Commissioner Initiated Investigation into Kmart Australia Limited (Privacy) [2025] AICmr 155 (26 August 2025)

Decision and reasons for decision of Privacy Commissioner, Carly Kind

Respondent	Kmart Australia Limited
Decision date	26 August 2025
Case reference number	CII22/00002
Catchwords	Privacy — *Privacy Act 1988* (Cth) — Australian Privacy Principles — APP 3.3 – APP 3.4 – APP 5.1 – APP 5.2 – APP 1.3 – APP 1.4 — whether personal information was collected – whether permitted general situation existed in relation to collection – whether reasonable steps were taken to notify or otherwise ensure individuals were aware of APP 5.2 matters – whether the respondent had a clearly expressed and up-to-date privacy policy – breaches substantiated – must not repeat or continue acts and practices found to be an interference with individuals' privacy

Determination

1. I find that Kmart Australia Limited (**respondent** or **Kmart**) interfered with the privacy of the individuals whose personal information and sensitive information it collected via its facial recognition technology (**FRT**) system at 28 of its retail stores (**relevant stores**) between 22 June 2020 and 15 July 2022 (**relevant period**), within the meaning of s 13(1) of the *Privacy Act 1988* (Cth) (**Privacy Act**), by:
    a. collecting the sensitive information of those individuals in circumstances where the individuals did not consent to the collection of the information and Australian Privacy Principle (**APP**) 3.4 did not apply in relation to the information, contrary to APP 3.3; and

b. failing to take such steps as were reasonable in the circumstances to notify or otherwise ensure those individuals were aware about the relevant APP 5.2 matters, contrary to APP 5.1.

2. I also find that the respondent breached APP 1.3 by failing to include in its privacy policies information about the kinds of personal information that it collected and held, and how it collected and held that personal information, as required by APP 1.4(a) and APP 1.4(b).

Declarations

3. I declare, under s 52(1A) of the Privacy Act, that the respondent:

   a. must not repeat or continue the acts or practices that I have found to be an interference with the privacy of individuals, as outlined at paragraph [1];

   b. must, within **30 days** of the publication of the determination, make an apology available on its website (https://www.kmart.com.au/ - **Kmart website**) and in relevant stores for at least 30 days;

   c. must, within **30 days** of the publication of the determination, publish a statement (**statement**) which is accessible from and prominently featured on the homepage of the Kmart website for at least 30 days, setting out:

      i. the fact that I have made a determination finding that the respondent interfered with the privacy of individuals and the date on which the determination was made;

      ii. a detailed description of its use of the FRT system, including the dates of operation and stores in which it operated;

      iii. how the FRT system operated, including how it collected facial images, what it did with the facial images, the fact that matches were generated, and how the respondent acted on such matches;

      iv. the fact that the respondent did not seek consent for the collection of individuals' personal information and sensitive information for the purposes of operating the FRT system;

      v. a detailed description of the relevant APP 5.2 and APP 1.4 matters that the respondent omitted from its privacy policies during the relevant period; and

      vi. advice to individuals about how they may contact the respondent to find out more information and how to make a complaint if they wish;

   d. must ensure that the statement is otherwise available on the Kmart website, which is accessible from the webpages relevant to the respondent's privacy policy, for a period of **12 months** following publication of the statement;

   e. is to retain all personal information and sensitive information obtained or generated through the FRT system that it still holds, including any images, biometric information, personal information, and information in relation to the use of the FRT system, including any guidelines, procedures or other documents, including any produced under the 'Minimum Standards for the Use of Facial Recognition'[1], for **12 months** following publication of the statement as required by declaration [3.c.];

[1] The 'Minimum Standards for the Use of Facial Recognition' are discussed at paragraph [32].

f. subject to declaration [3.e.] and to the extent permitted by law, destroys all personal information the subject of declaration [3.e] **12 months and one day** after the respondent has taken the action required by declaration [3.e]; and

g. is to provide written confirmation to the OAIC when it has complied with declaration [3.f].

Key issues

4. This determination concerns the deployment of an FRT system to detect and prevent refund fraud in a large retail chain, Kmart. It involves an analysis of the 'permitted general situations' enumerated by the Privacy Act,[2] according to which entities are not required to obtain consent to collect sensitive information, including biometric information, when certain circumstances apply.[3] The permitted general situation relied upon by the respondent applies when an entity has reason to suspect that unlawful activity has been, is being or may be engaged in, and it reasonably believes that the collection, use or disclosure of sensitive information is necessary in order for them to take appropriate action in relation to it.[4]

5. The permitted general situations were introduced into the Privacy Act in 2012,[5] at a time when public deployment of FRT was a speculative and futuristic notion. Understanding how FRT accords with the protections contained in the Privacy Act therefore requires both a textual and purposive analysis, taking into account the objects of the Privacy Act, including the need to balance the interests of individuals in having their privacy protected, on the one hand, and the interests of entities in carrying out their functions or activities, on the other. Relevant to a technology like facial recognition, is also the public interest in protecting privacy.

6. Indeed, in 2024 the Privacy Act was amended to explicitly recognise this public interest by the *Privacy and Other Legislation Amendment Act*.[6] In the second reading speech to that legislation, then Attorney-General the Honourable Mark Dreyfus KC MP observed that, "[t]he right to privacy is a fundamental human right. As Sir Zelman Cowen said in his 1969 Boyer Lectures, a person without privacy is a person without dignity. We must be vigilant in ensuring that evolving technology does not erode our ability to protect information about who we are, what we do and what we believe from being misused."[7]

Investigation by the OAIC

7. The respondent operates 'Kmart' retail stores across Australia. During the relevant period, the respondent operated between 214 and 303 stores,[8] 28 of which were selected to implement FRT as part of a 'pilot program'.[9] The pilot program included stores within all Australian states and territories, except for the Northern Territory and Tasmania.[10]

---

[2] *Privacy Act 1988* (Cth) s 16A.
[3] APP 3.3, APP 3.4.
[4] *Privacy Act 1988* (Cth) s 16A, Item 2.
[5] The amending legislation was the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).
[6] *Privacy and Other Legislation Amendment Act 2024* (Cth).
[7] Commonwealth, *Parliamentary Debates*, House of Representatives, 12 September 2024, 6652 (The Hon Mark Dreyfus KC MP, Attorney General) (*Privacy and Other Legislation Amendment Bill 2024 Second Reading)*.
[8] R2.1.A1 – Appendix 1 to R2.1: Answers to the questions in the OAIC notice p.2.
[9] R1.1 – Attachment to R1: Letter from the respondent to the OAIC dated 8 August 2022 p.1.
[10] R1.1.A3 – Appendix 3 to R1.1: List of FRT stores.

The FRT software used by the respondent was provided by a third-party supplier (**third-party supplier**) and was integrated with the respondent's systems and servers (collectively, the **FRT system**).

8. Initially, the respondent used the FRT system in one store from 22 June 2020.[11] From 27 July 2021 to 22 December 2021, the respondent progressively deployed the FRT system in a further 27 stores.[12] [Redacted].[13]

9. On 11 July 2022, the former Australian Information Commissioner (**Commissioner**) commenced an investigation into the acts and practices of the respondent relating to its use of FRT under s 40(2) of the Privacy Act. In response to the Commissioner's investigation, the respondent ceased operating the FRT system on 15 July 2022.[14]

10. On 27 February 2025, a preliminary view was issued to the respondent for comment and the respondent made substantive submissions in response.[15]

11. For the purposes of s 43(4) of the Privacy Act, I am satisfied that:

    a. the acts and practices to which the investigation relates can be adequately determined in the absence of a hearing with the respondent; and

    b. there are no unusual circumstances that would warrant holding a hearing before making this determination.

Findings and Reasons

The relevant law

12. The APPs in Schedule 1 of the Privacy Act regulate the handling of personal information by Australian government agencies and certain private sector organisations (**APP entities**).

13. An APP entity is prohibited from doing an act, or engaging in a practice, that breaches an APP.[16] An act or practice of an APP entity is an interference with the privacy of an individual if it breaches an APP in relation to personal information about an individual.[17]

14. I am satisfied that the respondent is an APP entity because it is a body corporate that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.[18]

---

[11] R1.1 – Attachment to R1: Letter from the respondent to the OAIC dated 8 August 2022 p.1.
[12] R1.1 – Attachment to R1: Letter from the respondent to the OAIC dated 8 August 2022 p.1; R2.1.A1 – Appendix 1 to R2.1: Answers to the questions in the OAIC notice p.6.
[13] R2.1.A1 – Appendix 1 to R2.1: Answers to the questions in the OAIC notice p.2.
[14] R1.1 – Attachment to R1: Letter from the respondent to the OAIC dated 8 August 2022 p.1.
[15] R3.1 – Letter from the respondent to the OAIC dated 10 April 2025; R3.2 – Respondent's spreadsheet of financial information for relevant years; R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025; R4.2 – Witness Statement – Respondent's General Manager Central Operations and Safety dated 30 April 2025.
[16] Privacy Act s 15.
[17] Privacy Act s 13(1).
[18] Privacy Act s 6C(1).

