

Independent Review of Compliance with Part IIIA

**Equifax Australia Information Services
and Solutions Pty Limited (EAISS)**

June 2017



The Directors
Equifax Australia Information Services and Solutions Pty Limited
PO Box 964
North Sydney NSW 2059

30 June 2017

Dear Directors

Independent Review of Compliance with Part IIIA

It is with pleasure that we enclose our report on the independent review of the operations and processes of Equifax Australia Information Services and Solutions Pty Limited ('Equifax'), to assess compliance with Part IIIA of the Privacy Act 1988 (Cth) ('Act'), the Privacy Regulation 2013 ('Regulations') and the Credit Reporting ('CR') Code.

This report details the findings and recommendations arising from our independent review of the operations and processes of Equifax as they apply to the Equifax Apply product to assess compliance with the Part IIIA of the Act, the Regulations and the CR Code as per our Engagement Letter dated 21 April 2017. The review was performed in May 2017.

In the report that follows we detail our results of performing the following activities:

- Desktop review of relevant Equifax policies and procedures relating to Equifax's fulfilment of its obligations
- Interviews and walkthroughs with stakeholders based on the scope of the review as outlined in our Engagement Letter with Equifax dated 21 April 2017
- Assessment of current state of design of Equifax's operations and processes in relation to Equifax Apply in meeting Equifax's obligations
- Risk assessment of potential improvements identified against Equifax's risk rating table
- Fact checking with Management to verify the factual accuracy of the systems and control processes.

Grant Thornton Australia

Level 17, 383 Kent Street
Sydney NSW 2000

grantthornton.com.au

We take this opportunity to extend our appreciation to the Equifax team for their assistance and cooperation during the course of the review.

We trust that you find this report informative and we appreciate the opportunity to be of service to you. If you have any queries or wish to discuss any issues further, please do not hesitate to contact us.

Yours faithfully



Mark Griffiths
Partner – Business Risk Services
Grant Thornton Australia Limited

Contents

Executive Summary	4
Findings:	8
1.0 Open and transparent management of credit reporting information	9
2.0 Credit reporting system arrangements	10
3.0 Credit information handling practices, procedures and systems	11
4.0 Security of credit reporting information	18
5.0 Record keeping	19
6.0 Access	21
7.0 Correction of information	23
8.0 Protections for victims of fraud	26
9.0 Complaints	28
10.0 Credit reporting system integrity	30
11.0 Independent review of compliance	31
Appendix	32
Equifax Risk Assessment	33
Glossary	34

Executive Summary



Executive Summary

Overall Conclusion

Overall, the design of Equifax's operations and control processes as they apply to the Equifax Apply product is compliant with its obligations under Part IIIA of the Act, the Regulations and the CR Code. It was evident during our review that there is strong awareness and knowledge within Equifax's employees of the business' privacy obligations, which resonates with the overarching policies and procedures at Equifax which reiterate its compliance obligations. Equifax has robust processes and secure systems in place to ensure that the credit information it uses and discloses is permitted within the legislation. Equifax also has adequate controls in place to address its obligations to provide access, correct information and investigate complaints as required by the legislation. However, our review identified two potential improvements in relation to Equifax's collection of credit information and destruction of credit information that could result in a residual risk of non-compliance with the relevant sections of Part IIIA of the Act, the Regulations and the CR Code until such time as processes are fully automated or updated.

Background

Under paragraph 24.2 of the Privacy (Credit Reporting) Code 2014 (version 1.2) ('CR Code'), every three years (or more frequently if the Commissioner requests) a credit reporting body ('CRB') must commission an independent review of its operations and processes to assess compliance by the CRB with its obligations under Part IIIA of the Privacy Act 1988 (Cth) ('Act'), the Privacy Regulation 2013 ('Regulations') and the CR Code.

Equifax Australia Information Services and Solutions Pty Limited ('Equifax') is part of a global organisation that provides insights and knowledge to help its customers make informed decisions through assimilating and analysing data on consumers and businesses. One of Equifax's main services is providing credit reports and scores based on personal information. This is delivered via the Equifax Apply and other products.

Equifax is a CRB under the Act and accordingly, is required to commission an independent review under paragraph 24.2 of the CR Code. Following consultation with the Office of Australian Information Commissioner ('Commissioner') regarding the scope and approach for this review, namely the operations and processes of Equifax in relation to Equifax Apply, and a reviewer selection process, Grant Thornton Australia Limited ('Grant Thornton') was engaged on 21 April 2017 to conduct this review.

Equifax Apply is a solution that provides credit reporting information to enable a credit provider ('CP') to assess the credit risk of individuals applying for personal finance using negative and comprehensive credit reporting ('CCR') data, as permitted under Part IIIA of the Act.

Objective and Scope

The objective of this review was to assess the design of Equifax's operations and control processes required under Part IIIA of the Act, the Regulations and the CR Code, as they specifically apply to the Equifax Apply product. The scope of our review included:

- Policies and procedures relating to Equifax's obligations under Part IIIA of the Act, the Regulations and the CR Code as they apply to the Equifax Apply product, e.g. Credit Reporting Policy
- Staff involved with the development, maintenance, or day-to-day use of Equifax Apply privacy and credit reporting training
- Sources and types of information collected (solicited and unsolicited) in relation to Equifax Apply, including any due diligence undertaken on sources of information
- Use and disclosure of information, including de-identified information and derived information
- Quality of information stored and used for Equifax Apply, specifically the accuracy, currency, completeness and relevance of information
- Security of Equifax Apply and any other relevant systems to the product to protect information from unauthorised access and misuse / loss
- Provision of access to information, and correction of credit reporting information
- Retention of credit related information
- Internal handling of complaints.

