



Australian Government

Office of the Australian Information Commissioner

October 2016

# Submission on the Review of the financial system external dispute resolution framework – Issues Paper



## Introduction

I welcome the opportunity to comment on the *Review of the financial system external dispute resolution framework – Issues Paper* (the issues paper), which examines the role of Financial Ombudsman Service (FOS); the Credit and Investments Ombudsman (CIO); and the Superannuation Complaints Tribunal (the SCT), and considers whether changes to current dispute resolution and complaints schemes in the financial sector are necessary to deliver effective outcomes for users.<sup>1</sup>

As the national privacy regulator, the Office of the Information Commissioner (OAIC) plays an important role in the financial system's dispute resolution and complaint handling framework. This includes having regulatory oversight of the Australian Privacy Principles (APPs) in Schedule 1 of the *Privacy Act 1988* (Cth) (Privacy Act), which covers personal information handling by Australian Government agencies and many private sector and not-for-profit entities and Part IIIA of the Privacy Act, which covers information handling in Australia's consumer credit reporting system.

The Privacy Act applies to a significant number of participants in the finance sector, that handle a large volume of personal information (including credit information) which is accessed and updated frequently by multiple sources. Veda, for example, is Australia's largest credit reporting body and claims to hold credit information on around 20 million adult Australians and New Zealanders.<sup>2</sup> The OAIC's complaint statistics reflect the high level of privacy regulatory oversight of this sector. For example, statistics on the most complained about sectors in the *OAIC's Annual Report for the 2014 – 2015* ranks the Finance (including superannuation) sector second, and credit reporting bodies sector third, in the ten most commonly complained about sectors.<sup>3</sup>

External dispute resolution (EDR) schemes form part of the complaint handling framework in the Privacy Act. For example, all credit providers participating in the credit reporting system under Part IIIA of the Privacy Act must be a member of a recognised EDR scheme.<sup>4</sup> In addition, an individual who considers that an entity has interfered with their privacy may make a complaint to a recognised EDR scheme of which the entity is a member (if the complaint falls within the scope of the scheme's recognition), before making a complaint to the OAIC. Under the Privacy Act, the Australian Information Commissioner (the Commissioner) can recognise an EDR scheme for an entity or class of entities, or for a specified purpose.<sup>5</sup> Relevantly, FOS and the CIO are recognised EDR schemes under the Privacy Act.

The comments below provide further information about the Commissioner's functions and powers in relation to privacy regulation of the financial system, which may be of relevance to the panel's review of the financial system's EDR framework, and the role of FOS and the CIO in that framework.

## About the OAIC and the Privacy Act

The OAIC is an independent statutory agency within the Attorney-General's portfolio. The OAIC integrates three key functions:

---

<sup>1</sup> See <https://consult.treasury.gov.au/financial-system-division/dispute-resolution/>

<sup>2</sup> See p58 of Veda Advantage's 2015 [Annual Report](#)

<sup>3</sup> OAIC Annual Report 2014/15, Chapter 6 – Privacy Compliance, at [www.oaic.gov.au](http://www.oaic.gov.au)

<sup>4</sup> Section 21D(2)(a)(i) of the Privacy Act

<sup>5</sup> Section 35A(1) of the Privacy Act



- 
- privacy functions that include oversight of privacy protections in the Privacy Act
  - freedom of information functions, in particular oversight of the *Freedom of Information Act 1982 (Cth)*
  - government information policy functions conferred on the Australian Information Commissioner under the *Australian Information Commissioner Act 2010 (Cth)*.

