear example.

What are the specific changes and how would they improve outcomes?

It should restore achievement of the underlying objective of Part IIIA (Credit Reporting) of the Privacy Act – that being:

> *"One of the objects of the Privacy Act is to facilitate an efficient credit reporting system while ensuring that the privacy of individuals is respected. In recognition of that objective, the laws about credit reporting are intended to balance individuals' interest in protecting their personal information with the need to ensure that credit providers have sufficient information available to assist them to decide whether to provide an individual with credit. "The Australian credit reporting system also helps ensure that credit providers are able to comply with their responsible lending obligations under the* National Consumer Credit Protection Act 2009 *administered by the Australian Securities and Investment Commission (ASIC)."* [11]

by enabling the capacity to distinguish between those meeting the obligations of an original contract's terms and these meeting the obligations (almost always more lenient) of a temporary variation to the original contract.

Have such approaches been tried in other jurisdictions?
Australia has what is understood to be the most prescriptive regulatory regime in relation to Credit Reporting. Many other G20 markets already enable the exchange of considerably more detailed information than what is allowed in Australia. So they have not faced this issue, but rather have avoided by being less prescriptive in the first instance.

How could coordination across the different jurisdictions in regard to privacy protection and legislation be improved?
ASIC, APRA, Privacy regulation is not coordinated by design. Refer to section 5.2 for further comment on this matter.

How effective are existing approaches to confidentialisation and data security in facilitating data sharing while protecting privacy?
Firstly, it is important to ensure that this question addresses what is meant by 'data security'. It is often considered as only protection from external unauthorised access. However, The Privacy Act's definition is broader and includes protection from: "misuse, interference and loss; and from unauthorised access, modification or disclosure." This broader perspective means not only external threat but internal ones. It also covers every use other than the intended one and those specifically prescribed secondary uses linked to each original use.

One way of protecting personal data is to 'de-identify it.

There were two major CCR pilot studies – one by Dun & Bradstreet another by a competitor – which were undertaken prior to the Privacy Act changes and utilise a methodology to de-identify data for research purposes. These sorts of approaches can be effectively used, in particular where there is no interest in directly taking action in relation to finding at an individual level, as is the case in undertaking research. The processes of de-identification that were used were heavily scrutinised and thus far Dun & Bradstreet have not do concerned raised about our study and are not aware of any concerns being raised about the security of the data involved in the other study.

[11] *[https://www.oaic.gov.au/privacy-law/privacy-act/credit-reporting]*

With regard to data that has not been de-identified:

The Privacy Act calls for monitoring by CRBs of CP to consider matters of data security (all six aspects); and where risks are identified to undertake audits, agree remedial action where necessary, to monitor remedial action and report findings to the OAIC.

The OAIC is able to undertake own motion reviews of both CRBs and CP.

What lessons from overseas jurisdictions can Australia learn from regarding the use of individuals' and businesses' data, particularly in regard to protecting privacy and commercially sensitive or commercially valuable information?
In many jurisdictions where privacy has been breached (in relation to any of the 6 aspects defined under the Privacy Act) frequently there was not sufficient care taken to protect data. Things like simple encryption was not done, access controls were weak – such as easily identifiable sharing of access credentials, are frequently identified as the points of compromise or root cause of the data security being compromised.

Whilst it is unlikely that 'perfect security' can be achieved, it is possible to ensure that reasonably effective measures are taken and that an evolutionary program of maintaining what constitutes reasonably effective measures can be implemented.

What are the benefits and costs of allowing an individual to request deletion of personal information about themselves?

Limited to CCR Data:
The answer here assumes that this question does not relate to correcting or deleting information that is in error, i.e. data that is factually incorrect or precluded from being held by law. Allowing an individual to request that data that is correct and allowed to be held is deleted, would be highly unlikely to have a true benefit to the individual to whom it relates. In many instances it could have a detrimental effect, other than in instances the data held cannot be reasonably be relied upon to enable it to be used for assessment of credit worthiness. Such might be the case if the individual's credit reporting data was negatively impacted by a natural disaster or some other event that was out of their control and likely to cause an error in the assessment of their level of credit worthiness in the future. The Credit Reporting Code of Conduct already caters for such instances and in fact requires that they be considered.

In relation to broader personal information:
There are already many mechanisms that enable access to data to be restricted – certain types of court data for example. Typically such restriction is 'built in' to the process of this data being collected.