15. In making this determination, I have considered the information and submissions provided by the respondent. I have also considered the *Australian Privacy Principles Guidelines* (**APP Guidelines**)[19] and the *OAIC's Guide to privacy regulatory action*.[20]

16. The APPs relevant to this investigation are APPs 3.3, 3.4, 5.1, 5.2, 1.3 and 1.4.

The FRT system

17. The FRT system was an 'on premises [sic] solution' hosted by the respondent,[21] which stored data on technology infrastructure that was owned or controlled by the respondent, save for one central server located at an Australian data centre.[22]

18. The respondent claims that it used the FRT system for the sole purpose of detecting and preventing fraudulent refunds, and to assist in identifying individuals who had previously engaged in refund fraud or theft (**person(s) of interest**), some of whom were violent or threatened violence towards the respondent's staff and customers.[23]

19. The respondent's staff members were trained to check for refund fraud where the individual requested a refund and one or more of the following circumstances applied (**suspicious circumstances**):

    a. the individual did not provide a proof of purchase, such as a receipt;

    b. [Redacted];

    c. [Redacted]; or

    d. the individual was a person of interest as defined by the respondent and set out at paragraph [26] below.[24]

20. The operation and functionality of the respondent's FRT system during the relevant period is outlined below.

The matching process

21. The FRT system used video feed from Closed Circuit Television (**CCTV**) cameras to capture, in real time, the facial images of all individuals who entered a relevant store and all individuals who presented at the returns service desk (**Returns Counter**) of a relevant store during the relevant period.[25]

22. The FRT system was used in two locations in relevant stores to collect individuals' information. According to the respondent, it generated 5 to 6 facial images (**real time facial image**) from the CCTV footage of every individual at the point of entry to the relevant store, and again upon each individual's attendance at the Returns Counter.[26] The best quality of those facial images (both upon entry and upon attendance at the Returns Counter) was used to generate metadata. The process of creating metadata took

[19] December 2022 version – Australian Privacy Principles guidelines — OAIC.
[20] December 2024 version – Guide to privacy regulatory action — OAIC.
[21] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.2; T1.1 – Attachment to T1: Letter from the third-party supplier to the OAIC dated 3 October 2022.
[22] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.2.
[23] R1.1 – Attachment to R1: Letter from the respondent to the OAIC dated 5 August 2022 p.2.
[24] R1.1 – Attachment to R1: Letter from the respondent to the OAIC dated 5 August 2022 p.2; R1.1.A1 - Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.6; R2.1 - Attachment to R2: Letter from the respondent to the OAIC dated 7 October 2022 p.3.
[25] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.3.
[26] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.5-6.

approximately 1 to 2 seconds to complete[27] and involved the FRT system generating 'feature vectors' for each detected face[28] which created a digital representation or 'model' of the facial image.[29] These vectors effectively defined the location of the face within certain dimensions of feature space,[30] and were unique to an individual's face.

23. The metadata extracted from the facial image of an individual who presented at the Returns Counter was automatically compared against:

    a. the metadata of individuals' facial images held on a database of the relevant store that the individual entered (**History Database**). The History Database stored the facial images and metadata of all individuals who had entered the relevant store and all individuals who had presented at a Returns Counter at that store. Initially, the respondent retained the metadata in the History Database for [Redacted] and from April 2022, for [Redacted]. [Redacted];[31] and

    b. the facial images and metadata of individuals who had been included on the enrolment database (**Enrolment Database**), which was shared amongst the relevant stores, because the respondent believed that they may engage in refund fraud across stores. [Redacted], as outlined at paragraph [30];[32]

    to determine whether there was a match.

24. If a match was detected against the History Database, the store manager and team member managing the Returns Counter were able to view the relevant facial images and readily obtain the CCTV footage of the individual entering the store through the Milestone Return Desk (**MRD**) software system, which was accessible on the computer at the Returns Counter. However, staff members at the Returns Counter only completed this process where a person requested a refund and one of the suspicious circumstances at paragraph [19] applied.[33] The purpose of the review was to determine [Redacted].[34]

25. Staff members could 'refuse refunds when they detected fraud',[35] such as where [Redacted].[36] While I accept that the overall objective of the FRT system was to detect and prevent fraudulent returns, as discussed at paragraph [79], I would observe that in each instance where staff members [Redacted], they were likely forming a suspicion that fraud may have occurred rather than 'detecting' fraud as the respondent has claimed – particularly given the limitations of this method discussed at paragraphs [94] – [97].

26. Where a match was detected against the Enrolment Database, the team member managing the Returns Counter would receive a notification through the MRD System,[37] thereby alerting them that the individual was a person of interest. Where the individual was identified as a person of interest, this was one of the suspicious circumstances set out at paragraph [19.d.], that triggered the staff member to undertake the review process described at paragraph [24].

---

[27] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice pp.3 and 6.
[28] T1.1.A1 – Appendix to T1.1: Answers to the questions in the OAIC notice p.2.
[29] R1.1.A1 – Appendix 1 to R1:1 Answers to the questions in the OAIC notice p.4.
[30] T1.1.A1 - Appendix to T1.1: Answers to the questions in the OAIC notice p.3.
[31] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice pp.1, 3, 6 and 11.
[32] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.4.
[33] R1.1 – Attachment to R1: Letter from the respondent to the OAIC dated 8 August 2022 p.2; R1.1.A1. – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.4.
[34] R2.1.A1 – Appendix 1 to R2: Answers to the question in the OAIC notice p.4.
[35] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.22.
[36] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.22; R1.1.A7.2 – Appendix 7.2 to R1.1: ShrinK 365: FRT National Office Guide dated April 2022 p.4.
[37] R1.1.A1 – Appendix 1 to R1.1 Answers to the questions in the OAIC notice p.4.

27. The respondent submitted that where a match was not generated in respect of an individual's facial image, the real time facial images and real time metadata stored in the History Database was inaccessible to anyone, including the respondent's staff, and automatically deleted [Redacted] after collection.[38] The respondent considered a retention period of [Redacted] in the History Database was required, because from its experience [Redacted] was an insufficient period of time to allow the detection of refund fraud.[39]

Enrolment Database

28. The FRT system stored in the Enrolment Database the facial images and metadata of individuals who the respondent considered to be a person of interest because they had attempted, or were reasonably suspected of having attempted, to obtain a fraudulent return. In some circumstances, an attempt to obtain a fraudulent return included violence or threatened violence to the respondent's staff or customers (**enrolled individuals**).[40]

29. The respondent submitted that while enrolled individuals' facial images were typically obtained from real time facial images captured by store CCTV cameras, any images of sufficient quality could be uploaded to the Enrolment Database.[41] The respondent confirmed it did not upload any images to the Enrolment Database or History Database, other than real time facial images.[42]

30. The respondent was unable to provide the total number of individuals enrolled on the Enrolment Database throughout the relevant period due to the 'dynamic nature of enrolments'.[43] However, there were [Redacted] enrolled individuals on the Enrolment Database as at 15 July 2022.[44] At that time, the respondent had a [Redacted] retention period for information held in the Enrolment Database, which was capable of being extended by an additional [Redacted] in certain circumstances.[45] The respondent confirmed that, to the best of its knowledge, it never enrolled a child on the Enrolment Database.[46]

31. Individuals suspected of attempting to obtain a fraudulent return were enrolled in the Enrolment Database.[47] This could occur by:

    a. a team member of the respondent enrolling the individual into the Enrolment Database at the time of or immediately after reviewing footage; or

    b. the respondent's loss prevention business partner (**LP partner(s)**) manually enrolling an individual into the Enrolment Database at any time.[48]

32. The respondent's LP partners were responsible for delivering training on the FRT system to the respondent's staff, consistent with its 'Facial Recognition Technology National

---

[38] R2.1 – Attachment to R2: Letter from the respondent to the OAIC dated 7 October 2022 p.3; R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.8.
[39] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.1.
[40] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice pp.1 and 5.
[41] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.5.
[42] R3.1 – Letter from the respondent to the OAIC dated 10 April 2025 p.2.
[43] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.10.
[44] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.5.
[45] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice pp.5, 7 and 10.
[46] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.11.
[47] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.5.
[48] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.5; R1.1.A7.1 – Appendix 7.1 to R1.1: ShrinK 365: FRT Guide dated November 2021 pp.14-15.