The Privacy Act applies to Australian government agencies, organisations with an annual turnover of more than \$3 million, some small businesses and private sector health service providers (collectively called ‘APP entities’).<sup>6</sup> APP entities can include individuals (including sole traders), body corporates, partnerships, unincorporated associations and trusts. It contains 13 APPs that set out standards, rights and obligations for the handling, holding, accessing and correction of personal information.<sup>7</sup> Personal information is defined as information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.<sup>8</sup> Of particular relevance to this review is part IIIA of the Privacy Act, which contains requirements for the handling of credit-related personal information by credit reporting participants. Part IIIA is supported by the Privacy Regulation 2013 and the Privacy (Credit Reporting) Code 2014 (Version 1.2) (CR code).<sup>9</sup>

## Privacy regulation and the financial system

The Privacy Act provides the central framework for regulating the handling of personal information by APP entities, including Australian banks, financial institutions and other credit providers that handle a wide range of personal information in the course of carrying on their business. Consumer confidence, to a large degree, rests on responsible privacy practice in the financial sector. This is even more so in the age of online banking and digital services. The OAIC plays a pivotal role in assuring consumers that privacy protections will be enforced, and alleged misuse of personal information will be investigated. In addition, the OAIC engages with regulated entities to provide guidance, promote best practice compliance and identify and seek to address privacy concerns as they arise.

### Consumer credit reporting system

Part IIIA of the Privacy Act, the CR Code and the Privacy Regulation 2013 contain requirements for the handling of credit-related personal information by credit reporting participants. The requirements in Part IIIA are intended to facilitate an efficient consumer credit reporting system while ensuring that the privacy of individuals is respected. They balance individuals’ interests in protecting their personal information with the need to ensure that credit providers have sufficient information available to assist them to decide whether to provide an individual with credit. The requirements in Part IIIA also help ensure that credit providers are able to comply with their responsible lending obligations under the *National Consumer Credit Protection Act 2009* administered by the Australian Securities and Investment Commission.

---

<sup>6</sup> For more information about the entities that are covered by the Privacy Act, see <https://www.oaic.gov.au/privacy-law/rights-and-responsibilities>

<sup>7</sup> See Schedule 1 of the Privacy Act.

<sup>8</sup> See s 6(1) of the Privacy Act.

<sup>9</sup> The Privacy (Credit Reporting) Code 2014 (Version 1.2) (CR code) is available at <https://www.oaic.gov.au/privacy-law/privacy-registers/privacy-codes/privacy-credit-reporting-code-2014-version-1-2>



In particular, Part IIIA outlines:

- the types of personal information that credit providers can disclose to a credit reporting body, for the purpose of that information being included in an individual's credit report
- what entities can handle that information, and
- the purposes for which that information may be handled.<sup>10</sup>

For example, Part IIIA sets out when a credit provider can access a person's credit report from a credit reporting body. Most commonly, credit providers will seek access to a person's credit report when they have received a credit application, and are considering whether to grant credit to that person. For example, when a person applies for a personal or home loan, credit card, or new home or mobile telephone service account.

In contrast to the APPs, which apply to all APP entities, Part IIIA applies to credit providers and credit reporting bodies in relation to the exchange of 'credit information'.<sup>11</sup> 'Credit reporting bodies' are businesses which handle credit information for the purpose of providing information to other entities about individuals' creditworthiness.<sup>12</sup> As you will likely be aware, the three major credit reporting bodies currently operating in Australia are Veda, Dun & Bradstreet, and Experian.

The term 'credit provider' captures a wide range of entities that provide credit, issue credit cards, or otherwise provide goods or services on credit.<sup>13</sup> Goods or services are considered to have been provided on credit where payment is deferred for 7 days or more. The definition therefore covers banks, building societies, credit unions, payday lenders and other types of financial institutions/financial service providers, as well as utilities, telecommunication service providers, and toll road and public transport operators.

## Recognised external dispute resolution schemes

EDR schemes receive complaints about EDR member organisations from individuals, and provide independent dispute resolution services to resolve those complaints. The Privacy Act recognises that there may be benefits in individuals bringing their complaints to an EDR scheme that has experience in a particular industry. Importantly, as outlined above, a credit provider must be a member of an EDR scheme recognised under the Privacy Act to be able to participate in the credit reporting system.<sup>14</sup>

Under the Privacy Act, the Commissioner has discretion to recognise EDR schemes to handle privacy-related complaints – including complaints under the APPs and credit reporting provisions in the Privacy Act.<sup>15</sup> There are currently 10 recognised EDR schemes, including FOS and the CIO.<sup>16</sup> In considering whether to recognise an EDR scheme, the Commissioner must take into account the accessibility, independence, fairness, accountability, efficiency and effectiveness of the EDR scheme, and any other

---

<sup>10</sup> For more information about the credit reporting system, see privacy fact sheets 26 to 40 at <https://www.oaic.gov.au/individuals/privacy-fact-sheets/credit-reporting/>

<sup>11</sup> Credit information is defined in s 6N of the Privacy Act.