Contrary to what many might expect organisations frequently do not consolidate or link all of the data they may hold about an individual for a variety of reasons, including the fact that is it not a 'perfect science' or they form a view that there is no commercial need or obligation to doing so.
Even those that do attempt to link all of the data they hold about an individual together face the challenges of 'matching records' correctly in every instance. Things like name spelling variations, Mike Vs Michael, or the misspelling of Micheal may result in records that do relate to one person being thought to and treated as if they belong to multiple

people. Because generally the consequences of 'over matching' (attributing information to someone that is in fact not about them) are worse than under matching, as there is an in-build bias that would result in not all data about an individual being deleted upon request.

There are already provisions that required data to be destroyed when there is no further allowable use for the data.

In what circumstances and for what types of information should this apply?
With regard to CCR Data:

This data is specifically collected is for the purpose of making credit worthiness assessments – which would be totally undermined if data that is correct and allowed must be deleted simply on request. In such instances, those who have data that may suggests potential issues with their credit worthiness could seek to have such data removed, thereby leading to assessments that are incorrect. This is in fact already an issue resulting from the practices of credit repair companies who seek to abuse the External Dispute Resolution (EDR) scheme structure to have 'accurate' but inconvenient' data removed. Such companies profit from this activity which sees their clients from a debt perspective 'put in harm's way', by increasing the odds of them getting credit that is unsuitable.

What competing interests (such as the public interest) or practical requirements would indicate that the ability to request deletion should not apply?
In instances where an individual could use such a request to obviate their responsibilities – such as payment of debts, performance under a contract or adherence relative to a court order. Also in instances where there is a completing obligation to hold information, such as for statutory auditing purposes.

QUESTIONS ON DATA SECURITY

Is data breach notification an appropriate and sufficient response?
Notification is appropriate, as it may not be apparent to the holder of the data all of the potential risks that a breach of data security might hold. Also, individual may be able to do something to protect themselves or at least be able to better react to the situation if they are informed.

Whether breach notification is sufficient is likely to depend on the circumstances of the breach. Given the nature of data being perpetual, it is possible that the consequence of a breach may not be known for a period of time. It would seem reasonable that some limitation be placed on time after a breach that greater consequences can be applied, though this too many depend on the nature of the breach and surrounding circumstances.

8. Appendix 4: Data Gathering in relation to Capacity to Repay

There are an increasing number of alternative data gathering services that utilise various means of accessing an individual's internet banking to obtain transaction and account details.
The view that there is potential value from such "alternative data" for the purpose of making credit decisions and meeting responsible lending obligations is thought to be wide spread….at least in the credit provider community.

To be clear – such data is of incremental value – enabling assessment of the capacity to repay – and not as a substitute for credit reporting.

Suggestions that such information can effectively be used as a substitute for credit reporting are considered misguided at best. Credit reporting and its inherent independence as a data source are vital to effective assessment of credit risk (the likelihood/willingness to repayment) which is different capacity to repay. Both elements are required by commercial prudence (and by law under NCCP legislation) to be considered in assessing credit decisions.

The recently formed FinTech Australia 12– an industry body for FinTech start-ups established to work with Government's newly created FinTech Advisory Group - listed this topic as one of their priorities to solve, so it is clearly something that community seeks to progress.

Yet with all the data's potential to improve decision making and the vocal and visible support of this industry sector with the formation of the Government's FinTech Advisory Group the take up rate of these services (which have been around for over 15 years) is very low with well over 90% of the credit market and all of the 4 major banks yet to use them for widely this purpose.

Further, with a regulatory obligation to obtain and consider income and expense information in credit assessment under the National Consumer Credit Protection Act and value in using such data to predict credit risk, why aren't more credit providers using such services?
There seem to be 2 main issues:

1. Risk – Various Regulatory risks (from overlapping jurisdictions), IT security, legal liability and associated reputational consequences
2. Commercial Interests - (assuming that the Regulatory issues can be resolved) - Who has more to gain or lose from these new means of sharing data

[12] FinTech Australia have prepared a paper for the Department of Treasury outlining their priorities for reform of the Australian Financial Services Industry. That files is attached here as Appendix B.

Overwhelmingly these issues are linked to how the data is obtained and the liability in the event of a loss, and as a result it is important to understand who is involved and how it all works.