Limitations of Scope

The scope of the review was restricted to those Australian privacy laws comprising Part IIIA of the Act, the Regulations and the CR Code as they specifically apply to the Equifax Apply product. The review therefore did not include:

- The Australian Privacy Principles or any other privacy laws
- The laws of, and accordingly the activities of Equifax conducted in New Zealand or any other jurisdiction
- Any other Equifax product or service.

Compliance Mapping

The adjacent table summarises Equifax's compliance against the relevant sections / paragraphs of the Act and CR Code, and a reference to the potential improvements identified along with their risk ratings assessed using Equifax's Risk Rating Table set out in the **Appendix** section of this report.

Report Ref.	Area	Part IIIA Ref*	CR Code Ref	Potential improvement Identified
1.0	Open and transparent management of credit reporting information	20B	3	Nil
2.0	Credit reporting system arrangements			
2.1	Subscriber Agreements	20N(3) & 20Q((2)	2.1 & 15	Nil
2.2	Training	N/A	2.2	Nil
3.0	Credit information handling practices, procedures and systems			
3.1	Collection of Credit Information	20C, 20D & 20L	5.1(a), 5.2, 5.4(a)-(c), 6-12	3.1.4a (Low)
3.2	Use & Disclosure of Credit Information	20E, 20F, 20M & 20P	7, 8, 9, 14 & 16	Nil
3.3	Integrity of Credit Reporting Information	20N	5.4(d)-(f)	Nil
3.4	Credit Provider Audits and Breaches	20N & 20Q	5.4, 23	Nil
4.0	Security of credit reporting information	20Q	15.1	Nil
5.0	Record keeping	20V-20Z, 20ZA	1.2(f), 22	5.0.2a (Low)
6.0	Access	20R	19	Nil
7.0	Correction of information	20S-20U	20	Nil
8.0	Protections for victims of fraud	20K	17	Nil
9.0	Complaints	Div 5, 23	21	Nil
10.0	Credit reporting system integrity	N/A	23.11	Nil
11.0	Independent Review of Compliance	N/A	24.2	Nil

*All Part IIIA references to the Privacy Act relates to sections under Division 2, unless otherwise stipulated

Summary of Potential Improvements Identified

In the table below we present the two potential improvements identified during this review, along with Equifax's comments. The next section of this report provides further details of all the Part IIIA, Regulations and CR Code obligations we assessed Equifax's operations and processes against as they apply to Equifax Apply, including a summary of those obligations. The summary, by its nature, has attempted to simplify obligations that are inherently complex, to provide a general description of those obligations for the purpose of assisting a reader to comprehend this report. Accordingly, the summary should not be relied on by any person for any other purpose. Our review was conducted by reference to the applicable obligations rather than the summary included in the next section of this report.

Ref #	Details of Potential Improvements Identified	Risk Rating	Equifax Comments
3.1.4a	Some publicly available Queensland Court information collected is input manually into Equifax's credit bureau. Currently the process is for an employee to enter this information into the system manually, however there is no subsequent data validation to ensure that the transcription was complete or accurate. This may lead to the recording of inaccurate credit information. Equifax has advised that this process will be automated in the next couple of months, which will remove the need for manual entry.	Low	<p>It should be noted that publicly available information is predominantly input using automated processes, relying on carefully designed schemas. The potential improvement identified only relates to the Queensland District and Supreme Court data – which since January 2016 constitutes less than approximately 0.015% of the total data received into the bureau.</p> <p>Due to the format the data is provided to Equifax from the Queensland District and Supreme Court, the process must currently be manual. The automation of the data load largely depends on changes to be made by the Queensland courts. Until this is automated, we have implemented a manual testing procedure to assess the data accuracy which we deem an appropriate control.</p> <p>We believe that Equifax has reasonable practices, procedures and systems in place – pending a transition to a fully automated load – to deal with this very small percentage of court data to ensure that it is accurate, up-to-date, complete and relevant for its purpose.</p>
5.0.2a	Equifax's purging schema has not been set up to prevent deletion of items that are pending correction or are the matter of a dispute.	Low	Equifax notes that preventing the deletion of items outside the retention period, that are pending correction or are the matter of a pending dispute, would only be required in practice where a consumer has notified us about a correction or a matter of dispute at least two years, and up to seven years, after the data was first collected by Equifax or relevant event – depending on the type of data in question. This would be a very rare occurrence. Nevertheless, we are implementing improvements to our processes to address this possibility.

Findings



1.0 Open and transparent management of credit reporting information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
1.0.1	Div 2, Sec 20B(3) & (4)	Para 3	<p>Equifax must have a clearly expressed and up-to-date policy about the management of its credit reporting information, which must contain the following:</p> <ul style="list-style-type: none"> • the kinds of credit information collected and methods of collection • the kinds of credit reporting information held and how information is held • how personal information is derived from credit information Equifax holds • the purposes for which Equifax collects, holds, uses and discloses credit reporting information • information about the effect of the use or disclosure of credit reporting information for the purposes of direct marketing, and how an individual can request to not use their information for pre-screening purposes • how an individual may access credit reporting information about themselves and seek correction of such information • how an individual may complain about a failure of Equifax to comply with Division 2 or the registered CR Code and how Equifax will deal with the complaint. 	
1.0.2	Div 2, Sec 20B (5)	Para 3.1	Equifax must make its Credit Reporting Policy available for free and publish the policy on its website.	

