

# Chapter 2: Commissioner initiated investigations and referrals

## Contents

<b>Legislative framework</b>	<b>1</b>
<b>Referral of allegations to the OAIC</b>	<b>2</b>
<b>OAIC framework for considering referrals</b>	<b>3</b>
<b>Considerations in opening a CII</b>	<b>4</b>
<b>Procedural steps in conducting a CII</b>	<b>4</b>
1. Notification to respondent	4
2. Information gathering	4
3. Decision making	4
4. Conclusion and publication	5

## Legislative framework

- 2.1 Section 40 of the Privacy Act gives the Commissioner the power to conduct investigations.
- 2.2 Section 40(2) of the Privacy Act enables the Commissioner to commence an investigation on the Commissioner's own initiative, where:
- a. an act or practice may be an interference with the privacy of an individual or a breach of Australian Privacy Principle (APP) 1; and
  - b. the Commissioner thinks it is desirable to do so.
- 2.3 The Commissioner can also commence investigations into the privacy aspects of the CDR scheme. This is because s 56ET of the Competition and Consumer Act provides that s 40(2) of the Privacy Act extends to a possible breach of a privacy safeguard, or a privacy or confidentiality related CDR Rule, and a data breach made under Part IIIC of the Privacy Act relating to the CDR scheme.
- 2.4 Investigations conducted under s 40(2) are known as 'Commissioner initiated investigations' (CIIs).
- 2.5 Prior to commencing an investigation, the Commissioner may conduct preliminary inquiries under s 42(2) of the Privacy Act, to determine whether to commence a CII. Once a CII has been commenced, the OAIC will conduct its investigation in accordance with Part V of the Privacy Act.
- 2.6 Where the Commissioner has identified an interference with privacy, there are a number of enforcement powers available to the Commissioner.



- 2.7 The Commissioner endorses a focus on engagement, advice and support in preference to deterrence and punishment where appropriate.
- The Commissioner’s powers, ranging from less serious to more serious regulatory action, include the ability to:
    - conduct an assessment of an entity’s privacy practices (s 33C of the Privacy Act; s 56ER of the Competition and Consumer Act) and provide non-binding recommendations
    - accept an enforceable undertaking (s 80V of the Privacy Act; s 56EW of the Competition and Consumer Act)
    - make a determination (s 52 of the Privacy Act) directing an entity to take certain steps
    - bring proceedings to enforce an enforceable undertaking (s 80V of the Privacy Act; s 56EW of the Competition and Consumer Act)
    - bring proceedings to enforce a determination (ss 55A and 62 of the Privacy Act)
    - seek an injunction to prevent conduct that would constitute a contravention of the Privacy Act (s 80W of the Privacy Act), and against CDR participants to enforce the privacy safeguards (s 56EX of the Competition and Consumer Act)
    - apply to a court for a civil penalty order for a breach of a civil penalty provision (s 80U of the Privacy Act), and seek civil penalties for certain contraventions of the privacy safeguards (s 56EU of the Competition and Consumer Act), which includes serious or repeated interferences with privacy.
- 2.8 The Commissioner may, at any time, also decide to discontinue an investigation where the Commissioner is satisfied that no further regulatory action is warranted in the circumstances. This may occur where the Commissioner decides that the entity has not breached the Privacy Act or the requirements of the privacy safeguards and CDR Rules, or if the Commissioner considers there has been a breach that is immaterial or has been adequately dealt with.

## Referral of allegations to the OAIC

- 2.9 The OAIC becomes aware of matters that may warrant the commencement of a CII through a number of channels, including:
- a complaint by an individual, or a representative complaint (under the Privacy Act), or a CDR consumer (under the Competition and Consumer Act)
  - a referral from another regulator or external dispute resolution (EDR) scheme
  - media reports and social media commentary
  - a referral from a member of the community or information provided by an informant
  - information gathered in the course of other regulatory activity of the OAIC (for example, privacy assessments, data breach notifications, and engagement with the ACCC in relation to the CDR scheme).

## OAIC framework for considering referrals

- 2.10 The OAIC has a range of options available to respond to referrals, including no action, provision of general guidance or preliminary inquiries for the purpose of deciding whether to commence a CII. The OAIC will consider each referral it receives against its strategic regulatory priorities.
- 2.11 In deciding how to respond to a referral, the key considerations are the likelihood that the allegation referred to the OAIC is accurate, and the seriousness of the alleged breach. The OAIC may also consider the other matters outlined in the *Privacy regulatory action policy*, or the *CDR regulatory action policy* for CDR matters. In deciding whether to take any action in response to an alleged breach of the Privacy Act, the OAIC will consider the likelihood of an allegation, and its seriousness. The OAIC's response will be based on an evaluation of each allegation with reference to its potential seriousness, as summarised in the table below.