The remainder of this paper will seek to illustrate:

- The 4 process participants and their key interests
  - The individual
  - The Alternative service Vendor
  - The Current Credit Provider
  - The Future (or potential) Credit Provider

- The 2 primary approaches being taken to accessing the data (and how they differ)

- The various regulatory issues (which cut across multiple jurisdictions) that seem to be intertwined, including:
  - Privacy;
  - E-payments Code / Trade Practices / Contract Law;
  - National Consumer Credit Protection Act – Responsible Lending; and
  - ACCC – Anti Competition

These issues are not 'new'… many were highlighted in an ASIC report published 15 years ago[13]. From the executive summary of: CONSULTATION PAPER 20 Account aggregation in the financial services sector:

> *"Consumer and regulatory issues identified*
> *The main consumer and regulatory issues generated by account aggregation services include:*
>
> - *disclosure – including disclosure about the risk of using an aggregation service;*
> - *liability for unauthorised transactions – it is important to determine for losses caused by unauthorised transactions. For example, under the current regime, a consumer who discloses their password or PIN to an aggregation service may lose the protection offered by the EFT Code if an unauthorised transaction occurs;*
> - *liability for other losses – for example, losses caused by misrepresentations, inaccurate information, poor quality of the service, downloading software, interruption of the service, etc;*

[13]: http://download.asic.gov.au/media/1933166/what-do-you-want-to-do-with-acctaggreg_issues.pdf

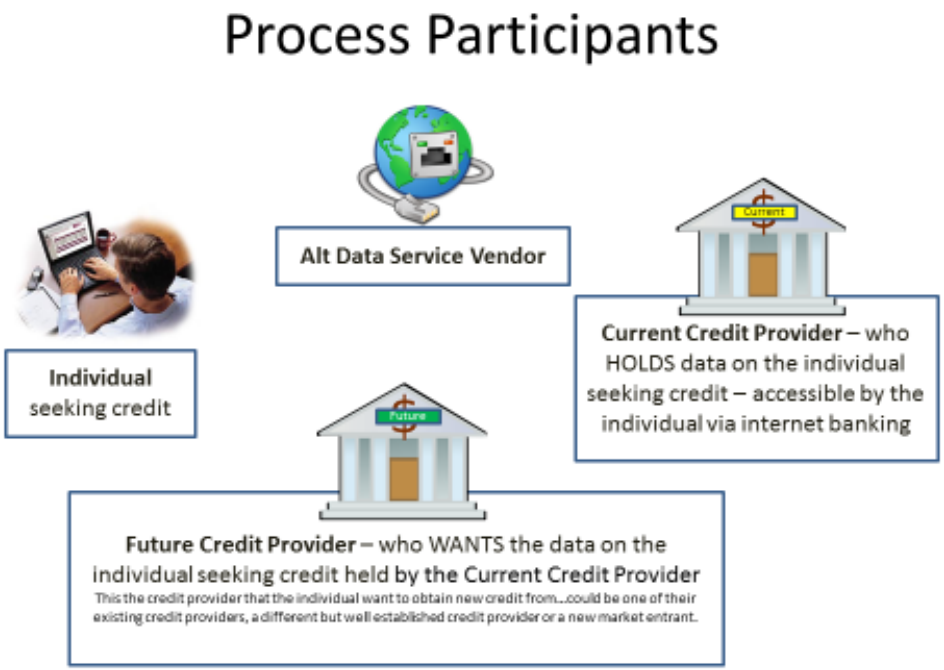
- *privacy – e.g. who has access to personal information, and what will the information be used for;*
- *security – especially the security of any location where account information is stored by the aggregator;*
- *consumer education;*
- *complaints and dispute resolution – most aggregation services surveyed do not appear to provide internal or external complaints resolution processes;*
- *cost of aggregation services, and debt recovery;*
- *cross-jurisdictional issues – for example, what are the implications if the aggregator is based in another jurisdiction;*
- *regulation of aggregators – should they be subject to the same prudential supervision framework and other regulations that apply to deposit-taking institutions and/or other financial institutions?;*
- *the implications of the Financial Transaction Reports Act, which is designed to deter money laundering and tax evasion."*
-