2.0 Credit reporting system arrangements

2.1 Subscriber Agreements

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
2.1.1	Div 2, Sec 20N(3) and 20Q((2)	Para 2.1 and 15	<p>Equifax must enter into written agreements with CPs that require the providers to:</p> <ul style="list-style-type: none"> • ensure that credit information that they disclose to Equifax is accurate, up-to-date and complete • protect credit reporting information that is disclosed to them from: <ul style="list-style-type: none"> • misuse, interference and loss • unauthorised access, modification or disclosure. <p>The agreement Equifax enters into with a CP must also oblige both parties to comply, to the extent applicable from time to time, with Part IIIA, the Regulations and the CR Code.</p>	

2.2 Training

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
2.2.1	N/A	Para 2.2(a)	<p>Equifax must take reasonable steps to</p> <ul style="list-style-type: none"> • inform employees who handle credit reporting information of the requirements of Part IIIA, the Regulations and the CR code; and 	
2.2.2	N/A	Para 2.2(b)	<ul style="list-style-type: none"> • train employees who handle credit reporting information in the practices, procedures and systems that are designed to achieve compliance with those requirements. 	

3.0 Credit information handling practices, procedures and systems

3.1 Collection of credit information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
3.1.1	Div 2, Sect 20C	Para 5.1(a), 5.2, 5.4(a), (b) & (c), 6, 7, 8, 9, 10 and 12	<p>Unless required or authorised by or under an Australian law or a court / tribunal order, as a CRB, Equifax can only collect solicited credit information about an individual by lawful and fair means in the course of carrying on a credit reporting business from a CP who is permitted under section 21D of the Act to disclose the information to Equifax. Equifax may also collect credit information from an entity other than a CP, in accordance with section 20C(4).</p> <p>Where the information collected from a CP is</p> <ul style="list-style-type: none"> • <i>identification information</i> – Equifax also collects from the provider, or already holds, credit information of another kind about the individual • <i>consumer credit liability information</i> – Equifax must not agree or implement procedures with CPs to standardise CP's numbering conventions for consumer credit, however Equifax must develop and maintain in conjunction with CPs common descriptors of the types of consumer credit provided to individuals. <p>Equifax must have reasonable practices, procedures and systems that are designed to cover the obligations under Part IIIA, the Regulations and the CR code and in particular enable Equifax to:</p> <ul style="list-style-type: none"> • use the information disclosed by CPs in relation to individuals' dates of birth to identify any information disclosed by a CP that: <ul style="list-style-type: none"> ○ relates to an act, omission, matter or thing that occurred or existed before the relevant individual turned 18; and ○ that is prohibited by Part IIIA, the Regulations or this CR code from being disclosed by the CP to Equifax • as soon as practicable identify whether collected information includes information that Equifax is prohibited by Part IIIA, the Regulations or this CR code from collecting and, if so, to destroy the prohibited information • as soon as practicable, notify the relevant CP where Equifax destroys information on the basis that Part IIIA, the Regulations or this CR code prohibits Equifax from collecting that information. 	  
3.1.2	Div 2, Sec 20C(4)(e)	Para 8	Where Equifax collects information from an entity (other than a CP), if the information is RHI about the individual, Equifax collects the information from another CRB that has an Australian link.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
3.1.3	Div 2, Sec 20L	N/A	If Equifax holds credit reporting information about an individual and the information is a government related identifier of the individual, Equifax must not adopt the government related identifier as its own identifier of the individual unless the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order.	
3.1.4	N/A	Para 11	Equifax must only collect publicly available information about an individual: <ul style="list-style-type: none"> • from an agency or a state or territory authority; and, • if the content of the information that is collected is generally available to members of the public (whether in the form provided to Equifax or another form and whether or not a fee must be paid to obtain that information); and, • if the other requirements of Section 6N(k) are met, i.e.: <ul style="list-style-type: none"> ○ it relates to the individual's activities in Australia or the external Territories and the individual's credit worthiness; and, ○ it is not court proceedings information about the individual or information about the individual that is entered or recorded on the National Personal Insolvency Index (AFSA data). 	 <div style="background-color: #0056b3; color: white; padding: 2px; text-align: center; font-weight: bold;">LOW</div> Potential Improvement 3.1.4a – <i>Refer to page 7</i>
3.1.5	Div 2, Sec 20D	N/A	<p>If Equifax receives unsolicited credit information about an individual, Equifax must, within a reasonable period after receiving the information, determine whether or not it could have collected the information under section 20C if Equifax had solicited the information.</p> <p>If Equifax determines that it could have collected the credit information, Equifax may deal with that information as though it had collected the information. If Equifax determines that it could not have collected the credit information, Equifax must, as soon as practicable, destroy the information.</p>	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
3.2.2 (cont)	N/A	Para 16	<p>Para 16 – Equifax must only disclose credit reporting information to a CP, for the purposes of enabling the CP to assist the individual to avoid defaulting on his or her obligations in relation to consumer credit provided by the CP to the individual where either:</p> <ul style="list-style-type: none"> • the CP confirms to Equifax that it is aware of circumstances that reasonably indicate that the individual may be at significant risk of defaulting in relation to those obligations; or • Equifax is aware that an event has occurred in relation to the individual that is an event of the kind that the CP has identified could, if it were to occur, reasonably indicate that the individual may be at significant risk of defaulting in relation to those obligations. 	
3.2.3	Div 2, Sec 20P	N/A	<p>Equifax must not use or disclose credit reporting information that is materially false or misleading, unless:</p> <ul style="list-style-type: none"> • it is to determine whether unsolicited credit information received could have been collected if Equifax had solicited the information • it is in consultation for the correction of credit information. 	
3.2.4	Div 2, Sec 20M	N.A	<p>Equifax may use or disclose de-identified credit reporting information in the following circumstances:</p> <ul style="list-style-type: none"> • the use or disclosure is for the purposes of conducting research in relation to credit; and • Equifax complies with the rules made by the Commissioner which by legislative instrument, make rules relating to the use or disclosure by a credit reporting body of de-identified information for the purposes of conducting research in relation to credit. 	

