

April 2021

EQUIFAX AUSTRALIA INFORMATION SERVICES AND SOLUTIONS PTY LTD


Independent Review of Compliance with Part IIIA Privacy Act 1988



CONTENTS

PAGE 3	EXECUTIVE SUMMARY
PAGE 6	FINDINGS
PAGE 29	APPENDIX





EXECUTIVE SUMMARY

INTRODUCTION

This triennial Independent Review of Compliance was undertaken by BDO to ensure Equifax Australia Information Services and Solutions Pty Ltd's (Equifax) compliance with Part IIIA of the Privacy Act 1988 (Cth) ('Act') every three years.

Under paragraph 24.2 of the Privacy (Credit Reporting) Code, as a Credit Reporting Body (CRB), Equifax must undertake an independent review of its operations and processes to assess compliance with its obligations detailed in Part IIIA of the Privacy Act 1998 (Cth) ('Act').

The Engagement Letter dated December 2020 sets out the purpose, scope, and limitations in relation to this Independent Review.

OBJECTIVE AND SCOPE

The objective of this Independent Review was to assess the design effectiveness of operations and process controls that assist Equifax to comply with Part IIIA of the Act as follows:

- 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;
- 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; and
- Internal handling of complaints.

In preparing this report, compliance has been assessed against the requirements of the Act and the Code. Any instances of non-compliance would be risk rated using Equifax's risk rating matrix. Given there are no instances of non-compliance to assess, as detailed in the **Summary of Findings** section, the risk rating matrix is omitted from this report.

LIMITATION OF SCOPE

The scope of this review is limited to ensuring Equifax's designed controls pertaining to the Equifax Apply product comply with requirements of:

- Part IIIA of the Privacy Act 1998 (Cth) ('Act');
- The Regulations; and
- The Privacy (Credit Reporting) Code 2014 (version 2.1).

No other Equifax product or service has been considered and no other Privacy or Security principles, regulations, legislation or guidelines have been considered.

SUMMARY OF KEY FINDINGS

No instances of non-compliance were observed during the independent review. The **Summary of Compliance** table on the following page details the compliance on a section level.

ACKNOWLEDGEMENT

We would like to take this opportunity to thank all Management and staff of Equifax for their co-operation and assistance during the course of the Independent Review.

Yours faithfully,



MARK GRIFFITHS
Partner, Risk Advisory

SUMMARY OF COMPLIANCE

Report Ref	Area	Part IIIA	CR Code Ref	Compliance Status
1.0	Open and transparent management of credit reporting information	20B	3	Full Compliance
2.0	Credit reporting system arrangements			Full Compliance
2.1	Subscriber agreements	20N(3) & 20Q(2)	2.1& 15	Full Compliance
2.2	Training	20N(3) & 20Q(2)	2.2	Full Compliance
3.0	Credit information handling practices, procedures and systems			Full Compliance
3.1	Collection of credit information	20C, 20D & 20L	5.1(a), 5.2, 5.4(a)-(c), 6-12	Full Compliance
3.2	Use and disclosure of credit information	20E, 20F, 20M & 20P	7, 8, 9, 14, 16 & 18	Full Compliance
3.3	Integrity of credit reporting information	20N	5.4(d)-(f)	Full Compliance
3.4	Credit provider audits and breaches	20N & 20Q	5.4, 23	Full Compliance
4.0	Security of credit reporting information	20Q	15.1	Full Compliance
5.0	Record keeping	20F, 20K, 20V-20Z & 20ZA	1.2(f), 22	Full Compliance
6.0	Access	20R	19	Full Compliance
7.0	Correction of information	20S-20U, 21V, 21U & 21W	20	Full Compliance
8.0	Protections for victims of fraud	20K	17	Full Compliance
9.0	Complaints	20T & Div5, 23	20 & 21	Full Compliance
10.0	Credit reporting system integrity	N/A	23.11	Full Compliance
11.0	Independent review of compliance	N/A	24.2	Full Compliance