Office Guide' (**FRT Guide**) and completing operational sign offs to verify that the training had been completed.[49] LP Partners were also responsible for monitoring, reviewing and assessing the respondent's compliance with the 'Minimum Standards for the Use of Facial Recognition' (**Minimum Standards**).[50] The Minimum Standards were a Wesfarmers document adopted by the respondent for the purpose of ensuring compliance with 'applicable laws and regulations', among other matters.[51]

33. The capability of the respondent's LP partners to manually upload an individual's details to the Enrolment Database was enabled in circumstances where:

    a. the relevant store team had not identified the occurrence of refund fraud at the time of an individual's return request and fraud was later uncovered; or

    b. the relevant store team was unable to enrol the individual at the time as a result of violent or threatening behaviour by the individual.[52]

34. As discussed at paragraph [24], if an individual met one of the suspicious circumstances outlined at paragraph [19], the staff member used the MRD system to view the matched facial images and the CCTV footage of the individual's entry into the store. This information assisted the staff member [Redacted].[53]

35. If an incident was identified, they logged the issue through a loss prevention incident form.[54] That form included the date and time of the incident and report, store, type of incident, whether the incident was prevented, the value of the attempted refunds, particular counter, summary of the event, whether there was threatening or intimidating behaviour, whether there was property damage, and still images from the FRT system.[55]

36. Where any 'suspicious activities'[56] were identified by staff using the FRT system to check entry footage (distinct from the 'suspicious circumstances' described at paragraph [19]) , they 'marked' a customer's face as a person of interest for entry into the Enrolment Database. In that event, the customer's image was labelled with a status of 'known', together with their name, prefix of person of interest, store name, date and time recorded by the CCTV cameras.[57]

37. If a person of interest entered the respondent's store, an alert would be generated, and the face would appear in the system with a 'known' status.[58]

38. In circumstances where an enrolled individual attempted to obtain a refund and a staff member refused the refund, the staff member would record in the system the amount the person attempted to claim and that the refund was 'prevented'.[59]

---

[49] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.3; R1.1.A7.1 - Appendix 7.1 to R1.1: ShrinK 365: FRT Guide dated November 2021; R1.1.A7.2 – Appendix 7.2 to R1.1: ShrinK 365: FRT National Office Guide dated April 2022; R1.1.A13 – Appendix 13 to R1.1: Example of operational signoff.

[50] R2.1.A1 – Appendix 1 to R2.1: Answers to the questions in the OAIC notice p.14; R1.1.A10 - Appendix 10 to R1.1: Wesfarmers Minimum Standards for the use of FRT dated 3 September 2020.

[51] R1.1.A10 – Appendix 10 to R1.1: Wesfarmers Minimum Standards for the use of FRT dated 3 September 2020 p.1.

[52] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.5.

[53] R2.1.A1 – Appendix 1 to R2.1: Answers to the question in the OAIC notice p.4. R1.1.A7.1 - Appendix 7.1 to R1.1: ShrinK 365: FRT Guide dated November 2021 p.3.

[54] R1.1.A7.1 – Appendix 7.1 to R1.1: ShrinK 365: FRT Guide dated November 2021 pp.12-13; R1.1.A1 - Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.9.

[55] R1.1.A7.1 – Appendix 7.1 to R1.1: ShrinK 365: FRT Guide dated November 2021 p.17.

[56] R1.1.A7.1 – Appendix 7.1 to R1.1: ShrinK 365: FRT Guide dated November 2021 p.14.

[57] R1.1.A7.1 – Appendix 7.1 to R1.1: ShrinK 365: FRT Guide dated November 2021 p.15.

[58] R1.1.A7.1 – Appendix 7.1 to R1.1: ShrinK 365: FRT Guide dated November 2021 p.15.

[59] R1.1.A7.1 – Appendix 7.1 to R1.1: ShrinK 365: FRT Guide dated November 2021 p.16.

APP 3 – Collection of personal information

39. APP 3 outlines when and how an APP entity may collect solicited personal information,[60] being information or an opinion about an identified individual, or an individual who is reasonably identifiable:

    a. whether the information or opinion is true or not; and

    b. whether the information or opinion is recorded in a material form or not.[61]

40. The requirements in relation to when an APP entity can collect personal information vary according to whether or not the personal information is sensitive information, and whether the APP entity is an agency or an organisation.

41. The respondent has submitted that to the extent that it collected any sensitive information, it was lawfully entitled to rely on the permitted general situation outlined at item 2 of s 16A of the Privacy Act, as reflected in APP 3.4, such that it has not breached APP 3.3.[62]

42. In relation to the collection of any other personal information through the FRT system, the respondent submitted that the collection was consistent with its obligations under APP 3.2 because the collection was reasonably necessary for, and directly related to, its functions or activities.[63]

43. For the reasons that follow, I am of the view that the FRT system involved the collection of sensitive information. I have therefore focused my analysis on APP 3.3.

APP 3.3 – Sensitive information

44. Sensitive information includes biometric information that is to be used for the purpose of automated biometric verification or biometric identification, and biometric templates.[64] It is generally afforded a higher level of protection under the Privacy Act than other personal information.[65]

45. Under APP 3.3, an organisation must not collect sensitive information about an individual unless:

    a. the individual consents to the collection of the information and:

        …

        ii. the information is reasonably necessary for one or more of its functions or activities;[66] or

    b. APP 3.4 applies in relation to the information.[67]

46. Relevant to the issues raised by the respondent, APP 3.4 applies where a 'permitted general situation exists in relation to the collection of the information by the APP entity'.[68] The permitted general situations are set out in s 16A of the Privacy Act.

---

[60] APP Guidelines [3.2].
[61] Privacy Act s 6(1).
[62] R1.1 – Attachment to R1: Letter from the respondent to the OAIC dated 8 August 2022 p.2; R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.4.
[63] R1.1 – Attachment to R1: Letter from the respondent to the OAIC dated 8 August 2022 p.3.
[64] Privacy Act s 6(1)(d) and (e).
[65] APP Guidelines [B.144].
[66] APP 3.3(a)(ii).
[67] APP 3.3(b).
[68] APP 3.4(b).

Collection of personal and sensitive information

47. 'Collection' includes gathering, acquiring or obtaining personal information from any source and by any means, including from biometric technology.[69] An entity 'collects' personal information within the meaning of the Privacy Act only if the entity collects the personal information for inclusion in a record or generally available publication.[70] A 'record' includes a document or an electronic or other device.[71]

48. In investigating the acts and practices of the respondent, it was open to me to consider that there was more than one act of collection involved in the process of using the FRT system in the relevant stores, including the collection of real time facial images and metadata at store entry and the collection of real time facial images and metadata at Returns Counters. Instead, as the collection of images at the entry points and those at the Returns Counters are closely interrelated, I have considered the separate acts of collection as part of a continuous course of action undertaken to detect and prevent fraudulent refunds. I have also considered the collection of persons of interests' facial images and metadata on the Enrolment Database within the operation of the overall FRT system.

49. With respect to the History Database, the facial images that were captured of each individual who entered a relevant store during the relevant period constituted personal information and were collected regardless of whether the individual attended a Returns Counter. That information was collected for inclusion in a record in circumstances where it was held in the relevant History Database on the respondent's servers,[72] which constituted electronic devices.

50. With respect to the Enrolment Database, the facial images of enrolled individuals, together with their name (if known) and information or opinions about them, constituted personal information. That personal information was uploaded to the Enrolment Database, with metadata generated from each facial image so that it could be compared against the metadata generated from the facial images of individuals who entered a relevant store during the relevant period as part of the matching process. The Enrolment Database was held on the respondent's central servers,[73] which constituted electronic devices. Consequently, the personal information of enrolled individuals was collected for inclusion in a record.

51. As noted above, sensitive information includes biometric information[74] that is to be used for the purpose of automated biometric verification or biometric identification, and biometric templates.[75]

---

[69] APP Guidelines [B.30].
[70] Privacy Act s 6(1).
[71] Privacy Act s 6(1).
[72] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.2.
[73] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice pp.2 and 10.
[74] While not defined by the Privacy Act, 'biometrics' encompass a variety of technologies that use probabilistic matching to recognise a person based on their biometric characteristics. Biometric characteristics can be physiological features (for example, a person's fingerprint, iris, face or hand geometry), or behavioural attributes (such as a person's gait, signature, or keystroke pattern). These characteristics cannot be easily changed and are unique to the individual. See Office of the Victorian Information Commissioner Biometrics and Privacy, available at https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/.
[75] A 'biometric template' is a set of stored biometric features comparable directly to a biometric probe, being a biometric sample or feature set input to an algorithm for comparison to a biometric reference.

52. I accept that an individual's facial image, whether contained in a still image or video footage, may not constitute sensitive information in all cases. However, I am of the view that the facial image, when used by the FRT system to generate the metadata stored on the Enrolment and History Databases, together with the metadata itself, was sensitive information because it constituted biometric information that was to be used for the purpose of automated biometric verification or biometric identification via the matching process.

53. The metadata was derived from physical characteristics that were unique to the individual's face, as captured by the relevant facial image. That is, the metadata generated for a particular individual was distinct from that of other individuals, which allowed the matching process to occur.

54. The third-party supplier advised that the metadata could not, on its own, be used to reconstruct the image of an individual's face.[76] Further, the respondent submitted that the facial images and metadata held in the History Databases were inaccessible and deleted within [Redacted] of being collected.[77] However, I do not consider those factors to be relevant to whether the respondent collected sensitive information within the meaning of the Privacy Act through its use of the FRT system.

55. Ultimately, I am not persuaded that a system involving facial recognition could, by its very nature, operate without biometric information.

Findings

56. I find that the respondent collected the sensitive information of all individuals who entered a relevant store during the relevant period. Consequently, I consider that APP 3.3 applied in relation to the collection.

APP 3.3(a)

57. In order for consent to be valid, it must be informed, voluntary, current and specific, and given by individuals who have the requisite capacity.[78] I am not satisfied that individuals who entered a relevant store during the relevant period consented to the collection of their sensitive information through the respondent's use of the FRT system. There is no evidence before me that would indicate that consent was sought and obtained, and I am not satisfied that individuals could have been taken to impliedly consent by virtue of the respondent's signage, which is discussed further below in respect of APP 5.

