

Report setting out findings of a review conducted pursuant to clause 24.2 of the *Privacy (Credit Reporting) Code 2014*



6 April 2021

Release date	
To	Experian Australia Credit Services Pty Ltd
From	Piper Alderman
Object	The review will be limited to assessing Experian's compliance with CRB-specific obligations of the <i>Privacy Act</i> and CR Code. It will not assess Experian's compliance with general privacy obligations in relation to personal information that is not credit reporting information, CP derived information or pre-screening assessments.
Report author	Andrea Beatty Partner Piper Alderman t: +61 2 9253 3818 m: +61 405 592 257 e: <a href="mailto:abeatty@piperalderman.com.au">abeatty@piperalderman.com.au</a> w: <a href="http://www.piperalderman.com.au">www.piperalderman.com.au</a> w: <a href="http://www.andreabeatty.com.au">www.andreabeatty.com.au</a>

## Table of contents

<b>Glossary</b>	<b>3</b>
<b>Executive Summary</b>	<b>5</b>
1. Introduction	5
2. Background and report objectives	5
3. Conclusion	6
<b>Detailed observations</b>	<b>7</b>
1. Management of credit reporting information policy	7
2. Collection of credit information	8
3. Use and disclosure of credit reporting information	9
4. Quality of credit reporting information	11
5. Access to credit reporting information	14
6. Corrections	15
7. Security	16
8. Complaints	18
9. Information retention and destruction	19
10. Qualifications and assumptions	20
<b>Attachment 1: Documents reviewed</b>	<b>22</b>
<b>Attachment 2: Meetings</b>	<b>25</b>
<b>Attachment 3: Experian Credit Reporting Policy</b>	<b>26</b>

### **Disclaimer**

This report is intended solely for the information of the Office of the Australian Information Commissioner. Neither Piper Alderman nor Experian Australia Credit Services Pty Ltd accept any responsibility to any other person who accesses this report.

The facts asserted in this report and on which we base our findings are derived wholly from the documents identified in Attachment 1 and the responses provided in interviews and meetings with the persons identified in Attachment 2.

This report concerns compliance only with Part IIIA of the *Privacy Act 1988* and the *Privacy (Credit Reporting) Code 2014*. We have not examined and offer no opinion about any other obligations under the Privacy Act that may or may not be applicable to Experian Australia Credit Services Pty Ltd.

Terms used in this report that are defined in the Glossary have the meaning given in the Glossary.

This report is dated as at 6 April 2021.

## Glossary

Term	Definition
<b>AFCA</b>	Australian Financial Complaints Authority
<b>Australian Privacy Principles</b>	has the meaning given in section 14 of the Privacy Act.
<b>Bureau Database</b>	The NextGen information system in which Experian holds credit reporting information for the purpose of providing services to Clients.
<b>Bureau Member</b>	A customer of Experian that supplies credit information to Experian and/or to whom Experian discloses credit reporting information.
<b>Client</b>	A Bureau Member to which Experian discloses credit reporting information.
<b>CR Code</b>	The <i>Privacy (Credit Reporting) Code 2014 (Version 2.1)</i> (Cth) as in force at the Date of this Report.
<b>Credit Reporting Policy</b>	The document titled “Experian Australia Credit Services Privacy Policy 2020”, dated April 2020 and published at <a href="https://www.experian.com.au/wp-content/uploads/2020/04/202004-Experian-Australia-Credit-Services-Privacy-Policy_WEB.1.pdf">https://www.experian.com.au/wp-content/uploads/2020/04/202004-Experian-Australia-Credit-Services-Privacy-Policy_WEB.1.pdf</a> .
<b>Data Supplier</b>	A Bureau Member who supplies credit information to Experian.
<b>Date of this Report</b>	6 April 2021
<b>Experian</b>	Experian Australia Credit Services Pty Ltd (ACN 150 305 838).
<b>HSA</b>	Heightened Security Area (see part 7.1)
<b>Information Commissioner</b>	The Information Commissioner within the meaning of the <i>Australian Information Commissioner Act 2010</i> (Cth)
<b>Part IIIA Obligations</b>	Obligations contained in Part IIIA of the Privacy Act and the CR Code.
<b>Permitted CRB disclosure</b>	As defined in section 20F of the Privacy Act.
<b>Privacy Act</b>	<i>Privacy Act 1988</i> (Cth) as in force at the Date of this Report.
<b>Privacy Regulation</b>	The <i>Privacy Regulation 2013</i> (Cth), as in force at the date of this report.

<b>Report</b>	This “Experian Australia Credit Services Pty Ltd Report detailing the findings of a review conducted pursuant to clause 24.2 of the <i>Privacy (Credit Reporting) Code 2014</i> ”, dated 16 June 2017
---------------	---

## Executive Summary

### 1. Introduction

Experian is part of a group of companies whose ultimate holding company is Experian Plc, a company incorporated in the United Kingdom and listed on the London Stock Exchange. The Experian corporate group carries on a global information services business, providing data, analytics, marketing and credit services and related software to businesses and consumers.

Experian is a credit reporting body as defined under the Privacy Act and accordingly collects, uses and discloses personal information in the conduct of its credit reporting business. As a result, the information that Experian collects, uses and discloses is regulated by the Part IIIA Obligations. This report considers those obligations and not the Australian Privacy Principles.

This report relates only to Experian and not to any other entity, whether or not a related body corporate of Experian.

### 2. Background and report objectives

This report contains the findings of our independent review of Experian's operations and processes pursuant to clause 24.2 of the CR Code.

The objective of this review is to express an opinion regarding Experian's compliance with the credit reporting obligations in Part IIIA of the Privacy Act, the *Privacy Regulation 2013* (Cth) and the CR Code. This review does not encompass Experian's compliance with the Australian Privacy Principles or any other statute applicable to Experian and we offer no opinion in respect of such matters.

Our review involved performing procedures to obtain evidence regarding Experian's compliance with its Part IIIA Obligations. Procedures performed include:

- (a) reviewing policy and process documents;
- (b) interviews with key Experian personnel;
- (c) reviewing samples of de-identified credit reporting information held by Experian; and
- (d) reviewing regulatory logs maintained by Experian.

Where necessary or appropriate, our review involved analysing samples of documents created by Experian on the applicable topic. We consider that the evidence we have obtained is sufficient and appropriate to assess whether Experian complies with its Part IIIA Obligations.

In particular, our review involved the following procedures to assess Experian's compliance with the Part IIIA Obligations:

- (a) desk reviews at Experian's Sydney office of documents (policies and processes, standard forms and agreements);
- (b) interviews with selected Experian personnel;

- (c) analysis of regulatory breach logs, as relevant; and
- (d) analysis of a sample of default listings provided.

We examined Experian's operations and processes (as disclosed in the documents we examined and discussions we conducted with key Experian personnel) and assessed them against checklists for obligations under Part IIIA of the Privacy Act and related obligations under the CR Code.

Due to the commercial sensitivity of the documents and Experian's information security policies, most documents that we examined were supplied to us by Experian for our review at Experian's Sydney office premises and we were not able to take copies of the documents. We have not retained copies of the documents that we reviewed.