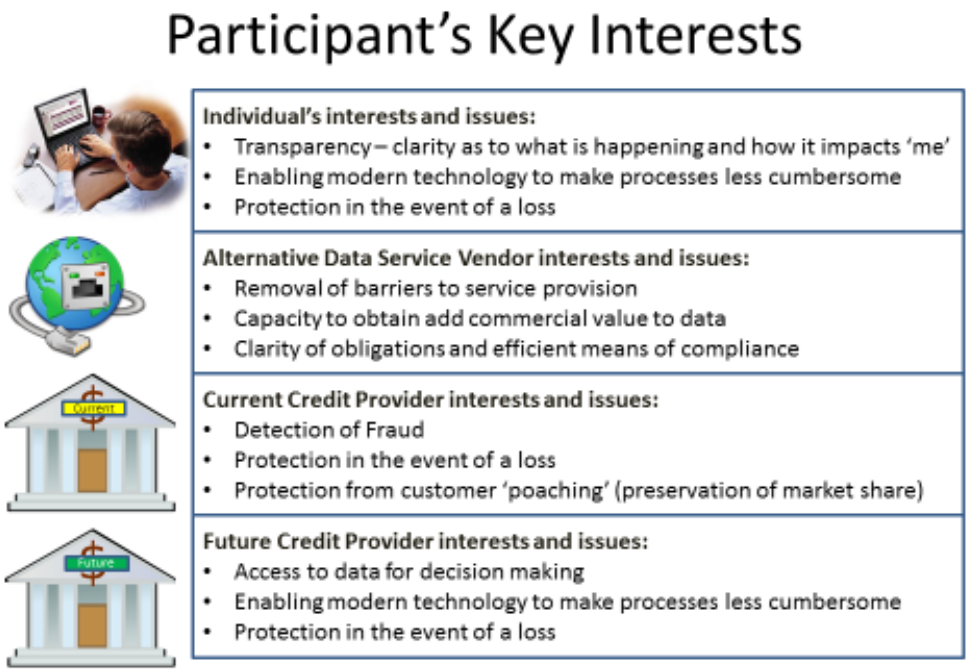
Whilst work on a variety of areas has been done, to date, specific to the topic of 'account aggregation services' there is not known to be have been a coordinated or holistic effort to address these matters, leaving industry largely to make up its own mind where they have questions about obligations, restrictions, liabilities or other concerns.

The purpose of the remainder of this section is to bring the discussion forward to 2016, illustrate what is happening today to provide clarity and context to a number of these elements. To illustrate how it really works and the issues that need to be addressed, and to assist Treasury and potentially other departments to be better placed to understand this topic and develop a coordinated regulatory response.

This section does not go into detail as to how the issues presented could be overcome though the author has done considerable background work reviewing various relevant regulation in detail and is both interested in and available to assist Government in working toward a coordinated and practical solution – one that will protect consumers, facilitate innovation and productivity improvements, and promote competition.

Who is involved, what role do they play in the process.





A Key Challenge:

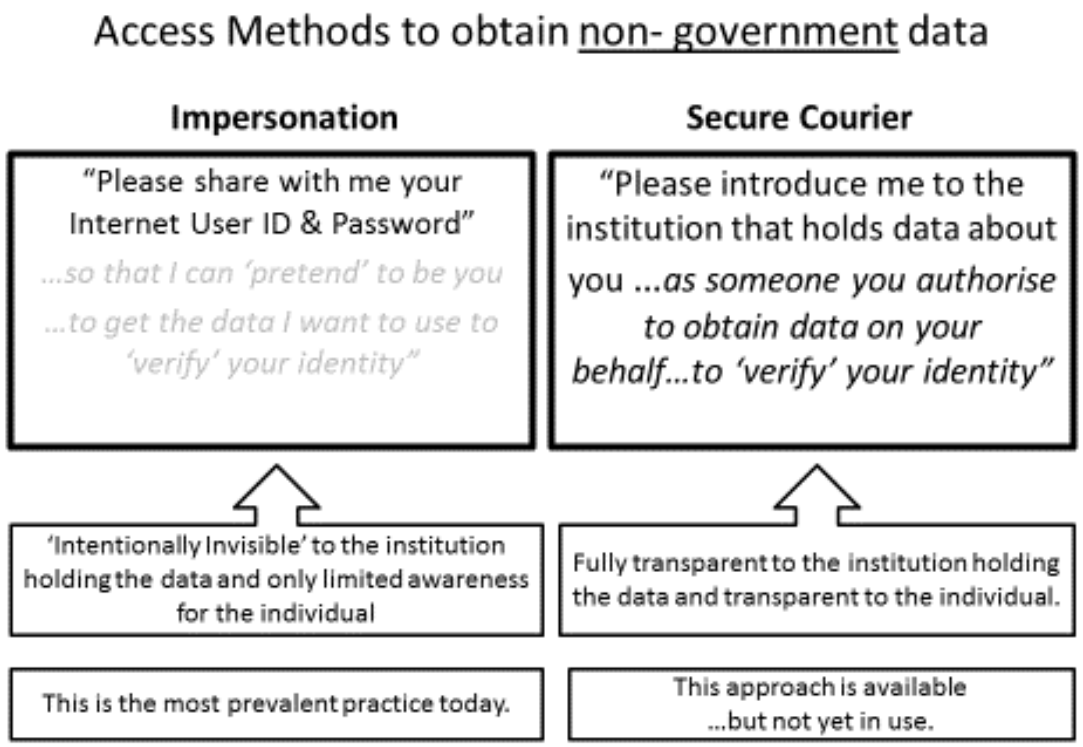
Overcoming inertia - it is clear that among the participant's there are competing interests. Ensuring that these are known and taken into account when assessing current approaches and alternatives and potential changes going forward is expected to be a challenge. The instinct to protect what one already has can be strong and this may manifest itself in participants seeking to delay or thwart change. The changes to credit reporting for example took from 2006 to 2013 to develop and implement, and in the nearly 3 years since adoption of the changes has been very slow…with only a very small number of participants supplying the newly allowed data and fewer still actively utilising it in decision making.