APP 3.3(b) and 3.4(b) – Existence of a permitted general situation

58. The permitted general situations contained in s 16A of the Privacy Act prescribe specific conditions which, if met, allow an APP entity to collect, use or disclose personal information or government identifiers without breaching the APPs.

59. The respondent has relied on the permitted general situation at item 2 of s 16A of the Privacy Act. I am satisfied that the requirements outlined in columns 1 and 2 are met, namely that the respondent is an APP entity and that the item applies to personal information (which, as I have discussed above, also constitutes sensitive information).

See also International Organization for Standardisation, Standard ISO/IEC 2382-37: 2022(en), Standard 37.03.22 < https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-3:v1:en>.

[76] T1.1.A1 – Appendix to T1.1: Answers to the questions in the OAIC notice p.2.

[77] R2.1 – Attachment to R2: Letter from the respondent to the OAIC dated 7 October 2022 p.3.

[78] APP Guidelines [B.38].

Therefore, I have focused my analysis on the conditions outlined in column 3, which relevantly states:

a. the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in (**Condition (a)**); and

b. the entity reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter (**Condition (b)**).[79]

60. The respondent submitted that it had reason to suspect that unlawful activity, or misconduct of a serious nature, in the form of refund fraud has been, is being or may be engaged in at its retail stores.[80] The respondent further submitted that it 'reasonably believed, and in fact, the only practical means available to [the respondent] to manage refund fraud was to use the [FRT system], as it enabled [the respondent] to accurately and efficiently [Redacted].[81]

Condition (a)

61. I am satisfied that refund fraud, which can be characterised as activity that is criminal, illegal, or prohibited or proscribed by law,[82] constituted unlawful activity that related to the respondent's functions and activities in respect of the sale of goods and loss prevention.

62. The material provided by the respondent suggests that refund fraud had occurred in its stores and that the respondent could reasonably suspect that such activity was occurring and may continue to occur. For example, the respondent estimated that refunds without proof of purchase, including genuine refund requests across the Kmart network, equated to [Redacted] in the 2020 financial year, [Redacted] in the 2021 financial year and [Redacted] in the 2022 financial year.[83]

63. The respondent conducted an analysis of the information it has regarding individuals who frequently seek refunds to determine the circumstances in which fraud, or likely fraud, may have occurred.[84] Based on that analysis, the respondent estimated that [Redacted] of refunds without proof of purchase are either fraudulent or likely to be fraudulent.[85] I accept that a proportion of refunds without proof of purchase were likely to have been fraudulent.

64. I therefore accept that, during the relevant period, the respondent had reason to suspect that unlawful activity that related to its functions or activities had been, was being, or may be engaged in, such that Condition (a) was met. This unlawful activity was refund fraud where individuals attempted to obtain a refund for a product they had not purchased.

---

[79] Privacy Act s 16A.
[80] R1.1 – Attachment to R1: Letter from the respondent to the OAIC dated 8 August 2022 p.2; R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.3.
[81] R2.1 – Attachment to R2: Letter from the respondent to the OAIC dated 7 October 2022 p.2.
[82] APP Guidelines [C.16].
[83] R3.2 – Respondent's spreadsheet of financial information for relevant years.
[84] R2.1.A.1 – Appendix 1 to R2: Answers to the questions in the OAIC notice p.10.
[85] R2.1.A.1 – Appendix 1 to R2: Answers to the questions in the OAIC notice p.10; R3.1 – Letter from the respondent to the OAIC dated 10 April 2025 p.3.

Condition (b)

65. In order to satisfy Condition (b), the respondent needed to reasonably believe during the relevant period that the collection of personal information via the FRT system was necessary in order for it to take appropriate action in relation to refund fraud.

66. The respondent submitted a view that, with respect to Condition (b), 'the focus is on the "action" which was supported by the collection', and that '[t]he correct question is whether the collection of sensitive information due to the use of FRT was reasonably necessary to take appropriate action to address refund fraud.'[86] In my view, the focus is on the necessity of the collection, use or disclosure of sensitive information. The appropriateness of the actions taken should also be considered, but the focus of Condition (b) is whether the use of the FRT system was necessary to achieve those actions.

Reasonable belief

67. As a body corporate, the respondent's reasonable belief is discerned through corporate attribution or identification.[87] The respondent's reasonable belief for the purpose of the permitted general situation at item 2 can be established by attributing the state of mind of its senior management staff during the relevant period, including those who were involved in recommending, approving, implementing and monitoring the use of the FRT system. On the evidence provided by the respondent, this concerns the reasonable belief held by its General Manager Central Operations and Safety, who was at the relevant time the Head of Central Operations and the person who was the project sponsor for the respondent's FRT trial.[88] I accept the evidence provided by the respondent's former Head of Central Operations, who held a belief at the time of adopting the FRT system that it was necessary to take appropriate action to address refund fraud. In particular, I accept that she held a genuine belief in this respect.

68. In order to meet Condition (b), there must also be a reasonable basis for the respondent's belief, not merely a genuine or subjective belief.[89] This necessitates consideration of the objective facts and circumstances, as they existed during the relevant period, and whether such facts and circumstances were sufficient to induce the belief in a reasonable person.[90] As such, I have considered whether there were reasonable grounds to believe that collecting sensitive information of every person that entered a relevant store was necessary to take appropriate action.

Appropriate action

69. The respondent submitted that it used the FRT system to:

    a. detect and prevent fraudulent refunds, which had been identified as a significant cause of stock loss; and

---

[86] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.5.

[87] See *Nationwide News Pty Ltd v Naidu & Anor; ISS Security Pty Ltd v Naidu & Anor* [2007] NSWCA 377 at 234, citing *Hamilton v Whitehead* (1988) 166 CLR 121; *Director General, Department of Education and Training v MT* [2006] NSWCA 270; and *North Sydney Council v Roman* [2007] NSWCA 27.

[88] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.2; R4.2 – Witness Statement – Respondent's General Manager Central Operations and Safety dated 30 April 2025 p.1.

[89] APP Guidelines [C.8].

[90] *George v Rockett* (1990) 170 CLR 104 at 112, 116; see also *Seven Network v Australian Competition and Consumer Commission* (2004) 140 FCR 170 at 182.

b. assist in identifying persons of interest, being those individuals who had engaged in refund fraud or theft, which in some cases involved those individuals engaging in violent or threatening behaviour.[91]

70. I accept that it was appropriate for the respondent to take action to detect and prevent fraudulent refunds. As I understand the respondent's evidence, identifying persons of interest was also undertaken in order to detect and prevent fraudulent returns.

71. In respect of item 2 of s 16A, the relevant explanatory memorandum addresses 'appropriate action':

> '*The provision, by specifying that the unlawful activity or serious misconduct must relate to an entity's functions or activities,* ***intends that the exception will apply to an entity's internal investigations****. Examples of 'appropriate action' in this context may include collection, use or disclosure of personal information or a government identifier for an internal investigation in relation to internal fraud or breach of the Australian Public Service Code of Conduct.'*[92] [Emphasis added]

72. Similarly, the APP Guidelines address the term 'appropriate action' as follows, in the context of the general permitted situation at issue:

> *'Whether action is 'appropriate' will depend on the nature of the suspected unlawful activity or misconduct and the nature of the action that the APP entity proposes to take. Appropriate action may include investigating an unlawful activity or serious misconduct and reporting these matters to the police or another relevant person or authority. For example, if an entity reasonably believes that it cannot effectively investigate serious misconduct without collecting, using or disclosing personal information, this permitted general situation may apply.'*[93]

73. Accordingly, I consider that the focus of the exception is on the internal investigation with respect to its objective or outcome, for example, to form a view about a breach of an employment contract, or to make a report to police where indicated by the investigation. With respect to the above APP Guidelines, I consider these factors – that is, the investigation, its objectives and outcomes – to be the 'nature of the action'.

74. Consistent with the above, and with reference to the unlawful activity described at paragraph [64], I accept that it was appropriate for the respondent to take action to prevent and detect refund fraud, by its staff investigating refund requests to form a view as to whether the requests were bona fide or fraudulent, and declining to process a refund where they considered that a refund request was fraudulently made.

75. The respondent submitted that the 'appropriate action' it took or otherwise wished to take in response to actual or suspected refund fraud by individuals entering its stores involved:
    a. where any of the 'suspicious circumstances' outlined at paragraph [19] applied, assessing whether the individual [Redacted];
    b. ascertaining whether the individual seeking the refund was an enrolled individual; and
    c. pending consideration of the above matters, deciding whether to process the refund.[94]

---

[91] R1.1 – Attachment to R1: Letter from the respondent to the OAIC dated 5 August 2022 p.2.
[92] Explanatory Memorandum – *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth) p.67.
[93] APP Guidelines [C.20].
[94] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.6.

76. I acknowledge that this articulation closely reflects my previous characterisation of the respondent's submissions on this point, in my preliminary view. However, on further consideration this articulation of the action (or investigation) at paragraph [75] captures not only the action taken in relation to the unlawful activity, but also its underpinning methodology – hinging on the availability of the Enrolment Database to access information about 'enrolled individuals' as well as images or other evidence pertaining to individuals at store entry.