### **3. Conclusion**

On the evidence that we reviewed and for the reasons that follow, and subject to our qualifications in this report, we find that that Experian complies with its Part IIIA Obligations.

## Detailed observations

### 1. Management of credit reporting information policy

Section 20B(3) of the Privacy Act requires Experian to have a clearly expressed and up-to-date policy about how it manages credit reporting information, addressing the matters listed in section 20B(4).

Experian has a Credit Reporting Policy which addresses the following matters:

- (a) the kinds of credit information held by Experian and how it is collected;
- (b) the kinds of credit reporting information held by Experian and the manner in which Experian holds such information;
- (c) the kinds of information that Experian derives from credit information that it holds;
- (d) the purposes for which Experian collects, holds, uses and discloses credit reporting information;
- (e) that individuals can request that Experian not use their credit reporting information for pre-screening direct marketing;
- (f) how individuals who reasonably believe that they are (or are likely to be) a victim of fraud can request a ban period be applied to their credit reporting information;
- (g) how individuals can access credit reporting information that Experian holds about them;
- (h) the measures that Experian takes to ensure that credit reporting information held about individuals is accurate and up-to-date;
- (i) how individuals may request correction of their credit reporting information;
- (j) how individuals may make complaints to Experian;
- (k) contact details for the Information Commissioner and the Australian Financial Complaints Authority (**AFCA**) and an explanation that if the individual is dissatisfied with Experian's handling of a complaint, they may refer the matter to those bodies, and
- (l) methods by which an individual can contact Experian.

Experian's Credit Reporting Policy contains all of the information required by section 20B(4) of the Privacy Act. It is clearly expressed and contains plain English explanations of Experian's practices and individuals' rights under the Privacy Act.

Section 20B(5) of the Privacy Act requires Experian to take such steps as are reasonable in the circumstances to make its Credit Reporting Policy available free of charge and in an appropriate form. Clause 3.1 of the CR Code requires Experian to publish its Credit Reporting Policy on its website. Experian complies with both of

these obligations by publishing its Credit Reporting Policy on a freely accessible section of its website in PDF format.

## 2. Collection of credit information

In the course of our audit, we were instructed by Experian that Experian collects credit information from the following sources:

- (a) Data Suppliers;
- (b) State and Territory courts; and
- (c) Australian Financial Security Authority (**AFSA**).

Bureau Members are entities with which Experian has an agreement to receive credit information. Experian conducts due diligence on prospective Bureau Members, part of which involves verifying that the applicant:

- (a) is in fact a credit provider as defined in sections 6G-6K of the Privacy Act;
- (b) has an Australian link (verified by Australian Company Number and Australian Business Number searches); and
- (c) is a member of the AFCA dispute resolution scheme.

As an additional measure, Experian also verifies that the address of a prospective Bureau Member has a commercial premises and is not just a residential address. These aspects of the due diligence process ensure that Experian only collects credit information from persons who are permitted under section 21D to disclose such information to credit reporting bodies. On the basis of these processes, we are of the view that Experian complies with section 20C(3) of the Privacy Act.

Experian's due diligence procedures also require it to verify that a prospective Bureau Member is appropriately licensed or authorised to engage in credit activities, or is exempt from the requirement to hold an Australian credit licence. This requirement is applied to all prospective Bureau Members, regardless of the type of data they will be supplying to Experian and exceeds the requirements of section 21D of the Privacy Act.

Experian's data validation rules include requirements to reject records for which the borrower's date of birth is less than 18 years prior to the relevant date for the information item (i.e. account opening date for consumer credit liability information, payment date for repayment history information or reporting date for default information). This requirement ensures that credit reporting information relating to acts, omissions, matters or things occurring before an individual turned 18 is filtered out and not collected in the Bureau Database, thereby ensuring that Experian complies with clause 5.4(a) of the CR Code.

As a further measure to ensure that Experian only collects credit information that it is entitled to collect, Experian's agreements with Bureau Members contain terms requiring the Bureau Member to only supply information to Experian that the Bureau Member is authorised under the Privacy Act to disclose to Experian.



Experian further reviews the privacy policies of prospective Bureau Members to ensure that they provide the relevant information and contact details for internal and external dispute resolution and the Information Commissioner.

Experian therefore complies with the obligation in section 20C(3) of the Privacy Act to collect credit information only from credit providers who are themselves authorised under section 21D to provide credit information to Experian.

In our review, we did not find any evidence of Experian receiving unsolicited credit information. As credit information is given to Experian via a secure transfer service maintained by Experian and is processed by Experian prior to loading into the Bureau Database, there does not appear to be any practical means by which unsolicited credit information can be given to Experian.

Our review found no evidence of Experian collecting records containing only identification information about an individual, without the record also containing credit information of another kind about the individual (see section 20C(4)(d) of the Privacy Act).

### **3. Use and disclosure of credit reporting information**

#### **3.1 Use of credit reporting information**

Experian uses credit reporting information for the purposes of:

- (a) compiling credit reports in respect of individuals;
- (b) computing credit scores in respect of individuals; and
- (c) carrying out procedures to test system integrity.

These activities constitute use of such information in the course of carrying on its credit reporting business and are therefore permitted under section 20E(2)(a) of the Privacy Act.

#### **3.2 Disclosure of credit reporting information**

Experian discloses credit reporting information to Client Bureau Members (some of whom may also be Data Suppliers). Client Bureau Members are subject to the same onboarding process as Data Supplier Bureau Members, part of which involves verifying that they are a credit provider as defined in the Privacy Act and that they have an Australian link.

When requesting credit reporting information from Experian, a Bureau Member must specify the reason for which they are requesting the information (by way of system codes that correspond to permitted CRB disclosures in section 20F of the Privacy Act) and other particulars such as the type of credit for which the applicant is applying, the account type and amount of credit specified in the application. Experian's Master Services Agreements with Bureau Members also require Bureau Members to use credit reporting information supplied by Experian only in ways permitted by law.

All activities on Experian's information systems, including requests for and disclosures of information, are electronically recorded and those records are saved

permanently for future reference. Since the footprint information is readily retrievable (by appropriately authorised Experian personnel) in future if the need arises, the *Electronic Transactions Act 1999* (Cth) operates to qualify it as a written note of the disclosure for the purposes of section 20E(5) of the Privacy Act.

If requests for information are made by the Information Commissioner or a law enforcement body, Experian's policies provide that the request is escalated to the Head of Compliance (Australia and New Zealand) to assess and determine Experian's response.

Both Experian's policies and personnel interviewed do not address the disclosure of credit reporting information to other credit reporting bodies outside the facilitation of Client data corrections through the Corrections Exchange product included in the Bureau Database.

Discussions with relevant Experian personnel indicated that Experian's policies and procedures in relation to the use and disclosure of credit reporting information were being complied with, and our review of the procedures did not find any evidence to suggest otherwise. The policies and procedures we reviewed were compliant with the Privacy Act. We therefore consider that in using and disclosing credit reporting information, Experian complies with its obligations under section 20E of the Privacy Act.

### **3.3 Direct marketing and pre-screening**

Experian personnel advised that Experian does not use credit reporting information for the purpose of direct marketing or pre-screening individuals' eligibility to receive direct marketing communications from a credit provider.