FINDINGS

GLOSSARY AND COMPLIANCE LEGEND

COMPLIANCE LEGEND

Full Compliance

Partial Compliance

Non-compliance





ACRONYMS AND ABBREVIATIONS USED

Full Terminology	Abbreviation
Office of the Australian Information Commissioner	Commissioner or OAIC
Part IIIA Privacy Act 1988	The Act
Privacy (Credit Reporting)Code	The Code or CR Code
Credit Provider	CP
Credit reporting Body	CRB
Customer Relationship Management	CRM
External Dispute Resolution	EDR
Repayment History Information	RHI
Affected Information Recipient	AIR



FINDINGS

1 Open and transparent management of Creditor Reporting Information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
1.1	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 includes the following information:</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; and • 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. 	
1.2	Div 2, Sec 20B (5)	Para 3.1	The Credit Reporting Policy must be available for free and published on the Equifax website.	

2 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, which oblige both parties to comply with Part IIIA, the Regulations and CR Code to the extent applicable at the time. The signed agreement must require the provider to:</p> <ul style="list-style-type: none"> • ensure that credit information that they disclose to Equifax is accurate, up-to-date and complete; and • protect credit reporting information that is disclosed to them from misuse, interference and loss, unauthorised access, modification or disclosure. 	

2.2 Training

2.2.1	Div 2, Sec 20N(3) and 20Q(2)	Para 2.2(a) and Para 2.2 (b)	<p>Equifax must ensure processes are in place to inform employees who handle credit reporting information of the requirements of Part IIIA, the Regulations and the CR code; and train employees who have ownership of or handle credit reporting information in the practices, procedures and systems that are designed to achieve compliance with those requirements.</p>	
-------	------------------------------	------------------------------	---	--



3 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>Equifax must 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 (unless required or authorised by or under an Australian law or a court/tribunal order). Equifax may also collect credit information from an entity other than a CP, in accordance with section 20C(4) Where the information collected from a CP is:</p> <ul style="list-style-type: none"> • identification information - Equifax also collects from the provider, or already holds, credit information of another kind about the individual; and • consumer credit liability information - 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; and • 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	In cases where Equifax collects information from an entity which is not a CP and the information is RHI about an individual, Equifax must ensure it only collects the information from another CRB with an Australian link.	
3.1.3	Div 2, Sec 20L	N/A	Unless the adoption of government related identifiers is required or authorised by or under an Australian law or a court/ tribunal order, when Equifax holds credit reporting information about an individual which is a government related identifier of the individual, Equifax must not adopt the government related identifier as its own identifier of the individual.	



3 Credit Information Handling Practices, Procedures and Systems cont'd

3.1 Collection of Credit Information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
3.1.4	Section 6N(K)	Para 11	<p>Equifax must ensure only publicly available information is collected for an individual from an agency or a state or territory authority and the content of the information collected must be generally available to the public. Additional requirements of Section 6N(k) must also be met, i.e.:</p> <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). <p>Publicly available information does not include:</p> <ul style="list-style-type: none"> • originating process issued by a Court or Tribunal; or • any judgment or proceedings where the individual's rights have been subrogated to an insurer; or • any judgment or proceedings that is otherwise unrelated to credit; because this information does not relate to the individual's creditworthiness. 	
3.1.5	Div 2, Sec 20D	N/A	<p>In cases where Equifax receives unsolicited credit information about an individual, the company must determine whether the information could have been collected under section 20C if Equifax had solicited the information. This must occur within a reasonable period after receiving the information.</p> <p>If Equifax determines that it could have collected the credit information, Equifax can choose to 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 have processes in place to destroy the information as soon as possible.</p>	