77. If I were to apply this articulation of 'appropriate action' it would result in a circular and referential analysis in relation to the general permitted situation in Item 2 of s 16A, insofar as a particular investigatory methodology is likely to necessitate collection of a specific type of information as the only practicable way to utilise that methodology.

78. Consequently, and with the exception of paragraph [75.c], to the extent it relates to deciding whether to provide a refund, I do not consider the actions at paragraph [75] above to constitute 'appropriate action' for which the collection of sensitive information must be necessary. They are instead the tools for, or interim steps towards, an implementation of the respondent's appropriate action in relation to the unlawful activity.

79. Accordingly, in my view, the action sought to be taken by the respondent was to detect and prevent fraudulent returns by ascertaining whether an individual was seeking, or likely to be seeking, to fraudulently return a product they purported to have purchased from the respondent, in circumstances where they had not purchased the product. I consider this action to be appropriate in the context of the unlawful action described at paragraph [64].

80. The respondent's then Head of Central Operations set out 'further actions'[95] which the respondent sought to take through using the FRT system including to:

    a. give the respondent's staff the confidence and ability to refuse refund requests by relying upon easily accessible supporting evidence that a customer [Redacted]; and

    b. reduce the likelihood of those customers behaving in a threatening or aggressive manner upon being refused a refund, including by reducing processing times for a refund request and having evidence available for staff to rely upon to justify the refund refusal.[96]

81. While I appreciate these may be conveniences and benefits of using the FRT system, I do not consider them 'appropriate actions' in the context of the general permitted situation at issue.

Necessity

82. 'Necessary' is not defined in the Privacy Act but is, for the purposes of the permitted general situations, something more than merely helpful, desirable or convenient,[97] but not essential or indispensable.[98]

---

[95] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.6.

[96] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.6; R4.2 – Witness Statement – Respondent's General Manager Central Operations and Safety dated 30 April 2025 pp.3-4.

[97] APP Guidelines [C.8].

[98] APP Guidelines [B.116]; *Mulholland v Australian Electoral Commissioner* [2004] HCA 41 [39] (Gleeson CJ).

83. The respondent has contended that the context in which it used the FRT system during the relevant period 'was reasonably appropriate and adapted in all of the circumstances'.[99]

84. Considering the question of whether the collection of sensitive information was necessary, in order to determine whether the conditions of Condition (b) are met, requires me to consider the respondent's FRT system. In summary, the FRT system operated by collecting individuals' sensitive information: at the point of entry for all customers, and upon attendance at a Returns Counter for those customers who attended that counter. This sensitive information consisted of the individual's facial image and metadata extracted from the individual's facial image – constituting biometric information as discussed. The collection of this sensitive information facilitated a matching process so that staff were able to quickly [Redacted], when they requested a refund in the circumstances outlined at paragraph [19].

85. I have considered the following factors in assessing whether the respondent could have reasonably believed that the collection of the sensitive information via the FRT system was necessary for the purposes of satisfying Condition (b):

    a. the **suitability** of the FRT system, including its efficacy in addressing refund fraud;

    b. the **alternatives** available to the respondent to address refund fraud; and

    c. whether the use of the FRT system was **proportionate**, which involves balancing the privacy impacts resulting from the collection of sensitive information against the benefits gained by the use of the FRT system.

86. In its submissions, the respondent has described this approach as 'structured proportionality'.[100] Rather, I have applied the above factors in order to determine whether the facts and circumstances, as they existed at the relevant time, constituted reasonable grounds for the respondent's belief that collection of sensitive information by the FRT system was necessary for it to take appropriate action in relation to refund fraud.

Consideration

Suitability

87. The suitability of the FRT system and in particular, its effectiveness with respect to action against refund fraud, is relevant to considering the reasonableness of the respondent's belief that the collection of personal information via that system was necessary.

88. The respondent submitted that it intended to monitor the effectiveness of the FRT system and to conduct a review after 12 months of continuous use. However, this was allegedly impacted by the effects of the COVID-19 pandemic, including lockdown periods and mask-wearing, together with 'stores actually using the FRT and stores actually reporting refund fraud prevention'.[101] In any event, I accept that, as the respondent submitted, 'it is possible that a person holds a "reasonable belief" that a system is necessary, without having qualitative proof to that effect.'[102]

---

[99] R2.1 – Attachment to R2: Letter from the respondent to the OAIC dated 7 October 2022 p.2; R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.3.

[100] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.10.

[101] R2.1 – Attachment to R2: Letter from the respondent to the OAIC dated 7 October 2022 p.2; R1.1.A1 - Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.15.

[102] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.14.

89. With respect to suitability, the respondent draws attention to the reasoning underpinning the recommendation of its (then) Head of Operations, as set out in her statement, which it submits draws on her lived experience both as a store manager and in senior leadership roles. In particular, the respondent highlights the then Head of Operations' awareness of increasing shrinkage – described as 'loss of stock or money for reasons unrelated to sales, such as shoplifting and refund fraud' – across the respondent's stores.[103] The respondent also points to the then Head of Operations' account of the limitations of alternatives to collection via the FRT system, that is, [Redacted] and amending the refund policy, discussed below in my analysis of the available alternatives.[104]

90. I accept that the FRT system facilitated the detection and prevention of a subset of refund fraud: that is, [Redacted]. Noting that the respondent sought to ascertain where individuals were seeking, or likely to be seeking, to fraudulently return an item they had not purchased from the store, I accept that the FRT system enabled staff members to easily and quickly access and [Redacted].

91. It appears however that the FRT system was not suitable for the purposes of responding to potentially fraudulent returns in other circumstances, such as where [Redacted].

92. In its evidence, the respondent described five known refund fraud techniques without acceptable proof of purchase.[105] It is apparent that not all techniques would be suitably addressed by the FRT system – in particular:

    a. [Redacted]

    b. [Redacted][106]

93. I accept that the FRT system would be more suitable to facilitate detection and prevention in relation to the following fraud techniques:

    a. [Redacted]

    b. [Redacted]

    c. [Redacted][107]

94. However, even in the above circumstances, it appears that the effectiveness of the FRT system in facilitating the detection and prevention of refund fraud was limited. The respondent's FRT Guide, and its FRT National Office Guide, specifically address this in its instructions to staff members:

    a. [Redacted]

    b. [Redacted]

    c. [Redacted][108]

---

[103] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.14; R4.2 – Witness Statement – Respondent's General Manager Central Operations and Safety dated 30 April 2025 p.1.

[104] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 pp.14-15; R4.2 – Witness Statement – Respondent's General Manager Central Operations and Safety dated 30 April 2025 pp.3-7.

[105] R2.1.A1 – Appendix 1 to R2.1 – Answers to the questions in the OAIC notice p.10.

[106] R2.1.A1 – Appendix 1 to R2.1 – Answers to the questions in the OAIC notice p.10.

[107] R2.1.A1 – Appendix 1 to R2.1 – Answers to the questions in the OAIC notice p.10.

[108] R1.1.A7.1 - Appendix 7.1 to R1.1: ShrinK 365: FRT Guide dated November 2021 pp.12-13; R1.1.A7.2 – Appendix 7.2 to R1.1: ShrinK 365: FRT National Office Guide dated April 2022 p.6.

95. These limitations appear to be significant, noting for example that I would expect many customers entering one of the respondent's stores to [Redacted].

96. I therefore consider that the FRT system was effective in detecting the subset of refund fraud described at paragraph [90] in certain circumstances. This would usually be where individuals present item(s) for return that are [Redacted]. Additionally, there may be other circumstances where the FRT system is less effective, such as where [Redacted].

97. I note that, even in those circumstances, there is an element of uncertainty in detecting fraudulent returns, given the known possibility of [Redacted].

98. I consider that to have formed a reasonable belief with respect to the necessity of the FRT system, consideration ought to have been given to the practical limitations of that system. I accept that this consideration may have been undertaken with respect to the subset of fraud as described at paragraph [90] – at least, it is evident from the statement of the then Head of Operations that there is no expectation it would apply to other types of refund fraud, such as those described at paragraph [92].[109] However, there is no evidence before me that the practical limits of the FRT system with respect to the circumstances in which it could effectively detect refund fraud – as described at paragraphs [94] to [96] – were considered in forming a belief as to its suitability, and therefore necessity, in taking appropriate action in relation to the unlawful activity.

99. At its highest, I can accept that the FRT system was partially suitable to take action to prevent and detect refund fraud and it was reasonable to believe that it was partially suitable for this purpose.

100. The partial or limited suitability of the FRT system is reflected by the figures provided by the respondent with respect to incidents of prevented refund fraud using this system, and the value of the same. The respondent provided data showing that, during 2021 and 2022 across the 28 relevant stores, it recorded a total of [Redacted] incidents of prevented refund fraud.[110] The total sum of the fraudulent refunds prevented amounted to [Redacted] across the 28 relevant stores during that period.[111] While the FRT pilot program commenced in one store in June 2020, for most stores the FRT system was implemented in the later months of 2021, continuing until the respondent ceased the use of FRT on 15 July 2022.[112] Even for a pilot program, this is a [Redacted] with respect to the scale of the issue. By way of indicative figures, it amounts to [Redacted], per relevant store, at an average of less than [Redacted] per refund.