3.0 Credit information handling practices, procedures and systems

3.3 Integrity of credit reporting information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
3.3.1	Div 2, Sec 20N	Para 5.4(d), (e) & (f)	<p>Equifax must take reasonable steps in the circumstances to ensure that the credit information it collects, uses and discloses is having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.</p> <p>Equifax must have reasonable practices, procedures and systems that are designed to cover the obligations under Part IIIA, the Regulations and the CR Code and in particular enable Equifax to:</p> <ul style="list-style-type: none"> • undertake regular testing of the credit information and credit reporting information that Equifax uses and discloses to ensure that it is accurate, up-to-date, complete and relevant, having regard to the purpose for which it is used or disclosed • take reasonable steps to initiate, as soon as practicable, targeted testing of its credit reporting information, where Equifax is informed, or identifies, that credit reporting information in relation to an individual is not accurate, up-to-date, complete and relevant, having regard to the purpose for which it is used or disclosed • rectify the situation where Equifax identifies that credit reporting information in relation to an individual is not accurate, up-to-date, complete and relevant, having regard to the purpose for which the information is used or disclosed, including by destroying any information in accordance with its obligations in Part IIIA, the Regulations and the CR code. 	

3.0 Credit information handling practices, procedures and systems

3.4 Credit provider audit and breaches

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
3.4.1	N/A	Para 23.1 & 23.2	<p>To ensure Equifax is able to tailor the frequency and extent of any audit requirements under Part IIIA to the CPs that present the greatest risk of non-compliance, it must establish a documented, risk based program to monitor CP's compliance with their obligations under Part IIIA incorporated in their agreements with Equifax which must:</p> <ul style="list-style-type: none"> identify and evaluate indications of risk of non-compliance by CPs with their obligations to: <ul style="list-style-type: none"> disclose credit information that is accurate, up-to-date and complete to Equifax protect the credit reporting information that Equifax discloses to the CP from misuse, interference and loss and from unauthorised access, modification or disclosure take the steps in relation to correct credit-related personal information required by Part IIIA, the Regulations and the CR code assess the risk posed by CPs of significant non-compliance with those obligations utilising those risk indicators and the range of information available to Equifax including correction requests and complaints utilise a reasonable range of monitoring techniques to validate and update those risk assessments from time to time include an audit program for CPs to assess compliance with their obligations referred to in paragraph 23.1 of the CR code. 	
3.4.2 (cont)	Div 2, Sec 20N (3)(b) & (c) and 20Q (2)(b) & (c)	Para 23.1, 23.3, 23.4, 23.5 & 23.6	<p>Equifax must:</p> <ul style="list-style-type: none"> ensure that regular audits are conducted by an independent person to determine whether agreements entered into with CPs are being complied with; and, identify and deal with suspected breaches of those agreements. <p>Equifax's risk based program must include a CP audit program for CPs to assess compliance with their obligations to ensure that:</p> <ul style="list-style-type: none"> credit information the CP discloses to Equifax is accurate, up-to-date and complete credit reporting information Equifax discloses to the CP is protected from misuse, interference, loss, and from unauthorised access, modification or disclosure the CP takes steps in relation to requests to correct credit-related personal information required by Part IIIA of the Act, the CR Code and the Regulations. 	 

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
3.4.2 (cont)	Div 2, Sec 20N (3)(b) & (c) and 20Q (2)(b) & (c)	Para 23.1, 23.3, 23.4, 23.5 & 23.6	<p>To be independent to conduct an audit of a CP as part of Equifax’s auditing program, an auditor:</p> <ul style="list-style-type: none"> • must not be a director or employee of the CP, have a significant financial interest in the CP or, at any time during the previous 12 months, had any such relationship or interest; • must achieve functional independence of Equifax’s organisational structure and supervision arrangements if the auditor is an employee of Equifax or functional independence of an organisation’s governance and supervision arrangements if an employee of an industry funded organisation • must not have any other association that would impair the perception of the auditor’s independence, nor had any such association at any time during the previous 12 months. <p>Equifax must take reasonable steps to ensure that a person who conducts an audit of a CP as part of its auditing program has sufficient expertise for the role including knowledge of Part IIIA of the Act, the CR Code and the Regulations, audit methodology and previous experience in conducting audits and credit reporting system experience.</p> <p>Equifax must take reasonable steps to ensure that its audit oversight, including reporting arrangements, is sufficient to enable it to form a view as to whether the CP is complying with its obligations.</p>	 
3.4.3	N/A	Para 5.4(g)	<p>Where Equifax identifies credit information that is not accurate, up-to-date and complete, raise this, where reasonable, with the CP that disclosed the information and request the CP to:</p> <ul style="list-style-type: none"> • take reasonable steps to review its credit information management practices, procedures and systems; • rectify any issues that are identified; and • advise Equifax of the results of the review; and • Equifax must have reasonable practices, procedures and systems that are designed to cover its legislative obligations and enable it to report about its testing (undertaken in accordance with paragraph 5.4(d) of the CR code), and any material findings or material changes to procedures, to CPs with which it has an agreement with in relation to the disclosure of credit information (by the CP) to Equifax and disclosure of credit reporting information (to the CP) by Equifax as referred to in section 20N(3) and section 20Q(2) respectively. 	