Perhaps one of the keys to resolution:

Transparency - lifting and sustaining a higher level of transparency - what each of the 4 participants are aware of throughout the process - is likely to be an important element in the meeting the collective interests of all participants.

Methods of leveraging internet banking to obtain data and the consequences

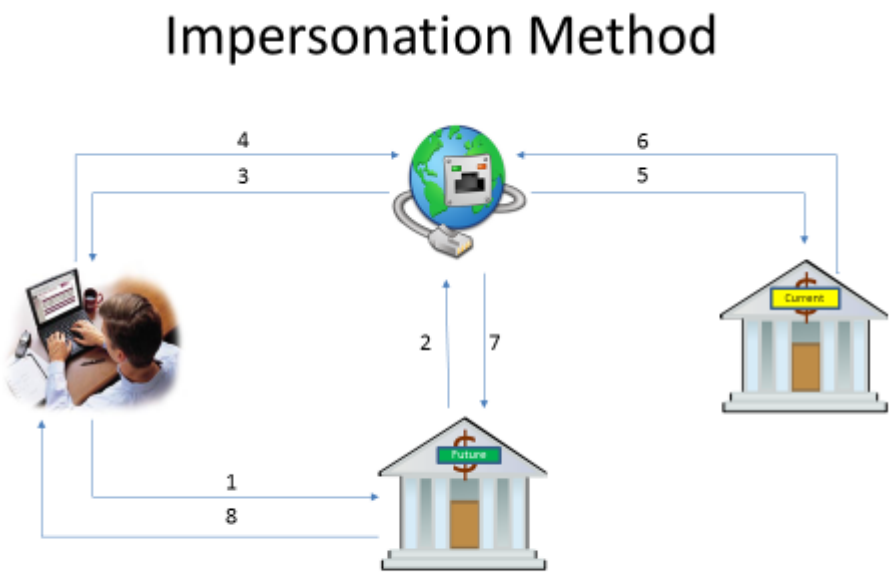
Fundamentally there are 2 different methods of access to obtain information….



The key question to ask when determining which approach a vendor uses is this:
Does the current credit provider (the holder of the data) know that someone other than the customer is obtaining the data and what it will be used for?
Answer:
No => Impersonation
Yes => Secure Courier

The primary driver behind the current prevalence of the impersonation method (the vast majority of whom are relatively new market entrants) is thought to be that it does not require commercial agreement by the current credit provider to obtain the data they hold (i.e. the larger and more established incumbents). Providers of Impersonation services get paid by the Future Credit Provider for their service.

Further Detail re: each method:



Steps:

1. Individual applies for credit at Future CP
2. Future CP engages service of Alt Data Service Vendor
3. Individual is asked to provide their User ID & Password directly or via an App or some other means to the Alt Data Service Vendor
4. Individual provide their User ID & Password directly or via an App or some other means to the Alt Data Service Vendor
5. Alt Data Service Vendor requests data held by the Current Credit Provider
   *(Note: Current Credit Provider IS **NOT** AWARE that the request has been authorised and who is actually making the request)*
6. Current Credit Provider gathers the data and provides it to the Alt Data Service Vendor
7. Alt Data Service Vendor provides the data to the Future Credit Provider
   (*Note: The individual IS **NOT** AWARE of what data will be disclosed and has NO capacity prior to disclosure to challenge the data in the event that it is inaccurate)*
8. Future Credit Provider informs Individual seeking credit of the outcome of their application.