3 Credit Information Handling Practices, Procedures and Systems cont'd

3.2 Use and Disclosure of Credit Information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
3.2.1	Div 2, Sec 20E (1) & (2)	Para 18.1	<p>Equifax is only permitted to, and has processes in place to ensure, that credit reporting information is limited to use in the following manner:</p> <ul style="list-style-type: none"> • in the course of carrying on its credit reporting business; • if the use is required or authorised by or under an Australian law or a court/tribunal order; and • if the use is a use prescribed by the regulations. 	
3.2.2	Div 2, Sec 20E, 20F and 20P	Para 7, 8, 9 and 14	<p>Equifax is permitted to disclose credit reporting information about an individual if:</p> <ul style="list-style-type: none"> • in relation to the individual the disclosure is a permitted CRB disclosure under section 20F; • the disclosure is to another CRB that has an Australian link; • the disclosure is for the purposes of a recognised external dispute resolution ('EDR') scheme and Equifax (or the CP) is a member of the scheme; • the disclosure is to an enforcement body and Equifax is satisfied that the body, or another enforcement body, believes on reasonable grounds that the individual has committed a serious credit infringement; and • in relation to RHI the recipient is a CP who is a licensee or is prescribed by the regulations or a mortgage insurer. <p>The CR Code also provides the conditions under which Equifax can disclose certain credit information, which include the following instances:</p> <ul style="list-style-type: none"> • Where a CP makes an information request to Equifax in connection with an application for consumer credit and the amount of credit is unknown or incapable of being specified, the credit information that Equifax may collect and disclose may include that an unspecified amount of consumer credit is being sought from the CP. • Equifax is only permitted to disclose RHI to a CP that is a licensee or is prescribed by the Regulations. • Equifax is only permitted to collect and disclose default information if certain preconditions are met, including the consumer credit payment must be overdue by at least 60 days, the overdue amount must not be less than \$150 (or if a higher amount is prescribed by the Regulations, that amount) and the CP must have met the notice obligations specified in Part IIIA, the Regulations and the CR Code. • Before Equifax discloses credit reporting information to a CP, mortgage insurer or trade insurer, Equifax must have taken reasonable steps to ensure that the CP, mortgage insurer or trade insurer has been notified of the requirements of the Privacy Act, the Regulations and the CR code governing limitations on use and disclosure of credit reporting information. 	


3 Credit Information Handling Practices, Procedures and Systems cont'd

3.2 Use and Disclosure of Credit Information


Ref #	Part IIIA Ref	CR Code REF	Summary of Obligations	Compliance Assessment
3.2.3	N/A	Para 16	<p>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 their obligations in relation to consumer credit provided by the CP to the individual. Equifax must have processes in place to ensure that:</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. 	
3.2.4	Div 2, Sec 20P	Para 20.4 (ii) & (iii)	<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; or it is in consultation for the correction of credit information. 	
3.2.5	Div 2, Sec 20M	N/A	<p>Equifax can only 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 Credit Information Handling Practices, Procedures and Systems cont'd

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 ensure that the credit information it collects, uses and discloses is having regard to the purpose of the use or disclosure and is accurate, up-to-date, complete and relevant. Equifax is also obligated to have reasonable practices, procedures and systems that are designed to cover the obligations under Part IIIA, the Regulations and the CR Code which allow 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 timely, 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; and • 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. 	

3.4 Credit Provider Audits and Breaches

3.4.1	Div 2, Sec 20N and 20Q	Para 23.1 & 23.2	<p>Equifax must establish a documented, risk based program to monitor CP compliance with obligations stipulated under Part IIIA. The established program must 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 and should be incorporated into CP agreements with Equifax. The program 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; and ○ 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; and • include an audit program for CPs to assess compliance with their obligations referred to in paragraph 23.1 of the CR code. 	
-------	------------------------	------------------	--	---


3 Credit Information Handling Practices, Procedures and Systems cont'd

3.4 Credit Provider Audits and Breaches


Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
3.4.2	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 ensure that regular audits are conducted by an independent person to determine if agreements with CPs are being complied with, identify suspected breaches of agreement and deal with these instances as they arise.</p> <p>The risk based program established by Equifax must include a designated CP audit program. The program must be designed for CPs to assess compliance with their obligations, in turn ensuring 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. <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; and • 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 have processes in place to ensure that a person conducting 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 Credit Information Handling Practices, Procedures and Systems cont'd