4.0 Security of credit reporting information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
4.0.1	Div 2, Sec 20Q	Para 15.1	<p>Equifax must take reasonable steps in the circumstances to protect the credit reporting information it holds from misuse, interference and loss and unauthorised access, modification or disclosure.</p> <p>Equifax must maintain reasonable practices, procedures and systems to ensure the security of electronic transmission and storage of credit reporting information.</p>	

5.0 Record keeping

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
5.0.1	N/A	Para 22	<p>Equifax must maintain adequate records to evidence their compliance with Part IIIA, the Regulations and the CR Code, in particular:</p> <ul style="list-style-type: none"> • where credit-related personal information is destroyed to meet legislative obligations (but only if possible) • for credit reporting information disclosures by Equifax: the date of the disclosure, a brief description of the type of information disclosed, the credit provider, affected information recipient ('AIR') or other person to whom the disclosure was made and evidence that the disclosure was permitted under Part IIIA, the Regulations or the Code • records of any consent provided by an individual for the purposes of Part IIIA, the Regulations or the CR Code. <p>Records must be retained for a minimum period of 5 years from the date on which the record is made unless, the record includes information that Equifax is required by Part IIIA, the Regulations or the CR code to destroy at the end of the applicable retention period, in which case the record must be retained for the duration of that retention period only.</p>	 
5.0.2	Div 2, Sec 20V, 20W, 20X, 20Z and 20ZA	Para 1.2(f)	<p>Equifax must destroy credit information and any related CRB-derived information or ensure that this information is de-identified within 1 month after the relevant retention period, unless:</p> <ul style="list-style-type: none"> • immediately before the retention period ends there is a pending correction request in relation to the information; or • immediately before the retention period ends there is a pending dispute in relation to the information; or • if Equifax is required by Australian law or a court / tribunal order to retain the information. <p>The prescribed retention periods range from 2 to 7 years, depending on the nature of the information, as per sections 20W, 20X, 20Y and 20Z of the Act. There is no retention period for identification information or credit information that is publicly available information about the individual that relates to the individual's activities in Australia or the external Territories, and the individual's credit worthiness and that is not court proceedings information about the individual or information about the individual that is entered or recorded on the National Personal Insolvency Index.</p> <p>An obligation on Equifax to "destroy" credit information or credit reporting information requires Equifax to ensure it irretrievably destroys the information. Where it is not possible to irretrievably destroy credit-related personal information held in electronic format, Equifax should take steps to put the information 'beyond use.'</p>	 <div style="background-color: #0056b3; color: white; padding: 2px; text-align: center; font-weight: bold;">LOW</div> <p>Potential Improvement 5.0.2a – Refer to page 7</p>

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
5.0.3	Div 2, Sec 20Y	N/A	<p>In cases where Equifax holds credit reporting information that relates to consumer credit and it is satisfied that the individual has been a victim of fraud (including identity fraud) and consumer credit was provided as a result of that fraud, Equifax must destroy the credit reporting information, and within a reasonable period after the information is destroyed:</p> <ul style="list-style-type: none"> • give the individual a written notice that states that the information has been destroyed and sets out the effect of the notification of destruction to prior recipients of the information • give the CP a written notice that states that the information has been destroyed. <p>Equifax is not obliged to destroy the credit reporting information or notify prior recipients of the information of the destruction if Equifax is required by or under an Australian law, or a court / tribunal order, to retain the credit reporting information or not give such notification.</p>	 

6.0 Access

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
6.0.1	Div 2, Sec 20R (1), (2) & (3)	Para 19.1	If Equifax holds credit reporting information about an individual, Equifax must, on request by an access seeker, grant that access seeker access to the information. Equifax must respond to a request for access within 10 days. However it must not grant access without first obtaining reasonable evidence necessary to satisfy itself as to the identity of the person making the request and their entitlement to access under relevant privacy laws.	
6.0.2	Div 2, Sec 20R (4)	Para 19.4 & 19.6	For access free of charge, Equifax must provide the access seeker with access to: <ul style="list-style-type: none"> • all credit information relating to the individual currently held in the databases that Equifax utilises for the purposes of making disclosures permitted under Part IIIA; and • all current Equifax-derived information about the individual that is available, presented clearly and accessibly with reasonable explanation and summaries of the information to assist the access seeker to understand the impact of their credit worthiness. • if not provided in the manner requested by the access seeker, then Equifax must take reasonable steps to provide access in a way that meets the needs of Equifax and the individual. 	
			Where Equifax derived information about the individual is provided to an access seeker, Equifax may do so in a way that preserves the confidentiality of the methodology, data analysis methods, computer programs or other information that is used to produce the derived information.	
6.0.3	Div 2, Sec 20R (7)	N/A	Equifax is not required to give an access seeker access to credit reporting information if: <ul style="list-style-type: none"> • giving the access would be unlawful; or • denying access is required or authorised by or under an Australian law or a court / tribunal order; or • giving access would be likely to prejudice one or more enforcement related activities conducted by or on behalf of an enforcement body. 	
			Where Equifax refuses to give access to information based on one of the reasons above, Equifax must give a written notice to the assess seeker that <ul style="list-style-type: none"> • sets out the reasons for the refusal unless it is unreasonable to do so; and, • states that if the access seeker is not satisfied with the response to the request, the access seeker may access the recognised EDR scheme which Equifax is a member of or make a complaint to the Commissioner under Part V of the Privacy Act. 	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
6.0.4	Div 2, Sec 20R (5)	Para 19.2	Equifax must not charge the access seeker for making the request or for giving access to the information if a request has not been made to Equifax (in relation to the individual) in the previous 12 months.	
6.0.5	Div 2, Sec 20R (6)	Para 19.3	<p>If a request has been made within the previous 12 months, Equifax may charge the access seeker for giving access to the information, but not for making the request and the charge must not be excessive.</p> <p>Where Equifax has a fee-based service for providing an access seeker with credit reporting information:</p> <ul style="list-style-type: none"> • the information it makes available about the fee-based service must prominently state that individuals have a right under Part IIIA to obtain their credit reporting information free of charge in the following circumstances: <ul style="list-style-type: none"> ○ if the access request relates to a credit provider's decision to refuse the individual's consumer credit application ○ if the access request relates to a decision by a credit reporting body or credit provider to correct credit reporting information or credit eligibility information about the individual; and ○ once every 12 months • Equifax must take reasonable steps to ensure that its service, whereby individuals may obtain their credit reporting information free of charge, is as available and easy to identify and access as its fee-based service. 	