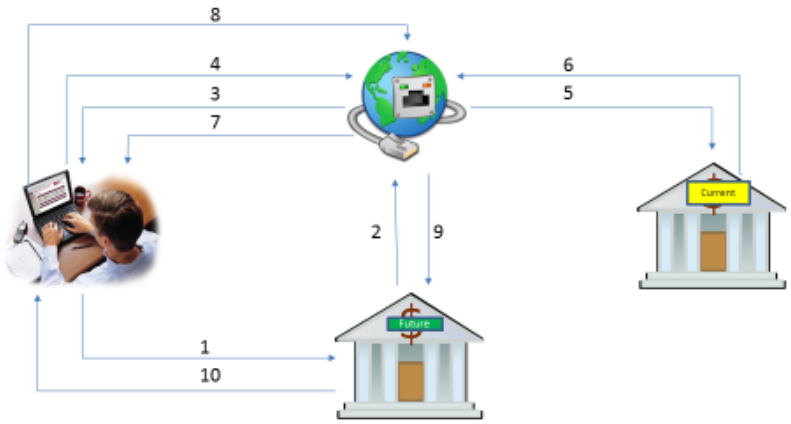
Very limited transparency:

Current Credit Provider is 'unaware' that they are participants in the process and in fact if they detect that such approaches are being used on them…primarily as a result of their fraud detection methods…they block them. From the Current Credit Provider's perspective the 'impersonation' method is indistinguishable from an attempted fraud.

The Individual does not have visibility of the data being obtained (this is the same situation they are in with regard to a traditional 'credit report' is obtained). This may be a factor in why some are of the view that the Privacy Act may apply to them as it does to Credit Reporting Businesses.
Some might argue that under the impersonation method by acting as an agent for the individual they are acting on behalf of the customer, however, the fact is that the individual never sees the data that their 'agent' obtains, so has no understanding of what data was obtained or capacity to seek correction of it prior to its use under this model.

These are fundamental similarities between the Impersonation approach and a traditional credit report…in terms of transparency and capacity for correction only being after the fact.

Secure Courier Method



Steps:

1. Individual applies for credit at Future Credit Provider
2. Future CP engages service of Alt Data Service Vendor
3. Individual is asked to provide their User ID & Password directly or via an App or some other means to the Alt Data Service Vendor
4. Individual authorises the Alt Data Service Vendor to seek data held by the Current Credit Provider
5. Alt Data Service Vendor requests data held by the Current Credit Provider
   (Note: Current Credit Provider IS AWARE that the request has been authorised and who is actually making the request)
6. Current Credit Provider gathers the data and provides it to the Alt Data Service Vendor
7. The Alt Data Service Vendor presents the data to the Individual seeking authorisation to disclose the data to the Future Credit Provider
8. The Individual seeking credit 'authorises' the Alt Data Service Vendor to release the data to the Future Credit Provider to assess their credit application
   (Note: The individual IS AWARE of what data will be disclosed and has the capacity to challenge the data (*) in the event that it is inaccurate)
9. Alt Data Service Vendor provides the data upon receiving authorisation (assuming there is no challenge to the data) to the Future Credit Provider
10. Future Credit Provider informs Individual seeking credit of the outcome of their application.

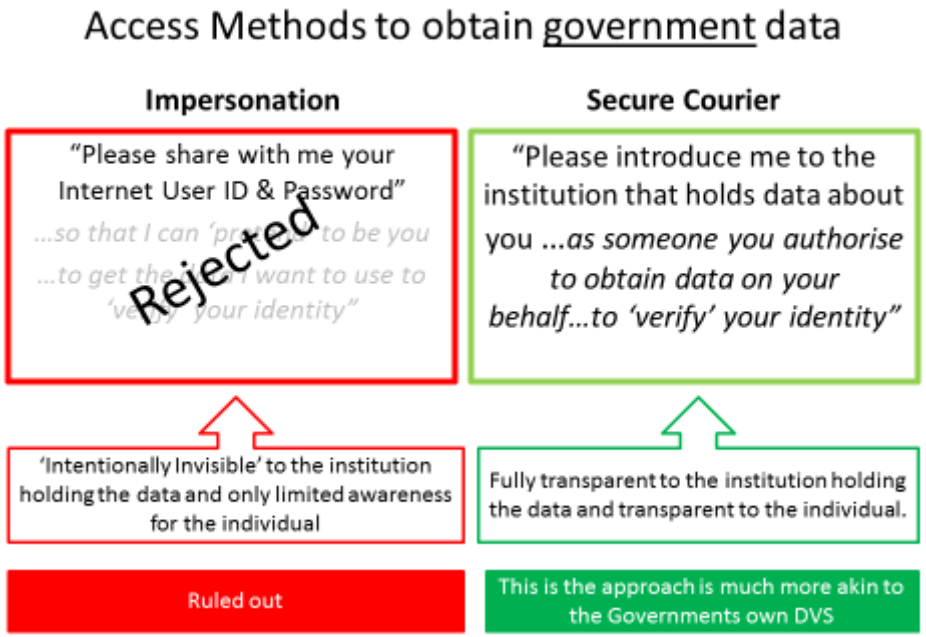
(*) The Individual is not be able to select which data to disclose or modify the data…any challenge would result in the individual needing to withhold authorisation of release and the request correction from their Current Credit Provider