101. I note the respondent considers that FRT was only being used by the relevant stores in a manner that would enable such an assessment to be made in the 3 to 4 months prior to it ceasing operation in July 2022.[113] However, I have had regard to figures provided by the respondent reflecting the value of refunds prevented through 2022 and those figures remained [Redacted] through that period.[114]

102. With respect to the scale of the issue, I have considered the figures the respondent has provided, including for the 2020 financial year as the period leading up to and overlapping with the beginning of the FRT pilot program. If I accept the respondent's

---

[109] R4.2 – Witness Statement – Respondent's General Manager Central Operations and Safety dated 30 April 2025 p.2.

[110] R2.1.A3 – Appendix 3 to R2.1: Incident reports and refunds prevented.

[111] R2.1.A3 – Appendix 3 to R2.1: Incident reports and refunds prevented.

[112] R1.1.A3 – Appendix 3 to R1.1: List of FRT stores; R1.1.A1 – Appendix 1 to R.1.1: Answers to the questions in the OAIC notice p.15.

[113] R2.1 – Attachment to R2: Letter from the respondent to the OAIC dated 7 October 2022 p.2 [7]. R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.15.

[114] R2.1.A3 – Appendix 3 to R2.1: Incident reports and refunds prevented.

estimate that [Redacted] per cent of such returns that are – or are likely to be – fraudulent, that amounts to [Redacted] in fraudulent, or likely fraudulent, returns in 2020.[115] I note as well that the then Head of Operations reported the respondent's figure for shrinkage in that same financial year to total [Redacted].[116]

103. I appreciate that the FRT system was a pilot program in a select number of the respondent's stores and its full potential may not have been realised during the relevant period for various reasons, including the impact of the COVID-19 pandemic. I also acknowledge the then Head of Operations' evidence with respect to her belief that the circumstances in which the FRT system was utilised would likely expand as its use matured, enabling the respondent to prevent a higher proportion of fraud[117] although I have no evidence before me as to potential additional uses.

104. Generally, however, I consider that the limitations of the FRT system are reflected by the [Redacted] with respect to fraudulent or suspected fraudulent incidents detected, and the value of fraud prevented, in comparison to the estimated value of the unlawful activity as well as the figure provided by the then Head of Operations with respect to shrinkage.

Alternatives

105. In my view, in considering whether the collection of sensitive information by the FRT system was necessary to enable the respondent to take appropriate action to address refund fraud, it is open to me to consider whether there were alternative methods available to the respondent that were less privacy intrusive in nature.

106. The respondent has submitted that an alternative method to the FRT system will only be a comparator, that is, 'obvious and compelling', where it is 'reasonably practicable' and 'equally effective'.[118]

107. I agree that the practicality and effectiveness of other methods are relevant to assessing whether they represent genuine alternatives. However, I do not accept that the correct test is one of 'equal' effectiveness or that of a like for like comparison between FRT on the one hand and other standalone practices on the other. I note this case concerns the business practices of commercial entities seeking to secure their retail operations from fraudulent activities. I observe entities may take into consideration a range of different factors as to whether a particular measure is practical and effective, including the cost of the measure and the impost on the staff and customers of the store.

108. Furthermore, I understand in the context of retail security it is commonplace for entities to use a 'layered protection' approach to securing goods and premises, such as utilising a range of technical tools, staffing practices, store features and layouts, signage and lighting. In this context, it may be difficult to identify in isolation the contribution to enhanced security that each layer of protection makes. I am of the view that the purpose of my inquiry is to understand whether there were alternative methods that

---

[115] R2.1.A.1 – Appendix 1 to R2.1: Answers to the questions in the OAIC notice p.10; R3.1 – Letter from the respondent to the OAIC dated 10 April 2025 p.3. As discussed in paragraph [62], the respondent provided figures that refunds without proof of purchase amounted to [Redacted] in the 2020 financial year.

[116] R4.2 – Witness Statement – Respondent's General Manager Central Operations and Safety dated 30 April 2025 p.6; R2.1.A.1 – Appendix 1 to R2.1: Answers to the questions in the OAIC notice p.10; R3.1 – Letter from the respondent to the OAIC dated 10 April 2025 p.3.

[117] R4.2 – Witness Statement – Respondent's General Manager Central Operations and Safety dated 30 April 2025 p.6.

[118] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.16.

could have practically and effectively been deployed that were less privacy intrusive and ought to have been considered by the respondent before implementing a solution that operated by collecting sensitive information.

109. The respondent contended that the use of the FRT system was the 'only practical means available' to manage refund fraud.[119] It submitted that:

> *'Prior to the use of FRT [Redacted].'*[120]

110. The then Head of Central Operations expanded on this in her statement. She declared that, other than the FRT system, [Redacted].[121] As a consequence, she considered that this method was not practical because it:

    a. affected the customer experience;

    b. led to some customers being agitated, and in the worst cases, threatening or abusive towards staff;

    c. distracted the respondent's staff from their role serving customers or managing store operations; and

    d. [Redacted].[122]

111. The then Head of Central Operations submitted that, as a result of this impracticality, [Redacted] in any of the respondent's policies as a method to addressing retail fraud. I also note the then Head of Central Operations' evidence that [Redacted], and that this method would not have identified instances in which a customer [Redacted].[123]

112. I accept that the [Redacted] may have not been the most expeditious alternative to the FRT system and may have impacted customer experience. Nevertheless, it remained an option open to the respondent if a staff member was contemplating processing a refund where doubts remained about the legitimacy of the request. I note that the respondent could and did layer the [Redacted] with other security protections, [Redacted].[124]

113. I note that at the relevant time the LP Partners team comprised of [Redacted] in each of Victoria and New South Wales, and [Redacted] in each of Queensland, Western Australia and South Australia.[125] I observe that it was open to the respondent to scale up the LP Partner team, including placing a LP Partner or other appropriately qualified loss-prevention staff member in each store. In addition, or in the alternative, staff could be trained to observe signs of suspicious behaviour and escalate to [Redacted] in certain circumstances, although I acknowledge that, practically speaking, these circumstances may need to be more narrowly defined than the respondent was able to apply in conjunction with the FRT system.

---

[119] R2.1 – Attachment to R2: Letter from the respondent to the OAIC dated 7 October 2022 p.2.

[120] R2.1 – Attachment to R2: Letter from the respondent to the OAIC dated 7 October 2022 p.2.

[121] R4.2 – Witness Statement – Respondent's General Manager Central Operations and Safety dated 30 April 2025, pp.3-4.

[122] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.18; R4.2 – Witness Statement – Respondent's General Manager Central Operations and Safety dated 30 April 2025 p.4.

[123] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.18; R4.2 – Witness Statement – Respondent's General Manager Central Operations and Safety dated 30 April 2025 pp.4-5.

[124] See for example, Australian Bureau of Statistics, Occupation 452236 Retail Loss Prevention Officer, accessed 22 August 2025.

[125] R3.1 – Letter from the respondent to the OAIC dated 10 April 2025 pp.2-3.

114. The respondent also provided information about two other methods that were used to identify individuals engaging in refund fraud which did not require the FRT system:

    a. [Redacted].

    b. [Redacted].[126]

115. The respondent submitted that both methods were deemed ineffective compared to FRT, and do not offer alternatives in the requisite sense.[127] I accept that these methods may not have been as effective as the FRT system. However, they represent less privacy intrusive alternatives to the deployment of FRT.

116. Moreover, in my view there were other less privacy intrusive methods the respondent could have implemented to address refund fraud that were obvious and compelling. For example, the respondent could have considered locating the Returns Counter at or before the entrance to the store or making it outward facing so that customers would not need to enter a store to request a refund. This would limit the opportunity for individuals to acquire goods within the store and seek to return them without paying for them. Paired with increased use of technological solutions, such as radio frequency identification (**RFID**) tags to prevent individuals from taking stolen goods out of the store without detection, this may have been a practicable and effective way of reducing refund fraud.

117. A further option open to the respondent, subject to Australian consumer law,[128] was to consider implementing a more robust refund policy whereby refunds could not be processed, or only processed in exceptional circumstances (such as with the approval of a senior staff member, or where the value of the item(s) did not exceed a certain threshold), unless the requesting individual provided:

    a. adequate proof of purchase; and

    b. photo identification for sighting, recording and, where appropriate, checking against the details of individuals have previously requested refunds.

118. The efficacy of this method could be increased in combination with other methods, such as those described above at paragraph [114], and by training its staff to be alive to the suspicious circumstances outlined at points [a] to [c] of paragraph [19], and could be backstopped with [Redacted].

119. The respondent submitted that the adverse effects of adopting such an alternative approach on the 'customer experience' is a relevant factor as to whether there were alternatives available to the respondent to address refund fraud. I agree this is a relevant factor, but I do not accept that it renders the alternative impracticable or ineffective.

120. Further, from 1 August 2024, the respondent updated its Returns Policy to require adequate proof of purchase for eligible 'change of mind' returns.[129] The updated Returns Policy outlines the ways in which:

    a. individuals can demonstrate proof of purchase and verify their identity; and

---

[126] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.18; R2.1.A1 Appendix 1 to R2.1: Answers to the questions in the OAIC notice pp. 12-13.

[127] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.18.