### **3.4 Ban periods**

Experian enables consumers to request a ban period by ordering a copy of their credit report and including a ban period request with their order. Experian does, however, require ban period requests to be made in writing and to explicitly state that the individual is requesting a ban period. We were advised that Experian includes this requirement to ensure that the consumer is aware that they are requesting a ban period.

A ban period is noted on the individual's credit report. Experian's data validation rules automatically apply a default ban period of 21 days. The ban period is confirmed with the consumer by email. The consumer may request a copy of their credit report, at no cost to them, to confirm that it includes a notation reflecting the ban period. Experian facilitates the extension of ban periods in consultation with the relevant individual as required by the Privacy Act.

Our review procedures found no evidence that Experian uses or discloses, whether deliberately or inadvertently, information that is the subject of a ban period request. In accordance with clause 17.3 of the CR Code, Experian writes to an individual at least 5 days before the expiry of the ban period to remind them of their ability to extend the ban beyond its scheduled finish. Experian does not limit the number of times that an individual can have their ban period extended.

Experian does not charge individuals for requesting a ban period or extending their ban period.

### **3.5 Government-related identifiers**

Experian does not use government issued identifiers as its own identifier of an individual. Experian generates its own unique identifier for each individual credit report.

### **3.6 De-identified credit reporting information**

We were instructed by Experian that it no longer holds or uses de-identified credit reporting information for research or testing purposes, therefore, section 20M of the Privacy Act does not apply to Experian's activities.

## **4. Quality of credit reporting information**

In conducting our review, we found that Experian has robust measures to ensure that the data that it collects from Data Suppliers, and the data that it holds, uses and discloses to Clients, is accurate and of sufficient quality to satisfy its obligations under the Privacy Act. These measures assist Experian to comply with its obligations under section 20N of the Privacy Act to take reasonable steps to ensure that the credit information that it collects is accurate, up-to-date and complete and that credit reporting information that it uses or discloses is accurate, up-to-date, complete and relevant.

Experian's Master Services Agreement has a general requirement for Bureau Members to ensure that any personal information satisfies the requirements of the Privacy Act, is accurate and is amended, updated, corrected or supplemented as required. The Agreement does not specifically require that records provided are complete. We recommend that this Agreement be amended to specifically require its Bureau Members to ensure records are accurate, up-to-date, complete and relevant.

### **4.1 Collection**

Experian relies on Data Suppliers (and suppliers of public records such as AFSA and the courts) to supply complete, accurate and up-to-date data. It has in place processes to assess the quality of credit information supplied by Data Suppliers and to filter out data that does not meet Experian's requirements, prior to the data being loaded into the Bureau Database and becoming available for use and disclosure.

The process by which Experian collects credit information from a Data Supplier can be summarised as follows:

- (a) the Data Supplier loads a file containing records of credit information via a secure file transfer service maintained by Experian;
- (b) the file is converted to the format required by Experian;
- (c) the file is assessed against Experian's data validation rules (see below); and
- (d) once validated, the data is loaded into the Bureau Database.

In conducting our review, we reviewed Experian's internal policy document setting out its data validation rules. That document contains a number of rules that are applied to the data automatically by software, including format checks for certain

coded fields, logical checks and cross-field validation where multiple fields are related. The rules concern:

- (a) the logical possibility of data (for example, preventing default information wrongly assigned to a future date);
- (b) internal consistency of data (for example, the account closure date cannot be earlier than the account opening date of a record) and Privacy Act; and
- (c) CR Code limitations on certain credit information (for example, the date on which a payment was due must be at least 60 days before the date that the information was reported, or the act/omission must not have occurred when the individual was under 18).

Records that do not pass the rules are rejected. We were advised by Experian personnel that rejection rates in excess of 5% result in rejection of the entire file and the issue is raised with the Data Supplier.

Incoming data is assessed against Experian's data validation rules. It is rejected if it is logically inconsistent or if Experian is prevented by the Privacy Act from collecting it (e.g. information relating to defaults that occurred over five years ago). Experian's file handling process also compares each data load against past data loads by the same Bureau Member, both in respect of the data itself and in respect of characteristics of the data (e.g. number of records submitted, frequency of file submission by a Bureau Member) and variances in excess of 5% are investigated.

Whilst an issue with a data load is being investigated, the entire data load is not loaded onto Experian's live credit bureau environment until the issue is resolved.

We found that Experian's data validation rules correctly reflect relevant Privacy Act provisions applying to credit information – in particular, the definitions of the various categories of credit information and retention periods – and are effective to ensure that credit information collected by Experian is accurate, up-to-date and complete. We consider that, overall, Experian's process in collecting credit information from Data Suppliers causes it to comply with its obligation under section 20N(1) to ensure that the credit information that it collects is accurate, up-to-date and complete.

Experian's agreements with Data Suppliers require the Data Supplier to provide records of information that are accurate to the best of the Data Supplier's knowledge and to promptly correct or update information which it has previously provided to Experian. Under those agreements, Experian also has a right to require a Data Supplier to manually verify the accuracy of information that it has provided to Experian, and Experian personnel advised us that Experian exercises this right as part of its audit of a Data Supplier. We therefore consider that Experian complies with section 20N(3)(a) of the Privacy Act.

Experian's data collection process addresses data quality issues pre-emptively, before credit information is loaded into the Bureau Database, thereby reducing the need for later action against a Data Supplier for breach of its agreement with Experian (see section 20N(3)(c) of the Privacy Act).

However, where credit reporting information needs to be removed from the Bureau Database, Experian has processes and the technical ability to do so. The data in each file submitted by a Data Supplier is tagged with information about that file,

enabling it to be later identified in a search by a particular file, and extracted if necessary.

## **4.2 Audits of Bureau Members**

Experian's agreements with Bureau Members contain terms permitting Experian to audit a Bureau Member's compliance with the terms of the agreement, including the data quality and information security obligations in those agreements. Those terms expressly permit Experian to appoint an independent person to conduct the audit.

Experian takes a risk-based approach to conducting audits of Bureau Members. Every 6 months, Experian assesses each Bureau Member against a proprietary internal risk scorecard, which considers factors that are relevant to the risk that the credit information supplied by a particular Bureau Member is inaccurate, incomplete or not up-to-date and the risk of misuse, interference or loss or unauthorised access, use or disclosure of credit reporting information received from Experian. Bureau Members that exceed a threshold score are subject to an audit, which involves a questionnaire relating to the Bureau Member's systems and processes for collecting and supplying credit information to Experian, their data security arrangements and a review of a randomly selected sample of credit information that the Bureau Member has given to Experian.

The Bureau Member's responses to the questionnaire are considered by Experian, any shortcomings addressed with the Bureau Member and the data in the sample of records is manually verified with the Bureau Member. Each audit of a Bureau Member is overseen by an employee of the global Experian group outside the Experian credit reporting business, to provide for independence from both the Bureau Member and the Experian credit reporting business. We are instructed that in the past three years, Experian has conducted six audits of Bureau Members. In addition to its comprehensive onboarding process, Experian has in place a risk-based system to determine whether it conducts an audit of a Bureau Member. Based on this assessment, we consider that Experian's audit processes are sufficient to meet the requirements of sections 20N and 20Q of the Privacy Act.