Full Transparency:
The Current Credit Provider knows that their customer has authorised someone to seek data about them…data that under the Privacy Act the individual has a right to obtain (via an access seeker) on their behalf.
The Individual knows what data has been obtained and has the ability to ensure it is correct prior to it being used by others.
These are fundamental differences between the Secure Courier approach and a traditional credit report.

Regulatory risk/uncertainty issues:
There are various elements of regulation that are 'intertwined' that relate to this area.

- Privacy – Credit Reporting Part IIIA
    - Are those that collect data and disclose it to others for use in creditworthiness assessment Credit Reporting Businesses under the Act?
    - If not, how is that the case?
    - If so, are they then limited under the Privacy Act to what data they are allowed to collect, use and disclose?
    - If these businesses are breaching the Privacy Act, would the Credit Providers to whom Alternative Data Vendor Services are disclosing the data also be in breach?

    - Is the provision under the Privacy Act for an access seeker to obtain information on someone's behalf being 'abused'



Have we been here before?
Yes.
When the initial AML legislation came in industry developed the Impersonation Model and used it to access Government data. When this was identified, the Government took action to stop this approach and to develop a Secure Courier type approach. So, it would seem that at least at some level the Federal Government's view is clear on this matter when it comes to accessing the data they hold – they do not like the impersonation method.
In developing and enabling access to Government data via the Data Verification Service (DVS)14 – which can be used for ID Verification to meet AML/CTF obligations – the government clearly rejected the 'impersonation' approach and require the 'secure courier' approach when accessing the data they hold.

[14] http://www.dvs.gov.au/Pages/default.aspx

There appears to be no specific ruling or guideline document specifies this approach as also required to gain access to non-government data. However, it was a stated intention of the Government in the review of the Privacy Act to seek to align/harmonise the Government and private sector legislation re: the treatment of personal data.

- E-Payments Code / Trade Practices Act / Terms and Conditions – Contractual Liability
  - If the individual provides there internet banking User ID and password to another – most frequently a breach of their Internet Banking Terms and Conditions and there is a loss – will the individual be deemed to have lost their protections under the E-Payments Code by 'enabling the loss to occur'?
  - Can the Future Credit Provider and or the Alternative Date Service Vendor effectively shift all risk of loss to the individual via wording in their terms and conditions?

- NCCP Responsible Lending Obligations – efficient gathering of Income and Expense Data to enable assessment of capacity to service without hardship
  - There is a requirement for Small Amount Credit Contract providers to obtain the last 3 months-worth of bank statements and to consider them in their assessments….and an expectation…presumably unless there is an alternative… on all credit providers to do so as part of assessing capacity to repay without hardship.

Refer the Appendix A for more detailed discussion of each of the above matters is included above:

Commercial Vs Consumer Interests and Competition:

The data that Current Credit Providers hold on their customers is of material commercial value. It would be expected that they would seek to protect their business interests and therefore may be reluctant to provide Alternative Data Service Vendors with access.

Future credit providers (in particular new market entrants) are keen to obtain the data that Current Credit Providers hold…as a way of 'levelling' the competitive playing field.

Will those who hold data and seek to prevent or dissuade alternative data gathering services from obtaining the data – in an attempt to prevent attrition?

Current usage of the Alternative Data Service Vendors would seem to suggest that the above is precisely how things are playing out.

Would this be seen as being anti-competitive or possibly in breach of the consumer's right of access…assuming the other regulatory wrinkles can be ironed out?

Appendix A

Privacy – Credit Reporting Part IIIA

Potential issues surrounding both the data gatherers and credit providers being provided "alternative data":

Are those that supply 'alternative data' credit reporting businesses?

The definition of a Credit Reporting Business:

6P Meaning of *credit reporting business*

(1) A ***credit reporting business*** is a business or undertaking that involves collecting, holding, using or disclosing personal information about individuals for the purpose of, or for purposes including the purpose of, providing an entity with information about the credit worthiness of an individual.

NOTES:

This section of the Act does not include any mention of being able to avoid being classified as a CRB by virtue of 'consent' from the individual.