3.4 Credit Provider Audits and Breaches

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
3.4.3	Div 2, Sec 20N	Para 5.4 (g)	<p>Where Equifax identifies credit information that is not accurate, up-to-date and complete, processes must be in place to ensure this is raised, 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. <p>Equifax must have reasonable practices, procedures and systems in place to cover its legislative obligations and enable it to report about testing (which has been undertaken in accordance with paragraph 5.4(d) of the CR code), and any material findings or material changes to procedures of CPs with which it has an agreement regarding credit information disclosure (by the CP to Equifax and vice versa) as referred to in section 20N(3) and section 20Q(2) respectively.</p>	


4 Security of Credit Reporting Information

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




5 Record Keeping

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
5.1	Div 2, Sec 20F and 20K(2)	Para 22	<p>The minimum period of time which each record must be maintained for by Equifax is 5 years from the date on which the record is made. This is the case for all records, except if 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 these cases, the record must be retained for the duration of that retention period only.</p> <p>Records must be maintained in an adequate manner to evidence Equifax’s 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; and • records of any consent provided by an individual for the purposes of Part IIIA, the Regulations or the CR Code. 	
5.2	Div 2, Sec 20V, 20W, 20X, 20Z and 20ZA	Para 1.2(f)	<p>Retention periods do not exist 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. Other retention periods stipulated by the Act range from 2 to 7 years, depending on the nature of the information (refer sections 20W, 20X, 20Y and 20Z of the Act).</p> <p>Credit information and any related CRB-derived information must be destroyed or de-identified by Equifax within 1 month after the relevant retention period. Exceptions of this instance include the following, if:</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>Equifax is obligated to “destroy” credit information or credit reporting information, which is a requirement of Equifax to ensure it irretrievably destroys the information or places electronically formatted information ‘beyond use’.</p>	



5 Record Keeping cont'd

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
5.3	Div 2, Sec 20Y	N/A	<p>If Equifax holds credit reporting information that relates to consumer credit where the individual has reportedly been a victim of fraud and consumer credit was provided as a result of this fraud, Equifax must, if satisfied by the report, destroy the credit reporting information. Equifax must also ensure that within a reasonable timeframe after the destruction of information to:</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>In cases where 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, Equifax does not have an obligation to destroy the credit reporting information or notify prior recipients of the information relating to the destruction.</p>	

6 Access

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
6.1	Div 2, Sec 20R (1), (2) & (3)	Para 19.1	<p>When an access seeker makes a request for credit reporting information, Equifax must grant that access seeker access to the information, with a response to the request provided within a reasonable period, but no longer than 10 days. Equifax must take reasonable steps to ensure access is not granted without first obtaining reasonable evidence to satisfy the identity of the person making the request and their entitlement to access under relevant privacy laws.</p>	
6.2	Div 2, Sec 20R (4)	Para 19.4 & 19.6	<p>Equifax is obligated to provide the following information to access seekers free of charge:</p> <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. <p>Equifax may choose to provide Equifax-derived information about individuals to access seekers in a manner that preserves the confidentiality of the methodology, data analysis methods, computer programs or other information that is used to produce the information.</p> <p>Equifax must ensure that direct marketing communication is only provided to access seekers if the individual has consented to receipt of this communication. Pre-ticked consent boxes do not constitute consent.</p>	
6.3	Div 2, Sec 20R (7)	N/A	<p>Equifax is not required to give an access seeker access to credit reporting information if:</p> <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. <p>In the case 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</p> <ul style="list-style-type: none"> • states the reasons for the refusal unless it is unreasonable to do so; and, • provides information of the recognised EDR scheme which Equifax is a member of or make a complaint to the Commissioner under Part V of the Privacy Act should the access seeker remain unsatisfied. 	