We reviewed the scorecard, questionnaire, including Bureau Member responses and agreed next steps of one audit. We were advised by Experian personnel in meetings that audits typically uncover a failure to update data – for example, a failure to submit payment information in relation to previously submitted default information, or a failure to update consumer credit liability information if the credit account has subsequently been closed – rather than the intentional or negligent provision of incorrect "original" data. We were advised that no audit has, to date, uncovered intentional wrongdoing by a Bureau Member, and that Experian generally follows up a Bureau Member's implementation of the recommendations resulting from an audit.

We have therefore concluded that Experian complies with its obligations under section 20N(3)(b) and 20Q(2)(b) of the Privacy Act and the associated obligations in clause 23 of the CR Code.

## **4.3 Use or disclosure**

Experian has general baseline requirements which must be complied with by Bureau Members including a pre-screening and onboarding process. These steps ensure that Experian during pre-screening takes the appropriate data verification, Client risk assessment and sanction screening necessary. Experian also undertakes verification

and validation of data and evaluation of results prior to onboarding Clients. Existing Clients that renew their Bureau Member agreement with Experian undergo the same due diligence as new Clients.

Experian monitors data quality on an ongoing basis, with a monthly data quality report being prepared and the causes of data quality issues being investigated and rectified. Experian's agreements with Data Suppliers require each Data Supplier to provide records that are accurate, to the best of the Data Supplier's knowledge and to promptly update, amend, correct or supplement information previously provided to Experian if it is not correct. Experian's systems also provide for the 'back out' of information provided by a Data Supplier where the Data Supplier later informs Experian that the information is not accurate, up-to-date or complete. We consider that these measures comprise reasonable steps to ensure that the credit reporting information that Experian uses or discloses is accurate, up-to-date, complete and relevant.

## **5. Access to credit reporting information**

Section 20R(1) of the Privacy Act requires Experian to, on request by an individual, provide the individual with access to credit reporting information that it holds about them.

Our review confirmed that Experian complies with its obligations under section 20R of the Privacy Act and associated provisions of the CR Code in relation to giving individuals access to credit reporting information that Experian holds about that individual.

Experian offers a process by which individuals can receive a copy of their Credit Report, which is a record of all credit reporting information that Experian holds about them. Credit Reports are supplied free of charge to individuals. Experian's website contains a page entitled "Order your free Experian Credit Report", with a web form that individuals can complete to request a copy of their Credit Report and, as an alternative to the web form, there are also instructions for requesting a Credit Report by post. At the time of our review, Experian's website specified that postal requests are currently unavailable due to COVID-19 and directed individuals to request a credit report via the web form or by telephone. Once the web form is submitted, the individual receives an email requesting copies of identification documents totalling 100 points using the standard points scale (Experian therefore complies with clause 19.1 of the CR Code). Once the identification documents are supplied by the individual seeking access, a copy of their Credit Report is provided by email to the individual within 10 business days of receipt of the identification documents. The Credit Report is provided in the same manner as the access request was received, by PDF attachment for web/email requests and by post for postal requests.

Experian personnel advised that access requests from agents acting on behalf of an individual for this purpose are accepted, subject to the agent providing evidence of written authorisation from the individual.

As a fee is not charged to individuals to receive a copy of their Credit Report, whether for the first occasion or any subsequent occasion, section 20R(6) of the Privacy Act and clause 19.3 of the CR Code do not apply.

In conducting our review, a member of the review team requested a copy of their Credit Report via web form, without disclosing that they were doing so for the

purposes of the review. The process experienced by the team member was as described above and they received a copy of their Credit Report within 5 business days of making the access request.

We found no evidence that other requests for Credit Reports were not granted within the 10 day period required by the Privacy Act.

Experian has not refused any requests for access to Credit Reports by the individuals concerned or their authorised access seeker.

## **6. Corrections**

### **6.1 Corrections when Experian is made aware of the inaccuracy by a Data Supplier**

Section 20S(1) of the Privacy Act provides that if a credit reporting body holds credit reporting information about an individual and is satisfied that, having regard to the purpose for which the information is held, the information is inaccurate, out-of-date, irrelevant or misleading, it must take such steps as are reasonable in the circumstances to correct the information to ensure that it is accurate, up-to-date, complete, relevant and not misleading.

As the success of Experian's credit reporting business depends on the accuracy of the data that it holds, uses and discloses, Experian investigates and acts on any suggestion that data which it holds may be incorrect, correcting data or facilitating the correction of data as soon as possible.

Experian's internal manuals include a procedure for Data Suppliers to request correction of information that they previously supplied to Experian. It involves Experian identifying the representative of the Data Supplier that is making the request via Experian's KYC procedure, making the correction requested by the Data Supplier and then recording this change on the credit report/s in question.

As an alternative to specific correction requests, Experian has a data 'back out' procedure by which an entire file of credit information provided by a Data Supplier can be removed from the Bureau Database in bulk if data quality issues are pervasive throughout a file. Information is tagged with the file from which it was supplied, enabling an entire file to be removed from the Bureau Database even if the file contains credit information regarding multiple individuals.

We consider these steps to be reasonable and found no evidence that they are not being followed in practice. We therefore consider that Experian complies with section 20S(1) of the Privacy Act.

Under section 20U of the Privacy Act, if Experian corrects the personal information of an individual under subsection 20T(2), Experian must, if the correction relates to information Experian has previously disclosed, give each recipient of the information written notice of the correction. If there is a correction of information in an individual's Credit Report, Experian has in place processes to notify the fact of the correction to each Bureau Member to whom Experian has disclosed credit reporting information about the individual within the 3 month period leading up to the correction. Experian therefore complies with section 20U of the Privacy Act (we consider that giving notice to past recipients from beyond 3 months before the correction date would be impracticable).

## **6.2 Corrections requested by individuals**

We consider that Experian complies with its obligations under section 20T of the Privacy Act to take the reasonable steps to correct personal information requested by an individual.

Experian has processes in place to correct credit information at the request of the individual to which such information relates. Experian requires correction requests to be submitted in writing, either by post (this channel is temporarily unavailable due to COVID-19) or using a form on Experian's website. In each case, the individual is required to include their credit report number in the request and particulars of the change requested, including providing evidence of why the information is currently not correct. If an individual does not have a copy of their credit report, they are directed to first request a copy of their credit report (which Experian provides free of charge).

Correction requests are entered into a "Corrections Exchange" to facilitate investigation of the complaint together with the relevant Data Supplier. Experian's policies provide for correction requests to be investigated and resolved within 30 days, consistent with section 20T(2) of the Privacy Act. If there is no resolution within 20 days, Experian's procedure requires it to contact the individual to request an extension of time.

Experian has confirmed to us that, at the date of this Report, its average resolution time for a complaint is within the 30 day service level provided for by its internal policies.

Following resolution of the correction request, Experian sends the individual a letter advising them either that the information has been corrected as requested or the reasons why their request was denied. The letter also informs the individual that they can complain to AFCA and the Information Commissioner and includes contact information for both, as required by section 20U of the Privacy Act.

Experian does not charge individuals in relation to correction requests in compliance with section 20T(5) of the Privacy Act.