7.0 Correction of information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
7.0.1	Div 2, Sec 20S (1), 20T (2), (3) & (4) and 20U	Para 20.4	<p>Upon request by an individual, and if Equifax is satisfied that the credit-related personal information it holds about that individual is inaccurate, out-of-date, incomplete, irrelevant or misleading, Equifax must, within 30 days from when the request to correct was made or a longer period which the individual has agreed to in writing, take reasonable steps (if any) in the circumstances to:</p> <ul style="list-style-type: none"> • correct the information • ensure that any future derived information is based on the corrected credit information • ensure that any derived information that is based on the uncorrected credit information is not disclosed or used for the purpose of assessing the credit worthiness of the individual to whom the information relates. <p>If it considers that it cannot satisfy itself that the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, Equifax must consult with another CRB and / or CP which has an Australian link and holds or held the information.</p>	 
7.0.2	N/A	Para 20.2	If consulted by another CRB or CP about a correction request, Equifax must take reasonable steps to respond to the consultation request as soon as practicable.	
7.0.3	N/A	Para 20.3	<p>If Equifax forms the view that it will not be able to resolve an individual's correction request within the 30 day period, Equifax must as soon as practicable:</p> <ul style="list-style-type: none"> • notify the individual of the delay, the reasons for this and the expected timeframe to resolve the matter • seek the individual's agreement to an extension for a period that is reasonable in the circumstances • advise that the individual may complain to a recognised EDR scheme which Equifax is a member of (and provide contact details for that scheme) or to the Commissioner. <p>If the individual has not agreed to the requested extension, Equifax must as soon as practicable provide a response to the correction request within the timeframe sought for extension.</p>	 

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
7.0.4	N/A	Para 20.5 & 20.6	If, under paragraph 20.5(a), Equifax is satisfied that default information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to the purpose for which the information is held by Equifax then Equifax must correct the credit reporting information by destroying that default information.	
7.0.5	Div 2, Sections 20S (2) & (3) and 20U (2), (4) & (5)	Para 20.7	If, on request by an individual, Equifax makes a correction to credit-related personal information, Equifax must give the written notice of correction to the following within 5 business days of the decision: <ul style="list-style-type: none"> • The individual the correction relates to • The interested party, i.e. the CP or CRB it consulted with (if applicable) regarding a correction request • The recipient of the information if Equifax had previously disclosed the information (apart from disclosures made for the purposes of determining whether unsolicited credit information could have been collected by Equifax if it had solicited the information, or for purposes of consulting with another CRB or CP regarding a correction request) unless it is impracticable for Equifax or Equifax is required by or under an Australian law or a court / tribunal order not to give the notice. 	
7.0.6	Div 2, Section 20U (3) & (5)	Para 20.7 & 20.9	The notice to the individual must: <ul style="list-style-type: none"> • explain what CRBs, CPs and affected information recipients Equifax is intending to notify (<i>only applicable if Equifax relies on paragraph 20.9 of the CR Code</i>) • ask the individual if there is any other CP or affected information recipients that the individual would like Equifax to notify (<i>only applicable if Equifax relies on paragraph 20.9 of the CR Code</i>) • include all relevant credit reporting information held by Equifax so that the individual can check that the information has been appropriately corrected • explain that the individual has a right under the CR Code to obtain their credit reporting information from Equifax free of charge if the access request relates to the decision by a CRB or a CP to correct information about the individual, and how that right may be exercised. <p>Unless it is impracticable or illegal to do so, the notification obligation is met if within 7 business days of the correction Equifax gives notice of the correction to:</p> <ul style="list-style-type: none"> • All CRBs to which it disclosed the pre-corrected information; • All CPs and affected information recipients to which it disclosed the pre-corrected information within the previous 3 months; and • Any other CP or AIR nominated by the individual and to which it disclosed the pre-corrected information more than 3 months previously. 	 
7.0.7	N/A	Para 20.9	<i>Only applicable if Equifax relies on paragraph 20.9 of the CR Code:</i> Unless it is impracticable or illegal to do so, if notice is given to a CP or AIR that previously received Equifax derived information that is no longer correct by reason of the correction, the notice must include revised Equifax derived information that has been derived using the correct information.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
7.0.8	N/A	Para 20.8	Where Equifax corrects credit-related personal information by updating identification information about an individual, Equifax is not obliged to notify any previous recipient of the information about the updating of that information, unless requested by the individual.	
7.0.9	Div 2, Sec 20T (5)	N/A	Equifax must not charge the individual for requesting the correction or for correcting the information.	
7.0.10	Div 2, Sec 20U (3)	N/A	<p>If Equifax does not correct the personal information in response to an individual request, Equifax must give the individual written notice which covers the following within a reasonable period:</p> <ul style="list-style-type: none"> • states that the correction has not been made • sets out Equifax’s reasons for not correcting the information, including evidence substantiating the correctness of the information • states that if the individual is not satisfied with the response to the request, the individual may access the recognised EDR scheme which Equifax is a member of or make a complaint to the Commissioner. 	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
8.0.3	Div 2, Sec 20K (4) & (5)	N/A	<p>If the individual requests an extension to the ban period (of 21 days) before the period ends, and Equifax believes on reasonable grounds that the individual has been, or is likely to be, a victim of fraud (including identity fraud) Equifax must:</p> <ul style="list-style-type: none"> • extend the ban period by such period as Equifax considers is reasonable in the circumstances (a ban period for credit reporting information may be extended more than once); and • give the individual written notification of the extension. 	
8.0.4	Div 2, Sec 20K (6)	N/A	<p>Equifax must not charge the individual for the making of the request or for giving effect to the request for a ban and/or an extension of a ban period.</p>	