<sup>12</sup> Credit reporting body is defined in s 6(1) of the Privacy Act

<sup>13</sup> See ss 6G-6K of the Privacy Act.

<sup>14</sup> Section 21D(2)(a)(i) of the Privacy Act

<sup>15</sup> See s 35A of the Privacy Act.

<sup>16</sup> For more information about the schemes recognised under the Privacy Act, see <https://www.oaic.gov.au/privacy-law/privacy-registers/recognised-edr-schemes>



---

matter considered relevant.<sup>17</sup> These matters are based on the benchmarks developed in 1997 by the then Department of Industry, Science and Tourism for industry-based customer dispute resolution schemes.<sup>18</sup>

The OAIC has issued *Guidelines for recognising external dispute resolution schemes* (the EDR scheme guidelines)<sup>19</sup> which outline the matters the Commissioner will take into account in considering whether to recognise an EDR scheme, the steps an EDR scheme should take to apply for recognition and the general conditions for ongoing recognition. For example, the guidelines include more information about the benchmarks outlined above. They also make the recognition of EDR schemes subject to a scheme providing an independent review of the EDR scheme at least once every five years, and subject to meeting the OAIC's requirements for reporting serious or repeated interferences with privacy and systemic issues and data on privacy-related complaints.

Recognised EDR schemes play an important role in the process for privacy complaints handling. The process can generally be described as follows:

1. generally, an individual should complain to the respondent party and give them a chance to respond to the complaint
2. where not satisfied with the response or outcome, the individual may complain to a recognised EDR scheme of which the respondent is a member
3. if the individual is dissatisfied with the outcome of the EDR process, or would prefer to complain directly to the regulator, they may complain to the OAIC.

The inclusion of recognised EDR schemes in the privacy regulatory model is a relatively new development introduced as part of reforms to the Privacy Act that commenced on 12 March 2014. It was intended to increase efficiency in dispute resolution and to provide parties with a one stop shop for complaints that are partly about privacy and partly about service delivery.<sup>20</sup> Prior to its introduction, some concerns were raised that a greater role for EDR schemes could lead to more inconsistency in privacy complaint handling.<sup>21</sup> To address these concerns, the OAIC works collaboratively with EDR schemes to ensure consistency in the application of the Privacy Act. This collaboration includes regularly providing policy advice on request, and where appropriate sharing this advice with other schemes, regularly meeting with schemes to exchange information, holding biannual EDR-wide scheme meetings and offering free training sessions to schemes.

As noted above, the OAIC also systematically monitors complaint handling trends across EDR schemes. The EDR scheme guidelines state that it is a condition of recognition that each recognised EDR scheme must provide the OAIC with statistical information about the number of privacy complaints received, resolved, referred and finalised on an annual basis.<sup>22</sup> Additionally, serious or repeated interferences with privacy and systemic privacy issues must be reported to the OAIC when an EDR scheme has confirmed that such events have occurred. If EDR scheme members do not appropriately address

---

<sup>17</sup> Section 35A(2)(a) to (g).

<sup>18</sup> Department of Industry, Science and Tourism 1997, *Benchmarks for Industry-Based Customer Dispute Resolution Schemes*, Department of Industry, Science and Tourism, Canberra.

<sup>19</sup> Available on the OAIC's website at [Guidelines for recognising external dispute resolution schemes](#).

<sup>20</sup> Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, p. 1, available for download at: <https://www.legislation.gov.au/Details/C2012B00077/Download>

<sup>21</sup> ALRC 108, *For Your Information: Privacy Law and Practice*, paragraph 49.20

<sup>22</sup> For more information, see the OAIC's 2014-15 Annual Report at <https://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201415/>



serious or repeated interferences with privacy or systemic issues within a reasonable period of time, the Commissioner may investigate the act or practice of an entity on the Commissioner's own initiative under Part V of the Privacy Act.