Are alternative data providers doing the things listed in the definition?

If so, then is there a section of the Privacy Act, Regulations or Credit Reporting Code that these data providers would be able to rely that would exclude them from this being Credit Reporting Businesses?

Depending on the outcome of the above question…other questions naturally follow.

If 'alternative data collectors are CRBs based on what they do…is the data of the type the alternative data providers collect and disclose to credit providers allowed?

E.g. Transaction data and or account balance details.

The Privacy Act (Section 6 N) in combination with the Credit Reporting Code defines (and limits) what information a Credit Reporting Business can collect, use and disclose….largely because the data collection in the credit reporting process is not transparent and individuals are not aware of the data until they ask for it separately.

It seems clear that transaction data and account balance data are not within the limitations of 6N or the CR Code.

If that is the case, on what section of the Privacy Act, Regulations or Credit Reporting Code might CRBs rely that would allow for the collect and disclose of such information that is beyond these limits?

Whilst the above speaks to Credit Reporting Businesses, is there an exposure for CPs here as well?

80V Ancillary contravention of civil penalty provisions

(1) An entity must not:

…. (d) be in any way, directly or indirectly, knowingly concerned in, or party to, a contravention of a civil penalty provision; or….

(2) An entity that contravenes subsection (1) in relation to a civil penalty provision is taken to have contravened the provision.

Are Credit Providers who obtain such data from alternative credit providers and use such data also at risk of being in breach of the Act, or is there another section of the Act, Regulations or CR Code that would protect them?

Privacy - Data Security

'Impersonation' methods.

There are understood to be 2 primary technical means used to enable leveraging internet banking access to obtain transaction, account and other data … and there are varying views on which mechanism is 'safer'.

1. Directly obtaining the User ID and Password from the individual – using that information to obtain the data and storing those access details on a central server.

   There is suggestion that these servers are 'safe' but unless hacking them is totally impossible there is a risk. The AFP, the FBI, MI6 and other institutions thought to be highly secure have all been compromised. It is seems reasonable to think that the servers of 'alternate data gatherers' in spite of best efforts are still not 'risk free'.

   Currently Yodlee, their 'on-sellers', and others utilise this approach.

   Of specific note, in the FinTech Australia submission to Treasury, Yodlee is understood to have authored the section relating to this topic (Open Financial Data) and in that section they recommend 'open ADIs'…which interestingly is inconsistent with their current practice, however is consistent with the Secure Courier method of data exchange.

2. Via a downloaded APP – using data User ID and Password from the individual that is keyed into the APP obtain the data. Here the User ID and Password from the individual is not saved centrally.

   Unlike the centralised server model mobile devices don't hold large numbers of User IDs and Passwords, however they are frequently lost and compromised….and to the individual whose data is then lost…it will matter little that they are not among a larger group.

   Currently, this is the approach used by Mogo and their on-sellers.

Assuming that under either model there is a risk, then there could be a loss related to that risk, which the leads to a question as to how is liable for the loss.

Loss Liability - E-Payments Code / Trade Practices Act / Terms and Conditions

If the credit provider requests (or entices) the individual to use one of these services and there is a loss, who is liable?

E-Payments Code

Who is liable if, related to enabling the accessing of the alternative data, a loss was incurred?

It is near universal that the T&Cs of a customer's internet banking make clear that the sharing of user IDs and Passwords will cause the customer to be liable in the event of a loss.

This is supported by the E-Payments Code.

An example of how one of the Credit Providers (who do utilise an alternative data gathering service) further seeks to clarify that any liability for loss rests solely with the consumer by saying:

"By entering your log-in details, you're agreeing:

- *for us [the credit provider] and "the Alternative Data Gathering Service" to access and retrieve information from your bank account(s) as your agent;*
- *that your use of "the Alternative Data Gathering Service" does not involve you breaching any of your obligations in relation to your bank account(s); and*
- *your use of "the Alternative Data Gathering Service" is at your risk, and other than your rights under the law, we or "the Alternative Data Gathering Service" will not be responsible for any loss suffered by you as a result of you providing your log-in details to "Alternative Data Gathering Service" to access your bank statements on our behalf."*

Is such contractual language likely to be viewed as 'unconscionable' and thus 'unfair' and thus create issues with the Trade Practices Act as well as existing contractual terms and conditions of internet banking?

If so, how might this be dealt with in an instance where a consumer suffers a loss on the basis of the above terms?

Appendix B

DOC_FinTechAustrali
a_-_Position_paper.pd