9.0 Complaints

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
9.0.1	Div 5, Sec 23B and 23C (2)	Para 21.3 & 21.5	<p>If a complaint is made to Equifax about its acts or practices that may be a breach of certain provisions of Part IIIA or the CR Code, Equifax must investigate the complaint and make a decision about the complaint.</p> <p>Specifically Equifax must:</p> <ul style="list-style-type: none"> • give the individual a written notice within 7 days after the complaint is made that acknowledges the making of the complaint and sets out how Equifax will deal with the complaint • investigate the complaint • give the individual a written notice that sets out the decision and states that if the individual is not satisfied with the decision, the individual may access a recognised external dispute resolution (EDR) scheme of which Equifax is a member of or make a complaint to the Commissioner within 30 days from the day the complaint was made or a longer period that the individual has agreed to in writing. <p>Equifax must consult a CRB or CP about the complaint if it considers it necessary, and the use or disclosure of personal information for this purpose is permitted under the Act.</p> <p>If Equifax is consulted by another CRB or CP about a complaint , Equifax must take reasonable steps to respond to the consultation request as soon as practicable.</p> <p>If the complaint relates to credit information or credit eligibility information that a CP holds, Equifax must notify the provider of the making of the complaint and the making of a decision about the complaint as soon as practicable after each are made unless it is impracticable to give the notification or Equifax is required by or under an Australian law, or a court / tribunal order, not to give the notification.</p> <p>Unless it is impracticable or illegal to give notice to a CP about a complaint relating to a CRB's act of practice that may breach Section 20S, this obligation is taken to be met if Equifax gives notice as soon as practicable to:</p> <ul style="list-style-type: none"> • the CP if the complaint relates to credit information that was disclosed to Equifax by a CP • any other CP to which Equifax disclosed the credit information to which he complaints relates in the previous 3 months • any other CP that has been nominated by the individual for this purpose. 	  

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
9.0.2	N/A	Para 21.4	<p>If Equifax forms the view that it will not be able to resolve a complaint within the 30 day period required by Part IIIA, Equifax must</p> <ul style="list-style-type: none"> inform the individual of this before the end of the 30 day period and provide the reason for the delay, the expected timeframe to resolve the complaint and seek their agreement to an extension for a period that is reasonable in the circumstances advise that the individual may complain to the recognised EDR scheme of which Equifax is a member, and provide the contact details for that scheme, or to the Commissioner. 	
9.0.3	Div 5, Sec 23A (4)	N/A	<p>If Equifax discloses credit reporting information to which the complaint relates and a decision has not been made about the complaint at the time of the disclosure, Equifax must notify in writing the recipient of the information of the complaint at that time unless it is impracticable to give the notification or Equifax is required by or under an Australian law, or a court / tribunal order, not to give the notification.</p>	
9.0.4	Div 5, Sec 23A (5)	N/A	<p>Equifax must not charge the individual for making of the complaint or for dealing with the complaint.</p>	
9.0.5	N/A	Para 21.2	<p>Equifax must be a member of a recognised EDR scheme.</p>	

10.0 Credit reporting system integrity

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
10.0.1	N/A	Para 23.11	<p>Equifax must publish on its website by 31 August each year a report for the financial year ending 30 June of the same year that includes information about the following:</p> <ul style="list-style-type: none">• access• corrections• complaints• serious credit infringements• Equifax's monitoring and auditing activity• Disclosure of CCLI and RHI to Equifax• Any other information requested by the Commissioner.	

11.0 Independent Review of Compliance

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
11.0.1	N/A	Para 24.2	Every 3 years or more frequently if the Commissioner requests, Equifax must commission an independent review of its operations and processes to assess compliance by Equifax with its obligations under Part IIIA, the Regulations and the CR code.	
11.0.2	N/A	Para 24.2	Equifax must consult with the Commissioner as to the choice of reviewer and scope of the review.	
11.0.3	N/A	Para 24.2	The review report and Equifax's response to the review report must be provided to the Commissioner and made publicly available.	