[128] *Competition and Consumer Act 2010* (Cth) sch 2 ('Australian Consumer Law').

[129] Kmart Returns Policy: https://www.kmart.com.au/returns-policy/?srsltid=AfmBOoox_cGicKekxWE_9dapxoA-xOiesTQF0v9KlCehxWyCmG_CtuCg, accessed 21 August 2025.

b. the respondent will handle the personal information it collects for identity verification purposes.[130]

121. Prior to August 2024, the respondent's usual practice was to allow customers to return items based on a change of mind without providing proof of purchase.[131] The then Head of Operations declared that this change to its returns practice was introduced, in part, to mitigate the rate of refund fraud without using the FRT system. She further declared that the respondent's decision to require proof of purchase for change of mind returns has led to a significant rise in customers behaving in an aggressive, abusive, or threatening manner in the context of requesting a refund.[132] I do not wish to diminish the impact of such behaviours on the respondent and its staff. However, I note that irrespective of what method staff use to respond to refund fraud, including via the FRT system, there is the possibility it may lead to difficult interactions with some customers.

122. The respondent has referred to its legal obligations with respect to its employees and entrants to its premises. The focus of my consideration is limited to the Privacy Act. Generally, however, I consider that the introduction of new or changed refund fraud prevention strategies should be complemented with revised controls to address any risks to staff safety, or at minimum, consideration as to whether revised controls are necessary.[133] Moreover, implementing strategies that minimise the opportunity for refund fraud, such as outward facing returns counters, are likely to be more supportive of staff safety, given that it reduces their role in detecting refund fraud and declining refunds.

123. The then Head of Operations provided her assessment that, despite the change to the respondent's returns practice, and that the respondent 'has no practical means of detecting and quantifying Retail Fraud without FRT', she believes that retail fraud is:

> *[Redacted]. The change to [the respondent's] return practice does not combat Refund Fraud to the same degree as I expect FRT would if Kmart could continue using FRT and expand its use across the network'.*[134]

124. While I appreciate there may be gaps in the utility of a refund policy that relies on proof of purchase and identification, including with respect to [Redacted], there are similarly gaps within the FRT system in identifying and thus preventing refund fraud, as discussed in my analysis with respect to the suitability of the FRT system. As noted at paragraph [118], a combination of methods, or complementary strategies, may increase efficacy in addressing refund fraud.

125. Additionally, I do not have evidence before me that indicates an assessment of potential alternatives to the FRT system took place, other than the 'compelling lived experience of its senior management'.[135] There is no evidence, for example, of project planning documents or a privacy impact assessment having been conducted prior to the implementation of the FRT pilot program, that demonstrates the respondent

---

[130] Kmart Returns Policy: https://www.kmart.com.au/returns-policy/?srsltid=AfmBOoox_cGicKekxWE_9dapxoA-xOiesTQF0v9KlCehxWyCmG_CtuCg, accessed 21 August 2025.

[131] R4.2 – Witness Statement – Respondent's General Manager Central Operations and Safety dated 30 April 2025 p.2.

[132] R4.2 – Witness Statement – Respondent's General Manager Central Operations and Safety dated 30 April 2025 p.7.

[133] For example, Preventing workplace violence and aggression guide | Safe Work Australia, Appendix A - Industry hazards and control measures, see 'Retail and hospitality' pp.19-20.

[134] R4.2 – Witness Statement – Respondent's General Manager Central Operations and Safety dated 30 April 2025 p.7.

[135] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 p.20.

considered other, less privacy intrusive, options to minimise the risk of refund fraud and the basis upon which alternatives were considered to be ineffective or not viable.

126. Relevant to my consideration on alternatives to the FRT system is evidence that that the respondent was required by its own policies to consider 'relative benefits and risks when compared to other reasonable alternatives ...'[136] and that it had not done so as required by the Minimum Standards. The respondent provided the OAIC with 'Facial Recognition Technology: Compliance Plan Checklists' (**Compliance Checklists**) completed by its staff during the relevant period, which included an item described as 'benefits and risks compared to other alternatives'.[137] This was linked to a framework which relevantly stated:

> *'Consider the relative benefits and risks when compared to other reasonable alternatives, developments in the underlying technology and processes, stakeholder views including of customers, team members and regulators, and any relevant business specific matters.'*[138]

127. While the Compliance Checklists indicated that the respondent's loss prevention team was responsible for this item, the progress notes indicated that the previous loss prevention team 'did not hand over any assessments'.[139] However, it was noted in the completed Compliance Checklists that 'an assessment has been scheduled into the CCTV tender that will occur in early to mid-2022.'[140] I do not have any evidence available to me that supports a conclusion that that assessment, considering the relative benefits and risks of the FRT system compared to other reasonable alternatives, took place.

128. The FRT system may have been an effective and convenient tool available to the respondent to detect and prevent refund fraud. In my view, this was not of itself sufficient to induce a reasonable belief that collecting the sensitive information of every individual that entered the store via the FRT system was necessary to take appropriate action in relation to refund fraud, in circumstances where alternative methods were available to the respondent and were insufficiently explored.

Proportionality

129. The objects of the Privacy Act recognise the rights of individuals and the interests of entities, and the need to appropriately balance such rights and interests where they may be in conflict.[141] I have therefore considered, for the purposes of assessing the reasonableness of the respondent's belief in respect of necessity, whether the collection of personal information via the FRT system was proportionate to the benefit gained from its use.

---

[136] R1.1.A10 – Appendix 10 to R1.1: Wesfarmers Minimum Standards for the use of FRT dated 3 September 2020 p.2.

[137] R2.1.A4.1 - Appendix 4.1 to R2.1: FRT compliance plan checklist dated September 2021; R2.1.A4.2 - Appendix 4.2 to R2.1: FRT compliance plan checklist dated October 2021; R2.1.A4.3 – Appendix 4.3 to R2.1: FRT compliance plan checklist dated November 2021; R2.1.A4.4 – Appendix 4.4 to R2.1: FRT compliance plan checklist dated March 2022; R2.1.A4.5 - Appendix 4.5 to R2.1: FRT compliance plan checklist dated June 2022.

[138] R2.1.A4.1 – R2.1.A4.5 – Appendices to R2.1: 'FRT compliance plan checklist' for September 2021, October 2021, November 2021, March 2022 and June 2022 pp.1-2.

[139] R2.1.A4.1 – R2.1.A4.5 – Appendices to R2.1: 'FRT compliance plan checklist' for September 2021, October 2021, November 2021, March 2022 and June 2022 pp.1-2.

[140] R2.1.A4.1 – R2.1.A4.5 – Appendices to R2.1: 'FRT compliance plan checklist' for September 2021, October 2021, November 2021, March 2022 and June 2022 pp.1-2.

[141] *Privacy Act 1988* (Cth) s 2A(1).

130. The FRT system involved capturing and processing the facial images of every individual who entered a relevant store during the relevant period, regardless of their age, appearance, demeanour or intentions, and comparing the metadata generated from those facial images against other metadata as part of the matching process. Each collection of sensitive information from every individual who entered the relevant stores during the relevant period – potentially tens or even hundreds of thousands of individuals over the relevant period – impacts upon the privacy of the respective individual.

131. The respondent submitted that the interference with individuals' privacy was limited, due to a range of relevant factors as to the nature of the collection, such as the length of time the information was retained for, the steps taken to secure the information, and the likelihood of harm arising from the privacy interference.[142] It submitted that, due to those features of the collection, it was not 'disproportionate'.

132. I reiterate however that the sensitive information of every customer who entered a relevant store was indiscriminately collected by the FRT system. More generally, the potential harms generally arising from the use of FRT are significant, and include the risk of commercial surveillance, discrimination, unlawful and arbitrary arrest, and inequality before the law.[143] I note as well the impacts on enrolled individuals, including in circumstances where they had not engaged in the conduct they were suspected of.

133. I have earlier, at paragraphs [100] to [102], had regard to the figures and estimations provided by the respondent, concerning the extent of refund fraud at the respondent's stores as applicable to the 2020 financial year and the suspected fraudulent incidents identified using the FRT system. As I previously noted, the number of fraudulent incidents detected using the FRT system, and the value of fraud prevented by using that system, was small, including in comparison to the estimated value of the unlawful activity. The value of the fraud prevented by the FRT system is also minimal with respect to the respondent's annual revenue, which was $9.2 billion in the 2020 financial year.[144]

134. I appreciate the respondent was experiencing [Redacted] at the time of implementing the FRT pilot program and that the then Head of Operations believed that refund fraud was materially contributing to this problem.[145] I have previously considered the scale of refund fraud with respect to the respondent, based on estimations it has provided, in the context of returns made with no proof of purchase. I have calculated the estimated value of fraudulent, or likely fraudulent returns, in these circumstances as amounting to approximately [Redacted] in 2020.[146] This amounts to approximately [Redacted] per cent of the respondent's revenue in the 2020 financial year.