## Final comments

There are strong indications that the community considers credit and other financial data to be some of the most sensitive of all data sets, and therefore in need of strong and appropriate privacy protections.<sup>23</sup> In the credit reporting context in particular, an individual's ability to access credit can have a significant impact on many aspects of their life, and it is therefore crucial that the information in the credit reporting system is both as accurate as possible, and handled appropriately.

The Privacy Act provides a suitably flexible yet robust framework for the handling of all personal information in the financial system. The Privacy Act is the privacy oversight instrument with which the public is most familiar, and in the view of my Office continues to reflect the Australian community's expectations about the appropriate level of protection that should be afforded to personal information in Australia today, including sensitive financial information which is considered to be in need of particular protection.

Additionally, essential to an effective regulatory regime is an independent regulator with powers to monitor and investigate non-compliance, and encourage best privacy practices. The OAIC has considerable expertise and experience in privacy regulation of the financial sector. The OAIC also has extensive experience in complaint conciliation, meaning it provides a method for fast, informal and low-cost resolution of disputes. The inclusion of recognised EDR schemes in the privacy regulatory model was intended to facilitate efficient dispute resolution processes in this area and the OAIC has been committed to working collaboratively with EDR schemes to ensure consistency in the application of the APPs and credit reporting provisions. Over the past two years since the commencement of the Privacy Act reforms, the OAIC has been monitoring this approach to determine whether any efficiencies have been achieved.

The issues paper considers different dispute resolution models, including merging the various EDR bodies or creating an additional forum for dispute resolution. If any changes are made to the number of EDR schemes or their functions, the OAIC would need to consider whether the new scheme(s) could still be recognised under the Privacy Act. That is, the new scheme would need to satisfy the benchmarks for recognition to handle privacy complaints and other requirements for recognition set out in the Privacy Act and the recognised EDR scheme guidelines.

Should the panel recommend structural changes to the financial system EDR framework, I am of the view that the OAIC is best placed to handle any privacy-related aspects of any dispute under the existing provisions in the Privacy Act. The OAIC (and formerly the Office of the Privacy Commissioner) has performed these functions for a long time – since the *Privacy Amendment Act 1990* added a new Part IIIA to the Privacy Act (to provide for regulation of the practices of credit reporting agencies and credit providers), and since extension of the Privacy Act to the private sector generally under the *Privacy Amendment (Privacy Sector) Act 2000*. The Privacy Act and the OAIC have high visibility in the Australian

---

<sup>23</sup> OAIC, *Community attitudes to privacy survey: research report 2013*, <http://www.oaic.gov.au/privacy/privacy-resources/privacy-reports/oaic-community-attitudes-to-privacy-survey-research-report-2013>

---

community and my office is regularly approached by the community about privacy concerns.<sup>24</sup> This experience, expertise and visibility foster consumer confidence that privacy rights will be defended – confidence that is an indispensable part of a healthy financial system.

I am also of the view that if the panel were to consider changes to the credit reporting provisions in Part IIIA of the Privacy Act, it would be preferable instead to await the five-year review of the credit reporting system, due to be conducted in 2019. We also note that the Commissioner is required to initiate an independent review of the CR Code within 3 years of its commencement, that is, in 2017.<sup>25</sup> Given that the amended credit reporting provisions have been in force for less than three years, and there is a planned review to be conducted in consultation with all relevant industry and consumer stakeholders at this time, I suggest that this would be a more appropriate forum in which to consider whether any further changes to the credit reporting system are desirable.

## Further consultation

Given the relevance of the OAIC's responsibilities to the scope of the issues paper, I would welcome the opportunity to engage with the panel in the development of any recommendations that may impact on the credit reporting system in Part IIIA of the Privacy Act or privacy regulation more generally.

---

<sup>24</sup> More information about the OAIC's activities, including enquiries and complaints statistics, can be found in the OAIC's Annual Reports available at <https://www.oaic.gov.au/about-us/corporate-information/annual-reports/all/>

<sup>25</sup> CR Code, paragraph 24.3