Appendix



Equifax Risk Assessment

The risk assessment process implemented as part of this review was completed by developing an understanding of the risk by assessing the causes and sources of risk, their positive or negative consequences, and the likelihood of their occurrence. Existing controls and their effectiveness were taken into account.

The level of risk identified during risk analysis were ranked and prioritised in accordance with the following risk rating criteria:

Consequence

Determination of Consequence Rating					
Consequence Category	Insignificant	Minor	Moderate	Major	Significant
Consequence					
Reputation	Letters to local/state/trade media or stakeholders	Series of articles in local/state/trade media, or repeated queries from stakeholders	Extended negative local/state/trade media coverage or repeated criticism from stakeholders	Short-term nation wide negative media coverage or sustained campaign of criticism from stakeholders	Extensive negative nation wide media coverage or concerted campaign to constrain or operations by stakeholder
Regulatory	Minor breaches by individual staff members	No fine or disruption to service delivery	Fine but no disruption to service delivery	Fine and disruption to service delivery	Significant disruption to service delivery over an extended period of time

Likelihood

The likelihood that the business will be exposed to the specific risk considering factors such as:

- Anticipated frequency
- The external environment
- The procedures, tools and skills currently in place
- History of previous events

Likelihood assessment					
	Rare	Unlikely	Possible	Likely	Almost Certain
Industry evidence	No reported occurrences within the industry over the last 3 years	Has occurred internationally, but no reported incidents within the Australian / NZ industry	Has occurred in last 2 years within the Australian / NZ industry	Has occurred on multiple occasions in the last year within the Australian / NZ industry	Occurs frequently across the Australian / NZ industry

Risk Rating Table

The assessment of consequence and likelihood derived a risk score in accordance with the Risk Rating Table below:

		Consequence				
		Insignificant	Minor	Moderate	Major	Significant
L i k e l i h o o d	Almost Certain	Medium	High	Extreme	Extreme	Extreme
	Likely	Medium	High	High	Extreme	Extreme
	Possible	Medium	Medium	High	High	Extreme
	Unlikely	Low	Medium	Medium	High	High
	Rare	Low	Low	Medium	Medium	High

Glossary

Access Seeker	The individual or a person who is assisting the individual to deal with a credit reporting body or credit provider and who is authorised, in writing, by the individual to make a request in relation to the information under subsection 20R(1) or 21T(1) to access or correct the individual's information. The access seeker is not a credit provider, a mortgage insurer, a trade insurer or a person who is prevented from being a credit provider by subsection 6G(5) or (6).	Credit Provider	Each of the following is a credit provider: (a) a bank; (b) an organisation or small business operator if the organisation or operator carries on a business or undertaking; and a substantial part of the business or undertaking is the provision of credit; (c) an organisation or small business operator that carries on a retail business; and that, in the course of the business, issues credit cards to individuals in connection with the sale of goods, or the supply of services, by the organisation or operator (as the case may be); (d) an agency, organisation or small business operator that carries on a business or undertaking that involves providing credit; and that is prescribed by the regulations.
Affected information recipient	A mortgage insurer, trade insurer, body corporate, person or an entity or adviser.		The following are also credit providers (only in relation to the credit): (a) a supplier providing credit in connection with the sale of goods, or the supply of services, by the supplier; and the repayment, in full or in part, of the amount of credit is deferred for at least 7 days; (b) a lessor providing credit in connection with the hiring, leasing or renting of goods; and the credit is in force for at least 7 days; and no amount, or an amount less than the value of the goods, is paid as a deposit for the return of the goods.
Credit information	Personal information (other than sensitive information) that is: (a) Identification information (b) Consumer credit liability information (c) Repayment history information (d) A statement that an information request has been made in relation to the individual by a credit provider, mortgage insurer or trade insurer (e) The type of consumer credit or commercial credit, and the amount of credit, sought in an application that has been made by the individual to a credit provider and in connection with which the provider has made an information request in relation to the individual (f) Default information (g) Payment information (h) New arrangement information (i) Court proceedings information (j) Personal insolvency information (k) Publicly available information that relates to the individual's activities in Australia or the external Territories and the individual's credit worthiness and that is not court proceedings information about the individual or information about the individual that is entered or recorded on the National Personal Insolvency Index (l) The opinion of a credit provider that the individual has committed, in circumstances specified by the provider, a serious credit infringement in relation to consumer credit provided by the provider to the individual.	Credit Reporting Business	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.
		CRB derived information	Any personal information (other than sensitive information) about the individual that is derived by a credit reporting body from credit information about the individual that is held by the body, that has any bearing on the individual's credit worthiness and that is used, has been used or could be used in establishing the individual's eligibility for consumer credit.

Glossary

AIR	Affected information recipient
Commissioner	Office of the Australian Information Commissioner
CCLI	Consumer credit liability information
CCR	Comprehensive Credit Reporting
CRB	Credit Reporting Body
CRM	Customer Relationship Management
CP	Credit Provider
EDR	External dispute resolution
Equifax	Equifax's Credit Reporting Bureau
RHI	Repayment history information

Grant Thornton Australia Limited ABN 41 127 556 389 ACN 127 556 389

'Grant Thornton' refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. Grant Thornton Australia Ltd is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate one another and are not liable for one another's acts or omissions. In the Australian context only, the use of the term 'Grant Thornton' may refer to Grant Thornton Australia Limited ABN 41 127 556 389 and its Australian subsidiaries and related entities. GTIL is not an Australian related entity to Grant Thornton Australia Limited. Liability limited by a scheme approved under Professional Standards Legislation. Liability is limited in those States where a current scheme applies.