6 Access cont'd

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
6.4	Div 2, Sec 20R (5) & (6)	Para 19.2	<p>Provided an access request relating to an individual has not been made to Equifax in the prior 3 months, Equifax must not charge an access seeker for making the request or providing the information, in accordance with the legislative requirements in the period assessed.</p>	
6.5	Div 2, Sec 20R (6)	Para 19.3	<p>Equifax may charge the access seeker for giving access to the information if a request has been made in the prior 12 months, but not for making the request and the charge must not be excessive.</p> <p>In the case where a fee-based service for providing an access seeker with credit reporting information exists, Equifax must:</p> <ul style="list-style-type: none"> • ensure that the free service is equally as available and easy to identify as the fee-based charge; and • make available the information about the fee-based service but also 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. 	





7 Correction of Information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
7.1	Div 2, Sec 20S (1), 20T (2), (3) & (4) and 20U	Para 20.4	<p>If Equifax is satisfied that the credit-related personal information it holds about an individual is inaccurate, out-of-date, incomplete, irrelevant or misleading, and has been requested by an individual to correct it, 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):</p> <ul style="list-style-type: none"> • correct the information; • ensure that any future derived information is based on the corrected credit information; and • 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>In cases where Equifax is not satisfied 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>	
7.2	Div 2, Sec 20T and 21V	Para 20.2	<p>Equifax must have reasonable process in place to respond to consultation requests from other CRBs/CPs about correction requests as soon as practicable.</p>	
7.3	Div 2, Sec 20T and 21V	Para 20.3	<p>In cases where Equifax is not able to respond to a correction request within the designated 30 day time period, processes must be in place to ensure the following steps are made by Equifax:</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>Where an individual does not agree to a requested extension, Equifax must as soon as practicable provide a response to the correction request within the timeframe sought for extension.</p>	



7 Correction of Information cont'd

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
7.4	N/A	Para 20.5 & 20.6	Upon request by an individual, Equifax must correct credit reporting information by destroying that default information 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, or under paragraph 20.6, the CP is prevented by a statute of limitations from recovery of the amount.	
7.5	Div 2, Sections 20S (2) & (3) and 20U (2), (4) & (5)	Para 20.7	<p>Where Equifax makes a correction to credit-related personal information as a result of an individual request, Equifax must give the written notice of correction to the following within 5 business days of the decision:</p> <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; and • The recipient of the information if Equifax had previously disclosed the information (excluding 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. 	
7.6	Div 2, Section 20U (3) & (5)	Para 20.7 & 20.9	<p>Notices regarding corrections which are sent to the individual must:</p> <ul style="list-style-type: none"> • explain what CRBs, CPs and affected information recipients Equifax is intending to notify (only applicable if Equifax relies on paragraph 20.9 of the CR Code); • ask the individual if there is any other CP or affected information recipients that the individual would like Equifax to notify (only applicable if Equifax relies on paragraph 20.9 of the CR Code); • include all relevant credit reporting information held by Equifax so that the individual can check that the information has been appropriately corrected; and • 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 Correction of Information cont'd

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
7.7	Div 2, Sec 20S(2), 20U(2), 21U(2) and 21W(2)	Para 20.9	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 provided by Equifax must include revised information that has been derived using the newly correct information, excluding cases where it is impracticable or illegal to do so.	
7.8	N/A	Para 20.8	Unless Equifax is requested by the individual, in cases where Equifax corrects credit-related personal information by updating identification information about the individual, Equifax is not obliged to notify any previous recipient of the information about the updating of that information.	
7.9	Div 2, Sec 20T (5)	N/A	Equifax must provide a free service to the individual for requesting the correction or for correcting the information.	
7.10	Div 2, Sec 20U (3)	N/A	<p>In cases where Equifax does not correct the personal information in response to an individual request, Equifax must provide the individual with 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; and • 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. 	