Discussions with Experian personnel did not yield answers inconsistent with the policy set out in the Consumer Operations – Operations Manual, indicating that Experian effectively trains its staff in its procedures to comply with the applicable Part IIIA Obligations expressed in that manual and that the relevant personnel are complying with those policies.

## **7. Security**

### **7.1 Security of credit reporting information held by Experian**

We consider that Experian complies with its obligation under section 20Q(1) of the Privacy Act to take reasonable steps to protect credit reporting information that it holds from misuse, interference and loss and from unauthorised access, use or disclosure.

Experian has in place information security policies and practices to protect the security of the credit reporting information that it holds. The Bureau Database is quarantined from Experian's other information systems and protected by firewalls and



other hardware and software to prevent unauthorised access. Data Suppliers supply credit information via a secure transfer protocol and internal access is only via specific devices. Experian advises that these technical measures comply with industry best practice and unauthorised attempts to access Experian's information systems, including the Bureau Database, are continually monitored for and addressed. This monitoring protects the credit reporting information held electronically by Experian from external threats. Furthermore, Experian ensures that all faxes and incoming mail are scanned to the secure drive, with any copies of faxes and mail not being permitted to leave the mail room.

Within the organisation, Experian maintains a Heightened Security Area (**HSA**), which is a physically separate part of Experian's premises to which access is highly restricted. The Bureau Database is only accessible from within the HSA. Access to the HSA is limited to those staff who require access to perform their role and/or to supervise staff, with each person's application for access being personally approved by the General Manager – Credit Services and the Head of Compliance. Each person's physical access to the HSA is by way of electronic keycard, with each entry and exit being logged. Keycard access is configured to prevent tailing another person into or out of the HSA, with a person being unable to tap out of the HSA if they have not previously tapped in (and vice versa, if they have not tapped out following a prior entry). Persons entering the HSA are forbidden from taking bags or personal electronic devices into the HSA. HSA access is audited monthly, with persons no longer requiring HSA access having their access revoked. Within the HSA, there is a secure room to which access is limited only to those persons whose roles require them to deal directly with Credit Reports, adding a further layer of security to credit reporting information held by Experian. This sub-area is monitored continuously (24 hours, 7 days a week) by closed circuit television surveillance. Experian's HSA policies make provision for visitor access to the HSA has, with approval similarly required from both the General Manager – Credit Services and the Head of Compliance. Experian personnel advised us that visitors are met with outside the HSA wherever possible and that visitors to the HSA are accompanied by an Experian employee at all times.

Experian's Bureau Database is isolated from Experian's other information systems and all Experian assets are protected by firewalls and other hardware and software measures from unauthorised access. Experian ensures that its technical measures are to the industry best practice standard and attempted intrusions into the system are continually monitored. This protects the credit reporting information held electronically by Experian from external threats.

Credit reporting information received or held in hard-copy form does not leave a secure mail and printing room. The only exception is when credit reports are posted to the individuals whom they are about in response to an access or correction request by that applicable individual. Incoming mail does not leave the secure mail room; rather, it is scanned to the dedicated file server and sent to the relevant person by secure internal email, and then destroyed by being securely shredded.

Within the organisation, the Bureau Operations Team is physically separated from other Experian group activities by being located in the HSA – a physical room to which access is highly restricted. Access to the HSA is limited to those staff with a direct need to enter it to perform their role, and to supervisory staff. Visitor access can only be approved by the appointed HSA Manager, and all visitors must be accompanied by an Experian employee in the HSA at all times.

These measures ensure that the possibility of unauthorised access, modification or disclosure by persons within Experian is minimised.

## **7.2 Security of credit reporting information disclosed to Bureau Members**

Section 20Q(2) of the Privacy Act requires a credit reporting body to enter into agreements with credit providers, requiring them to protect credit reporting information disclosed to them from misuse, interference and loss, and unauthorised access, modification or disclosure.

Experian's Master Services Agreement with each Client imposes an obligation on the Client Bureau Member to keep information, including credit reporting information, disclosed by Experian to the Client strictly confidential. The Master Services Agreement also prohibits the disclosure of such information by the Client to any person except to the extent necessary for the performance of obligations under the agreement. It also requires the Client to take all reasonable steps to prevent unauthorised access to information supplied by Experian, including to, at a minimum, comply with any information security requirements advised or directed by Experian from time to time.

Experian's agreements with Clients contain terms requiring the Client to:

- (a) comply with all data protection obligations imposed on it by law, including those under the Privacy Act;
- (b) protect information received from Experian against misuse, interference and loss and from unauthorised access, use or disclosure; and
- (c) comply with any reasonable instructions and guidelines set by Experian in relation to information security.

These agreements also contain rights for Experian and Experian's Bureau Members to conduct audits, described in part 4.2 of this report, which involve detailed consideration of the Bureau Member's information security arrangements.

We therefore consider that Experian complies with section 20Q(2) of the Privacy Act.

## **8. Complaints**

Experian has complaints handling and complaints management procedures in place applicable to all Experian Asia-Pacific employees and third parties who receive or manage consumer communications that are complaints.

Section 23A(1) of the Privacy Act provides individuals with a right to complain to a credit reporting body about an act or practice that may be a breach of the Part IIIA Obligations. Experian enables individuals to make complaints, but defines complaints much more broadly to include any expression of dissatisfaction by a consumer with an Experian product, service, channel, policy or employee (but not including disputes regarding the correctness of information in a credit report or legal issues with separate resolution), whether or not it relates to an alleged breach of the Part IIIA Obligations. Experian uses Salesforce customer relationship management software to manage complaints.

Experian's complaints process provides for an initial letter to be sent to the complainant within 7 days of receipt of the complaint, acknowledging receipt of the complaint, and setting out how the complaint will be dealt with and advising that it is in the process of being resolved. Experian's standard form letters for this purpose, which we reviewed, contained information regarding how the complainant can complain to AFCA or the Information Commissioner and contact details for both.

If an individual makes a complaint under section 23A of the Privacy Act, Experian must within seven days after the complaint is made, give the individual a written notice that acknowledges the making of the complaint and sets out how Experian will deal with the complaint. Experian does, in practice, provide written acknowledgement to the client within the seven day period, as required by its Australia Complaints Policy.

Experian's complaints policy provides for complaints to be resolved within 45 days or any shorter period required by law. Experian advised that its complaints policy is a group policy covering non-credit reporting bodies in the corporate group, and that for Experian's credit reporting business the resolution deadline is 21 days, unless a longer period is agreed with the complainant. Experian's dispute resolution letter given to a complainant to advise them of the outcome of the complaint (for which we reviewed a template) also contains information regarding how the complainant can complain to the AFCA or the Information Commissioner and contact details for both.

Once a complaint is investigated, Experian notifies the complainant of its decision in writing, and of the fact that if the complainant is dissatisfied with Experian's decision then they can complain to AFCA or to the Information Commissioner.

Experian is a member of the AFCA dispute resolution scheme.

These policies appear to comply with section 23B and 23C of the Privacy Act and clause 21 of the CR Code. We found no evidence that Experian does not comply with these policies in practice.