 Seriousness	No action	<b>Commence CII (or preliminary inquiries)</b>	<b>Commence CII (or preliminary inquiries)</b>
	No action	Advise respondent of allegation and provide general guidance	Advise respondent of allegation and provide general guidance
	No action	No action	Advise respondent of allegation and provide general guidance
	 Likelihood		

- 2.12 If an allegation is both serious and likely, the OAIC will commence preliminary inquiries and may recommend the Commissioner conduct a CII.
- 2.13 If an allegation appears likely to be accurate, but is less serious, the OAIC will typically write to the respondent to advise that an allegation has been made, and provide general guidance to allow the respondent to address the issue itself.
- 2.14 In other cases the OAIC will not take action in response to a referral. However, the OAIC will keep a record of the referral and may refer to it in future.
- 2.15 The OAIC will not usually reveal the name of the person who made the referral to the respondent.
- 2.16 Where referrals relate to allegations about compliance with the CDR scheme, the OAIC may provide the ACCC with details of the allegation and any action the OAIC has taken in response.

## Considerations in opening a CII

- 2.17 The Commissioner's primary objective when undertaking a CII is improving the privacy practices of investigated entities and the regulated community generally.
- 2.18 When deciding whether to commence a CII, the OAIC will consider the factors identified in the OAIC's *Privacy regulatory action policy*, and where appropriate, the *CDR regulatory action policy* and its strategic regulatory priorities.
- 2.19 The Commissioner will also consider the specific and general educational, deterrent or precedential value of commencing a CII, and whether it presents an opportunity to provide guidance to industry, Government or the public on better privacy practice and acceptable privacy standards.

## Procedural steps in conducting a CII

- 2.20 Where the OAIC decides to commence a CII, the following four steps will be taken.

### 1. Notification to respondent

- 2.21 The OAIC will notify the respondent in writing about its decision to commence a CII, and the initial scope of the investigation. If during the course of the investigation other issues arise in relation to the respondent's compliance with the APPs or the privacy safeguards and CDR Rules, these may be considered as part of the investigation. After notifying the respondent of the investigation, the OAIC will typically place a notice on its website stating that it is commencing an investigation. However, the OAIC will not comment further until the investigation is complete.

### 2. Information gathering

- 2.22 The OAIC will correspond with the respondent to gather information. The OAIC will seek the cooperation of the respondent in the provision of necessary information, and the respondent is typically the OAIC's primary source of relevant information.
- 2.23 The OAIC may gather information from other sources as required, such as the ACCC for CDR matters.
- 2.24 The Commissioner may issue a notice under s 44 of the Privacy Act requiring a person to provide information or produce documents, or to give evidence to the Commissioner in person.

### 3. Decision making

- 2.25 The Commissioner will consider the information provided to the OAIC and form a preliminary view in relation to the matter.
- 2.26 The Commissioner may decide to exercise a discretionary power under s 41 of the Privacy Act to discontinue an investigation, including where the Commissioner is satisfied that no breach has occurred or that the breach has been adequately dealt with by the respondent and no further regulatory action is warranted in the circumstances.

- 2.27 Where the Commissioner forms a preliminary view that the respondent has failed to meet the requirements of the Privacy Act or the requirements of the privacy safeguards or CDR Rules, the Commissioner may take further regulatory action, including the following:
- The Commissioner may seek an enforceable undertaking from the respondent under s 33E of the Privacy Act and s 56EW of the Competition and Consumer Act. More information about enforceable undertakings is available in Chapter 3 of this guide.
  - The Commissioner may make a determination under s 52(1A) of the Privacy Act. The determination, including the Commissioner's reasons for the determination, will be published on the OAIC's website. More information about determinations is available in Chapter 4 of this guide.
  - The Commissioner may seek an injunction against a person to enforce the Privacy Act (s 80W of the Privacy Act) and against CDR participants to enforce the privacy safeguards (s 56EX of the Competition and Consumer Act). More information about injunctions is available in Chapter 5 of this guide.
  - Where a civil penalty provision has been breached, the Commissioner may apply to the court for a civil penalty order under s 80U of the Privacy Act and s 56EU of the Competition and Consumer Act. More information about civil penalties is available in Chapter 6 of this guide.
  - The Commissioner may report to the Minister about a CII under s 30 of the Privacy Act. In certain circumstances, the Commissioner is required to report to the Minister.
- 2.28 The Commissioner may decide that although the entity has breached the Privacy Act or the requirements of the privacy safeguards and CDR Rules, no further action is required. This will depend on the specific circumstances of the matter, and if the Commissioner forms this view, the Commissioner may send a warning letter to the entity which sets out the OAIC's awareness of acts or practices of the entity that may not be compliant with its privacy obligations, and warns the entity that the OAIC may take future privacy regulatory action if it does not improve its compliance.

## 4. Conclusion and publication

- 2.29 At the conclusion of a CII, the OAIC will typically place a notice on its website advising of the conclusion of the investigation.
- 2.30 Where the Commissioner considers there is sufficient public interest in an incident, the Commissioner may publish a report of the investigation, which would be published alongside or as part of any enforceable undertaking or determination.
- 2.31 The OAIC will make decisions about communications in connection with CIIs in accordance with the considerations set out in the 'Public communication as part of regulatory action' sections of the *Privacy regulatory action policy*, and where appropriate, the *CDR regulatory action policy*.