8 Protection for Victims of Fraud

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
8.1	Div 2, Sec 20K (1), (2) & (3)	Para 17.1 and 17.3	<p>If an individual believes on reasonable grounds that they have been, or are likely to be, a victim of fraud, and the individual has requested Equifax not to use or disclose credit reporting information about them, Equifax must instigate a ban period. During the ban period Equifax must not use or disclose information about an individual unless:</p> <ul style="list-style-type: none"> the individual expressly consents, in writing, to the use or disclosure of the credit reporting information; or the use or disclosure of the credit reporting information is required by or under an Australian law or a court/tribunal order. <p>The ban period commences when the individual makes the ban request and ends either 21 days after the day on which the request is made or on the day after any extension period ends.</p> <p>When a ban request has been initiated, Equifax must immediately:</p> <ul style="list-style-type: none"> include on the credit reporting information held in relation to the individual a notation about the individual's request and retain this for the duration of the ban period; and explain to the individual the effect and duration of the ban period, including that the individual may not be able to access credit during the ban period. <p>In cases where a ban period has been established, Equifax must notify the individual not less than 5 business days before the end of the ban period of the date the ban period is due to finish, about the individual's rights under Part IIIA, the Regulations and this CR Code to extend the ban period; and what, if any, information Equifax requires to support the individual's allegation of fraud.</p> <p>Equifax must explain to an individual that they may request a ban period with other CRBs, and that the individual can consent to Equifax notifying the CRBs nominated by the individual. Where this additional ban period request is made by the individual, Equifax must, as soon as reasonably practicable, provide the notified CRBs with the ban period request provided by the individual. Ban requests received from other CRBs must be treated as if they were received from the individual directly.</p>	
8.2	N/A	Para 17.2	<p>If Equifax received as request from a CP, mortgage insurer or trade insurer for credit reporting information about an individual whose credit reporting information has a ban period in effect, Equifax must inform the CP, mortgage insurer or trade insurer of the ban period and its effect.</p>	





8 Protection for Victims of Fraud cont'd

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
8.3	Div 2, Sec 20K (4) & (5)	N/A	<p>In cases where an individual requests an extension to the ban period (of 21 days) before the period ends, and Equifax is satisfied that the individual has been, or is likely to be, a victim of 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. 	
8.4	Div 2, Sec 20K (6)	N/A	<p>Equifax must provide ban-related services free of charge to the individual, including for the making of the request, for giving effect to the request and/or an extension of a ban period.</p>	


9 Complaints

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
9.1	Div 5, Sec 23B and 23C (2)	Para 21.3 & 21.5	<p>In situations where a complaint is raised 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. Equifax must ensure the following:</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; and • 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>If considered necessary, Equifax must consult a CRB or CP about the complaint. Use or disclosure of personal information for this purpose is permitted under the Act. In cases where 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 a complaint is raised that 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; and • any other CP that has been nominated by the individual for this purpose. 	<p>Compliance Assessment</p> 




9 Complaints cont'd

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
9.2	20T and 21V	Para 20.3 and 21.4	<p>Where Equifax feels it will be unable 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; and 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. <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>	
9.3	Div 5, Sec 23C (4)	N/A	<p>If cases where Equifax discloses credit reporting information to which a complaint relates and a decision is yet to be made about the complaint at the time of the disclosure, Equifax must notify in writing the recipient of the information 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>	
9.4	Div 5, Sec 23A (5)	N/A	<p>Equifax must not charge the individual for complaint-related services, including the making of the complaint or for dealing with the complaint.</p>	
9.5	N/A	Para 21.2	<p>Equifax must be a member of a recognised EDR scheme.</p>	

10 Credit Reporting System Integrity

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
10.1	N/A	Para 23.11	<p>A report for the financial year ending 30 June must be published by Equifax on its website by 31 August of the same year. The report must include 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; and • Any other information requested by the Commissioner. 	