In the year ending 30 June 2020, the average time taken to resolve complaints was 34 days. This resolution period is outside the 30 day time limit set out in section 23B(5) of the Privacy Act, although the Privacy Act provides for extension of the period with the written agreement of the complainant if a complaint cannot be resolved within 30 days.

Experian received 221 complaints within the 12 months to March 2021, with 68 being via AFCA and the remaining 153 being via Experian's internal dispute resolution procedure.

Experian does not charge individuals any fee to make a complaint.

## **9. Information retention and destruction**

Sections 20W and 20X of the Privacy Act set out the retention periods for different kinds of credit information. Section 20V of the Privacy Act requires a credit reporting body to destroy or de-identify credit information (and any credit reporting body derived information derived from that credit information) within one month after its retention period ends.

Experian's credit reporting system purges negative data on a weekly basis and positive data on a fortnightly basis. It is programmed to automatically destroy credit information during the next purge after the end of the retention period for that item of credit information. We have examined Experian's data validation rules and can confirm that the rules for automatic deletion of data correspond to the retention periods stipulated in sections 20W and 20X of the Privacy Act. However, they contain exceptions for circumstances where Experian is required by law to retain credit information beyond its retention period. This is:

- (a) where it is subject to a pending correction request
- (b) where it is the subject of a dispute, and
- (c) where it is otherwise required to be retained by an Australian law or an order of a court or tribunal.

As data purges are conducted on a weekly or fortnightly basis, there is no prospect of data being retained beyond one month after the end of the retention period unless section 20V(3), (4), (6) or (7) of the Privacy Act applies.

We examined Experian's data validation rules and found that the rules for automatic deletion of data correspond to the retention period stipulated in sections 20W and 20X of the Privacy Act and correctly provide for the circumstances where Experian is required by the Privacy Act to retain the information beyond its retention period (i.e. where it is subject to a pending correction request, where it is the subject of a pending dispute or it is otherwise required to be retained by an Australian law or an order of a court or tribunal). Such retained information is retained outside the Bureau Database and therefore is not used by Experian or disclosed to any Client.

We examined a sample of default information records randomly extracted from the Bureau Database and observed that none of the records were more than five years old (i.e. from the date on which they were supplied to Experian by the relevant Data Supplier) at the date on which they were extracted.

## **10. Qualifications and assumptions**

The facts asserted in this report and on which we base our findings are derived wholly from the documents identified in Attachment 1 and the responses provided in interviews and meetings with the persons identified in Attachment 2.

This report concerns compliance only with Experian's Part IIIA Obligations. We have not examined and offer no opinion regarding any other obligations under the Privacy Act or other laws that may be applicable to Experian. In particular, we did not consider compliance with the Australian Privacy Principles to the extent that they overlap with Part IIIA Obligations.

Our report is designed to provide reasonable assurance that Experian complies with its Part IIIA Obligations. In carrying out our review, we observed samples of documents and processes, rather than the entire population, where we considered it more appropriate and practical to do so.

The review procedures identified in this report were carried out between 19 January 2021 and 4 March 2021.

To the extent that there was an overlap between the Australian Privacy Principles and Part IIIA Obligations, the application of the Australian Privacy Principles is outside the scope of this report and therefore was not considered (for example, the incidental collection of personal information that is not credit information from individuals requesting access to their credit report).

We have not independently verified statements of facts supplied to us by Experian, other than to the extent specifically stated in this report.

Terms used in this report that are defined in the Glossary have the same meaning as in the Glossary.

This report has been prepared for the sole purpose of enabling Experian to comply with clause 24.2 of the CR Code and is intended solely for the information of the Office of the Australian Information Commissioner. The content of the report is not to be taken as advice of any kind and should not be relied on as such. Neither Piper Alderman nor Experian accepts any responsibility to any other person who may act in reliance on the report.

**Piper Alderman**

6 April 2021

---

## Attachment 1: Documents reviewed

Documents reviewed by Piper Alderman in conducting the review the subject of this report

No.	Title	Description
1	Partial CCLI and CCR Monthly Process	Process diagram – how credit providers update information they have provided to Experian on a monthly basis.
2	Current DM network data flow	Process diagram – data flow process within information system.
3	Customer onboarding a new customer	Table/matrix – taking on a new customer (data supplier or CR information user).
4	Data Load Process	Process diagram – how data enters Experian's information system.
5	Data Quality Issues	Process diagram – resolving data quality issues.
6	Default load and update process	Process diagram – inputting and updating default information into system.
7	HSA access	Process diagram – internal access to data/systems.
8	Business back out	Process – for removing data from Experian's credit reporting environment.
9	Default listings log	Log – sample of 100 default listings.
10	Data validation rules	Policy – data validation rules for credit information received by Experian.
11	Sources and types of credit information (as defined in s 6N of the Privacy Act 1988 (Cth) that will be covered	Matrix of data suppliers and the type of data they supply to Experian.
12	Master Services Agreement for Credit Services	Agreement by which Client Bureau Members obtain credit reporting information from Experian.
13	CCR Toolkit	Client facing documentation – about various obligations.
14	Audit questionnaire	Questions asked by Experian of credit providers when auditing Bureau Members' compliance with the Privacy Act, CR Code and data sharing agreements with Experian.

No.	Title	Description
15	Data management policy	Policy – concerning data handling and access to systems.
16	Onboarding process	Client Onboarding Process – PIM's.
17	Client services operations manual v 0.6	Policy – overarching policy document for Client Services division (i.e. division that deals with data suppliers and information customers).
18	Appendix 2 ACB Due Diligence screening	Policy – procedures that must be followed when taking on a new data supplier or client.
19	Appendix 3 ACB Member Account management	Policy – dealing with Bureau Members.
20	Appendix 4 ACB KYC Process	Policy – identification procedure to be undertaken before granting an access request.
21	Online credit reporting process	Procedure – instructions how to process an access request received by email.
22	Correction policy	Policy – data correction policy.
23	Complaints handling policy	Policy – for handling complaints from consumers and bureau members.
24	Consumer operations – operations manual	Policy – covering all aspects of dealing with consumers.
25	Complaints register	Log – complaints received by Experian.
26	Regulatory breach log	Log – of regulatory breaches.
27	Client On-Boarding Workflow	Client On-Boarding Workflow.
28	Appendix 1 – APAC Due Diligence Pack	Due Diligence Process overview.
29	Appendix 5 – Consumer Complaints	Process Flow.
30	Appendix 3 – Ban Request	Process Flow.
31	Appendix 6 – Client Corrections	Process Flow.
32	Appendix 2 – Credit Report Request	Process Flow.
33	Letter – complaint response	Template for initial letter to be sent to a complainant.

No.	Title	Description
34	Letter – dispute resolution	Template for letter advising complainant of outcome.
35	Letter – correction request	Template for letter advising individual of outcome of correction request.

**Piper Alderman**

6 April 2021



---

## Attachment 2: Meetings

### Meetings between Piper Alderman and Experian personnel

Date	Experian personnel
19 January 2021	Tristan Taylor, Sefike Kirikkaya, Robbie Dyer
21 January 2021	Sefike Kirikkaya, Rebecca Barbour, Becs Sione
2 February 2021	Robbie Dyer, Rebecca Barbour
4 February 2021	Sefike Kirikkaya, Becs Sione
9 February 2021	Sefike Kirikkaya, Rebecca Barbour, Becs Sione, Robbie Dyer, Michelle Edgtton
9 February 2021	Sefike Kirikkaya, Meaghan Simpson
4 March 2021	Sefike Kirikkaya, Michelle Edgtton

### Information about relevant Experian personnel

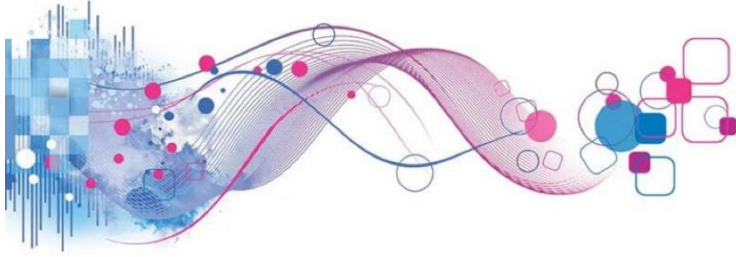
Name	Position
Rebecca Barbour	Manager, Bureau Client Relations
Robbie Dyer	Director of Operations
Michelle Edgtton	Team Leader, Consumer Operations
Sefike Kirikkaya	Head of Compliance, Australia and New Zealand
Meaghan Simpson	General Counsel
Becs Sione	Manager – Consumer and Client Services
Tristan Taylor	General Manager, Credit Services, Australia and New Zealand

### Piper Alderman

6 April 2021

---

## **Attachment 3: Experian Credit Reporting Policy**



# Experian Australia Credit Services Privacy Policy 2020

April 2020



## Our commitment

At Experian Australia Credit Services Pty Ltd and Compuscan Australia Pty Ltd (collectively referred to as Experian) we recognise the importance of your privacy and understand your concerns about the security of your Personal Information.

While information is the foundation for providing superior service, protecting your privacy and your Personal Information is of the highest importance to us. We believe that responsible stewardship of the information entrusted to us is crucial in developing and maintaining the public trust which in turn is essential for our continued success.

## Scope

Experian is a credit reporting body, bound by the Privacy Act 1988 (Cth) ("Privacy Act") and handles your Personal Information in accordance with law. As a result, the information Experian collects, uses and discloses is regulated under Part IIIA of the Privacy Act rather than the Australian Privacy Principles ("APPs"). You should be aware that other entities within the group of Experian companies may collect, use and disclose Personal Information in accordance with the APPs, which do not relate to credit reporting.

This privacy policy ("Policy") details how we will manage your Personal Information including:

- a) the kinds of credit reporting information that we hold, and how we hold that information;
- b) the purposes for which we collect, hold, use and disclose credit reporting information;
- c) how we use your information to contact or market to you directly (and your rights in respect of this);
- d) how you can access a copy of the credit reporting information we hold;
- e) how you can seek the correction of such information and your rights to correct;
- f) the kinds of personal information that we derived from credit information; and
- g) how you can complain if we don't meet our legal obligations and how we deal with such a complaint.

We may, from time to time, review and update this Policy, including taking account of new or amended laws, new technology and/or changes to our operations and practices. All Personal Information held by us will be governed by the most recently updated Policy. Accordingly, please regularly review our Policy so that you are aware of these updates and changes. If you have any questions, please contact us at:

**Attn: Privacy Manager**  
Experian Group Companies  
PO Box 1969  
North Sydney NSW 2060  
[experian.com.au/credit-services](http://experian.com.au/credit-services)  
[compuscan.com.au](http://compuscan.com.au)

## What kinds of Personal Information do we collect?

The kinds of Personal Information we may collect and hold from you or about you includes:

- a) Identification information (for example; name, surname, address and date of birth);
- b) Consumer credit liability information (for example; the name of the credit provider that granted you credit, the type of credit you have entered into, the terms or conditions of the credit agreement);
- c) Repayment history information (for example; whether you have met your obligation to make a payment, the day on which your payment is due and payable);
- d) Consumer credit defaults (an adverse record detailing that you have stop paying your account for more than 60 days and the overdue amount is more than \$150);
- e) Information requests (for example; the name of the credit provider that accessed your credit report, the reason for the enquiry);
- f) Court Records relating to court findings associated with financial obligations not being met (for example; sequestrations, liquidations, bankruptcies and non- payment of debt).

Other information we may collect and hold include:

- details of your financial and credit dealings with companies such as telecommunications providers and utilities;
- driver licence details.

Experian does not collect sensitive information such as:

- a) racial or ethnic origin;
- b) political opinions;
- c) membership of a political association;
- d) religious beliefs or affiliations;
- e) philosophical beliefs;
- f) membership of a professional or trade association;
- g) membership of a trade union;
- h) sexual orientation or practices;
- i) criminal record.

## How do we collect that information?

We may obtain information about you from public and private sectors.

We may collect information about you in the course of running a credit reporting business from:

- credit providers with whom you may have a relationship;
- mortgage or trade insurers;
- debt collection agencies;
- state and territory courts;
- Government agencies such as Australian Financial Security Authority, or Australian Securities Investment Commission;

- any other parties who are authorised under the Privacy Act to share your Personal Information.

There may be circumstances when we collect or use additional details from you for the purposes of servicing your request, for example to correct your Personal Information on our database or to assist you when you notify us of potential fraud.

Experian collects your Personal Information to enable us:

- to provide our products and services to parties who are authorised under the Privacy Act to access your credit information, such as credit providers; to provide you with your credit report when you ask us to do so;
- to test the accuracy of the process by which your information is provided to us, updated and loaded into our systems and the credit bureau; and
- to conduct research into the use of bureau product and services.

## How do we hold your information?

Experian holds your Personal Information in an Australian high security data centre. The Experian data centre and systems are only accessible by authorised Experian employees who are specially trained in security and data handling policies and protocols to Experian business standards and the credit reporting obligations under the Privacy Act.

As a global leader, Experian recognises and acknowledges the importance of keeping the Personal Information and data that it holds, secure and protected from unauthorised access. We adhere to international and industry standards around data privacy and protection. Access to your Personal Information is only provided to those employees who need to have access in order to perform their role. Access is also provided to users and subscribers of the products and services we offer and any law enforcement agency with whom we are required by law to provide your Personal Information.

## How does my information become an Experian Credit Report?

Experian uses the credit reporting information it holds on you to prepare your Experian Credit Report.

Your Experian Credit Report may include:

- a) your Experian credit score – a numeric representation of your credit worthiness based on mathematical algorithms;
- b) your identification details including name (former name(s)) and address (former address(es));
- c) details of any defaults reported to us;
- d) comprehensive credit reporting information including details of late or missed payments reported to us;
- e) court judgment information; and
- f) the number of information requests or enquiries made on your credit reporting information by credit providers.

## Our use and disclosure of your Personal Information

Experian holds, uses and/or discloses your Personal Information only for those purposes which are permissible under the Part IIIA of the *Privacy Act 1988* (Cth). Generally, credit reporting information is disclosed in the form of an Experian Credit Report and/ or score in response to an information requests or enquiries from a credit provider and where you have given consent to the credit provider seeking a credit report.