11 Independent Review of Compliance

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations	Compliance Assessment
11.1	N/A	Para 24.1 & 24.2	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. This must occur at minimum every 3 years or more frequently if the Commissioner requests.	
11.2	N/A	Para 24.2	Equifax is obligated to consult with the Commissioner regarding the choice of independent reviewer and scope of the review.	
11.3	N/A	Para 24.2	The Commissioner must be provided the review report and Equifax’s response to the review report, both of which must also be made publicly available.	



APPENDIX

APPENDIX A - CHANGES TO THE PRIVACY (CREDIT REPORTING) CODE 2014

The last triennial review was conducted against version 1.2 of the Privacy (Credit Reporting) Code 2014. The Current Version is now 2.1 and hence, we have summarised the core changes to the Code.

Paragraph	Version 1.2	Version 2.1
8.2C(ii)	<p>Where there is an amount overdue in relation to consumer credit, the age of the oldest outstanding payment:</p> <ol style="list-style-type: none"> 1. Up to 29 days overdue (after the grace period has been applied) 2. 30 - 59 days overdue 3. 60 - 89 days overdue 4. 90 - 119 days overdue 5. 120 - 149 days overdue 6. 150 - 179 days overdue 7. 180 + days overdue. 	<p>Where there is an amount overdue in relation to the consumer credit, the age of the oldest outstanding payment:</p> <ol style="list-style-type: none"> 1. 15 - 29 days overdue (this disclosure may only be made at day 15, as this allows for expiry of the 14-day grace period) 2. 30 - 59 days overdue 3. 60 - 89 days overdue 4. 90 - 119 days overdue 5. 120 - 149 days overdue 6. 150 - 179 days overdue X. 180 + days overdue.
11.2	Not previously present in the Code	<p>11.2 For the avoidance of doubt publicly available information does not include:</p> <ol style="list-style-type: none"> (a) originating process issued by a Court or Tribunal; or (b) any judgment or proceedings where the individual's rights have been subrogated to an insurer; or (c) any judgment or proceedings that is otherwise unrelated to credit; because this information does not relate to the individual's creditworthiness.
17.1C	Not previously present in the Code	<p>Explain to the individual that they may request a ban period with other CRBs, and that the individual can consent to the CRB (the first CRB) notifying the CRBs nominated by the individual (the notified CRBs) that the individual has requested that the notified CRB/s not use or disclose the individual's credit reporting information (additional ban period request). Where this additional ban period request is made by the individual:</p> <ol style="list-style-type: none"> (i) the first CRB must, as soon as reasonably practicable, provide the notified CRB/s with the ban period request provided by the individual to the first CRB; (ii) The notified CRB must treat the additional ban period request provided by the first CRB as if it had been provided by the individual directly to the notified CRB.
19.4C	No previous section was in the code, the section that was previously 19.4C is now 19.4D	The CRB may only provide the access seeker with a direct marketing communication where the access seeker has provided his or her consent to receipt of this communication by opting in to providing this consent. A pre-ticked consent box does not constitute opting in;



NEW SOUTH WALES
NORTHERN TERRITORY
QUEENSLAND
SOUTH AUSTRALIA
TASMANIA
VICTORIA
WESTERN AUSTRALIA

This publication has been carefully prepared, but it has been written in general terms and should be seen as a broad guidance only. The publication cannot be relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact the BDO member firms in Australia to discuss these matters in the context of your particular circumstances. BDO Australia Ltd and each BDO member firm in Australia, their partners and/or directors, employees and agents do not accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

BDO Services Pty Ltd ABN 45 134 242 434 is a member of a national association of independent entities which are all members of BDO Australia Ltd ABN 77 050 110 275, an Australian company limited by guarantee. BDO Services Pty Ltd and BDO Australia Ltd are members of BDO International Ltd, a UK company limited by guarantee, and form part of the international BDO network of independent member firms. Liability limited by a scheme approved under Professional Standards Legislation.

BDO is the brand name for the BDO network and for each of the BDO member firms.

© 2021 BDO Services Pty Ltd. All rights reserved.

1300 138 991

www.bdo.com.au