Experian also holds, uses and discloses information for lawful purposes, which include:

- where you have provided consent to a party to use or access your credit reporting information generally for the purpose of providing services to you and assessing an application for consumer or commercial credit, mortgage or trade insurance, or where you are looking to provide a personal guarantee;
- for your credit provider to assist you with credit related products and services,
- where you have provided consent to a third party to access your information on your behalf,
- for investigative purposes;
- where we are required to do so under an Australian law or a court/tribunal order;
- where your Personal Information is de-identified and used for research and other purposes where permitted by law. This includes de-identified credit data for the purposes of conducting research in relation to credit.

We may also use your Personal Information to test the accuracy and efficacy of the system and data processes by which it is provided to us including for inclusion in Experian's credit bureau and in relation to our provision of products and services.

## Direct marketing

Under the Privacy Act there are limited circumstances in which your credit reporting information can be used for the purposes of direct marketing to you and Experian will only use or disclose your credit reporting information where permitted by law. Generally, we can only permit use or disclosure for direct marketing purposes by or to an Australian credit provider for the purposes of determining whether you may be eligible to receive communications from that credit provider about a particular consumer credit offer ("**pre-screening**").

You may by written request per the details below, request that we do not use your credit reporting information for the purposes of pre-screening direct marketing. You may need to establish your identity and/or your authority to make the request. Where you have made a request for us not to use your credit reporting information for pre-screening direct marketing, we will make a note on your file and will not use or disclose your credit information for the purposes of pre-screening direct marketing.

## What if I am the victim of fraud, or am likely to become, a victim of fraud?

The Privacy Act provides that where you are a victim of fraud or have reasonable grounds to believe that you are (or are likely to be) a victim of fraud, you may request that we do not use or disclose your credit reporting information for 21 days from when you make the request ("**Ban Period**"). If we receive a request from a credit

provider during the Ban Period, we will notify the credit provider making the request that your credit reporting information is subject to a ban at your request.

To make a ban request you may need to provide us with proof of your identity and details of the fraud or the likely fraud and establish the reasonable grounds you have for requesting the ban.

During the Ban Period you may:

- a) request us to provide your credit reporting information to a specified credit provider/s; and
- b) apply to extend the Ban Period.

During the Ban Period to ensure your Personal Information is not compromised, your information cannot be disclosed or used. The existence of a ban on your file may impact the approval process for an application for credit. Please alert the relevant parties, if you are, or are intending to apply for credit and a Ban Period is under way with us.

## Access to your credit reporting information

You are entitled to request access to review the credit reporting information we hold in respect of you. To request access, you should send us a request with the following details:

- a) information required to identify you;
- b) proof of your identity;
- c) if you have authorised a person to act on your behalf;
- d) identifying the person, you have authorised;
- e) a written statement signed by you authorising the identified person to receive the information on your behalf.

We may require you to provide further information to reasonably verify your identity and/or to identify your credit reporting information from our systems (including details such as previous names, addresses and identity details).

Once we are reasonably satisfied of your identity or your authorisation, we will notify you of your options for accessing your credit information file.

Requests for credit reports are fulfilled within 10 business days of you contacting us.

Experian will not charge you a fee to access a copy of your credit reporting information including where you have not made a request within the last 12 months, or you can provide evidence that in the past 90 days an application for credit has been declined due to your credit history, or where your request for access relates to a decision by a credit reporting body or a credit provider to correct information on your credit report.

## How we maintain the quality of your Personal Information

It is extremely important to us that the Personal Information we hold about you is up to date and accurate. We take such steps as are reasonable to ensure that credit reporting information we hold about you is accurate and



up to date. To do this we undertake steps to verify information provided to us for use as credit reporting information, including:

- a) giving weighting to the most recent source;
- b) smart algorithmic matching to identify common typographical errors;
- c) internal data hygiene review, de-duplication and processing;
- d) use of proven advanced data quality software and systems.

We are required under the Privacy Act to acquire credit reporting information on terms that require providers to ensure that credit information contributed is accurate and up to date and complete. We are also required and do ensure that there is regular independent auditing of those agreements for compliance.

Experian ensures that information which is required to be removed and/or destroyed from your credit history is carried out within the timeframes as specified in the Privacy Act. For information as to how long we can retain your credit history, please contact us or visit our website at [experian.com.au/credit-services](https://experian.com.au/credit-services) and or [compuscan.com.au](https://compuscan.com.au)

## Corrections

There may be times when you feel information we have provided about you may not be accurate or up to date. Should this be the case we ask that you contact us so that we can investigate the matter on your behalf.

If you believe that we hold information we hold about you may not be up to date, accurate or complete, you have the right under the Privacy act to apply to us for a correction of that information.

On receipt of this information we will investigate and use all reasonable endeavours to resolve the issue within 30 days from receipt of your correction request. We may require further information or details from you to complete our investigation into your request. Depending on the nature of the correction we may require further information from or the assistance of another party such as another credit reporting body or credit provider to investigate or resolve the correction request. Where Experian is not the original provider of the information, we will liaise with the relevant parties to investigate the accuracy of the information we hold.

We will advise you of the outcome. Where the investigation is complex we may seek your agreement to allow more time for the investigation and resolution. Where, following our investigation we determine that a correction is warranted, we will take all reasonable steps to correct our records and we will provide you with written details of the correction and a copy of your updated credit record.

If we do not update your information as a result of your request, we will provide detailed feedback as to the reasons why we could not process your request. If you are unsatisfied with the outcome of the investigation you can contact the Australian Financial Complaints Authority (AFCA):

	<a href="https://afca.org.au">afca.org.au</a>		Australian Financial Complaints Authority GPO Box 3 Melbourne VIC 3001
	<a href="mailto:info@afca.org.au">info@afca.org.au</a>		
	1800 931 678		

## Complaints

We take every effort to ensure that our information management practices comply the applicable law, however, if you feel that Compuscan have not complied with our obligations under the Privacy Act, you can contact us with the details of your complaint. We will acknowledge receipt of your complaint within 7 days, we will investigate your complaint and will seek to resolve your complaint within 30 days.

If your concern relates to the correction of information we hold about you, we would request that you seek a correction in accordance with the process described above before submitting a complaint.

If you are not satisfied with the outcome of our investigation, you may refer the matter to the Office of the Australian Information Commissioner or Australian Financial Complaints Authority (our external dispute resolution scheme) using the details below.

Contact details for both parties are as follows:

Office of the Australian Information Commissioner GPO Box 5218 Sydney NSW 2001	Australian Financial Complaints Authority GPO Box 3 Melbourne, VIC 3001
--	---

## Further information

This Policy Statement reflects general information on how we:

- a) comply with our obligations under the Privacy Act;
- b) collect, hold, use, disclose and manage your Personal Information; and
- c) provide credit reporting business services to our clients and to consumers.

This Policy Statement is not legal advice and is not intended to replace the rights, duties and obligations a party has under the Privacy Act. Nothing in this statement is intended to create or impose rights, remedies or obligations additional to those set out in the Privacy Act. All reasonable care has been taken by Experian to prepare and keep this statement up to date, however, the information contained in this policy is not intended to be a warranty or representation or otherwise to create any legal contractual relationship or obligations between you and Experian.