135. I acknowledge that the figures with respect to the relative effectiveness of the FRT system are only available retrospectively, that is, following the implementation of the FRT system. However, given that the FRT system was intended to address only a subset of refund fraud, and its practical limitations in detecting that subset in all circumstances, I am of the view that the respondent could not have reasonably believed that the collection of sensitive information via the FRT system was a proportionate measure. This is particularly so in light of the impact on the privacy of the many

[142] R4.1 – Respondent's submissions in response to the preliminary view dated 30 April 2025 pp.19-20.
[143] Australian Human Rights Commission, Human Rights and Technology – Discussion paper, December 2019.
[144] Wesfarmers Annual Report 2020 p.7.
[145] R4.2 – Witness Statement – Respondent's General Manager Central Operations and Safety dated 30 April 2025 p.5.
[146] See paragraph [102].

thousands of individuals not suspected of refund fraud. Notably, the respondent collected the sensitive information of every customer who entered one of the relevant stores where the respondent was operating the FRT system with a view to detecting fraudulent returns perpetuated by a far smaller cohort of individuals.

136. As I discussed at paragraph [103], I appreciate that the FRT system was implemented as a pilot program in a limited number of the respondent's stores and its full potential may not have been realised during the relevant period. However, I do not consider that the respondent could have reasonably believed that the benefits of the FRT system in addressing refund fraud proportionately outweighed the impact on individuals' privacy having regard to the considerations discussed above. These factors are the estimated value of fraudulent returns against the broader sale of the respondent's operations and profits, the limits in the effectiveness of the FRT system, and the privacy impacts in collecting the sensitive information of every individual who entered the relevant stores.

137. Consequently, I am not satisfied that the respondent could have reasonably believed that the collection of personal and sensitive information via the FRT system was necessary to take appropriate action in relation to refund fraud. To find otherwise would arguably undermine the objects of the Privacy Act which seek to balance the rights of individuals and the interests of entities.

Conclusion

138. On the information available to me, I am not satisfied that a permitted general situation existed in respect of Item 2 because I am not satisfied that the requirements of Condition (b) were met.

Finding – APP 3.3

139. I find that the respondent collected the sensitive information of all individuals who entered a relevant store during the relevant period in circumstances where those individuals did not consent to the collection of the information and subclause 3.4 did not apply in relation to the information. I therefore find that the respondent breached APP 3.3.

APP 5 – Notification of the collection of personal information

140. APP 5.1 states that at or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

    a. to notify the individual of such matters referred to in subclause [APP] 5.2 as are reasonable in the circumstances; or

    b. to otherwise ensure that the individual is aware of any such matters.[147]

141. APP 5 is intended to ensure that an individual is aware of certain matters when an APP entity collects their personal information.[148] This includes, but is not limited to, an individual being made aware of how and why personal information is or will be collected and how the entity will handle that personal information.[149]

142. The respondent submitted that it complied with its obligations under APP 5.1 because:

---

[147] APP 5.1.
[148] Explanatory Memorandum – *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth) [79].
[149] Explanatory Memorandum – *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth) [79].

a. it did not collect the personal information of 'unmatched' individuals because those individuals were not reasonably identifiable. Therefore, no notice was required; and

b. in respect of 'matched' individuals, it was not reasonable in the circumstances to notify those individuals of the APP 5.2 matters.[150]

143. In any event, the respondent considers that it took reasonable steps in the circumstances to notify or otherwise ensure that individuals who entered the relevant stores were aware of the APP 5.2 matters via its 'layered' approach to notification.[151] The respondent considers that the notices it displayed at the entry point to its stores and its privacy policies complied with APP 5.1.[152] In its submissions, the respondent relied upon the APP Guidelines which state:

> '*An individual may be notified or made aware of APP 5 matters through a variety of formats, provided the matters are expressed clearly…A notice may also be provided in layers…*'[153]

144. As outlined in respect of APP 3 above, I am of the view that the respondent collected personal information, including sensitive information, within the meaning of the Privacy Act via its use of the FRT system for all individuals who entered the relevant stores. Therefore, the respondent had an obligation to take such steps, if any, as were reasonable in the circumstances to notify or otherwise ensure those individuals were aware of the matters in APP 5.2.

Was it reasonable in the circumstances for the respondent to take steps to notify or otherwise ensure individuals were aware of the APP 5.2 matters?

145. The obligation under APP 5.1 to take such steps, if any, as are reasonable in the circumstances to notify or ensure individuals are aware of the APP 5.2 matters, is an objective test that is informed by the circumstances of each case.[154]

Circumstances

146. I am of the view that the following circumstances are relevant to my assessment of whether it was reasonable for the respondent to take any steps to notify or ensure individuals were aware of some or all of the APP 5.2 matters:

a. **Nature of the entity** – The respondent is a large retailer that operated between 214 and 303 stores in Australia during the relevant period.[155] It made approximately $9.9 billion in revenue in the 2020-2021 financial year[156] and $9.6 billion in revenue in the 2021-2022 financial year.[157]

b. **Numbers of individuals affected** – The respondent collected the personal information of all individuals who entered the 28 relevant stores during the relevant period. While the respondent does not have a record of the number of individuals that entered the relevant stores,[158] a conservative estimate would likely

[150] R2.1 – Attachment to R2: Letter from the respondent to the OAIC dated 7 October 2022 p.3.
[151] R1.1.A.1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.15.
[152] R1.1.A.1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.13.
[153] APP Guidelines [5.5].
[154] APP Guidelines [B.111].
[155] R2.1.A1 – Appendix 1 to R2.1: Answers to the question in the OAIC notice p.2.
[156] Wesfarmers Annual Report 2021 p.9.
[157] Wesfarmers Annual Report 2022 p.9.
[158] R2.1.A1 – Appendix 1 to R2.1: Answers to the question in the OAIC notice p.2.

be tens of thousands of individuals noting the indiscriminate nature of the FRT system.

c. **Amount of personal information collected and used** – The relevant period for one store was approximately 24 months, while the remaining stores were between approximately 7 to 12 months. Individuals who entered the relevant stores had 5 to 6 real time facial images collected at two separate collection points, together with metadata. Therefore, the personal information and sensitive information of tens of thousands of individuals was collected throughout the relevant period and likely on multiple occasions.

d. **Length of time personal information was held** – The facial images and metadata of all individuals was retained for [Redacted] to [Redacted] on the History Database. For enrolled individuals on the Enrolment Database, the period varied from [Redacted] to [Redacted].

e. **Type of personal information** – As outlined above, I consider that the FRT system involved the collection of personal information that was also sensitive information, which is afforded a higher level of protection under the Privacy Act.

f. **Consequences of use** – For individuals who entered the relevant store and did not approach the Returns Counter, the consequences were that their personal information was collected without their knowledge or consent and used to generate metadata which was compared against the metadata associated with other individuals as part of the matching process. For individuals who approached the Returns Counter, the consequences extended to additional scrutiny and review by the respondent's staff, particularly if any suspicious circumstances applied. Those individuals would be the subject of a matching process, their information retrieved and viewed by the respondent's staff members via the MRD system and may have had their refund refused. For enrolled individuals on the Enrolment Database, the consequences included that they lost the opportunity to consent to the collection and retention of their sensitive information, particularly where they may not have actually engaged in the conduct they were suspected of. I also note that these consequences may have been exacerbated depending on the circumstances of the individual, including their race, citizenship, gender and vulnerabilities.

g. **Nature of technology** – At the time the respondent implemented the FRT system, FRT appears to have been a relatively novel technology in a retail setting and involved ways of collecting personal information that differed from what individuals entering the relevant stores were otherwise accustomed to or might have expected.

h. **Practicability** – The respondent had the opportunity to engage with individuals who entered the relevant stores at or immediately prior to the point of entry, and again if an individual presented to a Returns Counter. Therefore, it was not impracticable to take steps under APP 5.1.

147. In view of the circumstances outlined at paragraph [146], I am of the view that it was reasonable for the respondent to take steps to notify or otherwise ensure that individuals were aware of some or all of the APP 5.2 matters. I consider that it would not have been reasonable for the respondent to take no steps to notify individuals who entered the relevant stores that their personal information was being collected by the respondent via the FRT system.

APP 5.2 matters

148. I have considered which of the APP 5.2 matters the respondent could have reasonably notified or ensured individuals were aware of in the circumstances. I consider that it was reasonable in the circumstances for the respondent to take steps to notify or otherwise ensure individuals were aware of, at a minimum, the following APP 5.2 matters:

    a. **APP 5.2(b)** – the fact that the respondent was collecting individuals' personal information via the FRT system and the circumstances of that collection;

    b. **APP 5.2(d)** – that the purpose for which the respondent was collecting individuals' personal information was to detect and prevent the occurrence of fraudulent refunds;

    c. **APP 5.2(e)** – the consequences for an individual if all or some of their personal information was not collected by the respondent, for example being denied entry into its stores or being denied a refund; and

    d. **APP 5.2(g)** – that the respondent's privacy policy contained information about how individuals could access the personal information about them held by the respondent and seek the correction of that information.

What steps did the respondent take to notify or ensure that individuals were aware of the APP 5.2 matters?

Conditions of Entry Notice

149. During the relevant period, the respondent displayed an 'updated' Conditions of Entry Notice (**Entry Notice**) at the entry point of relevant stores[159] which stated:

    'This store has 24-hour CCTV coverage, which includes facial recognition technology.'[160]

150. While the respondent submitted that the Entry Notice was implemented at the entry point to all relevant stores during 2021, it was unable to confirm the actual date upon which the Entry Notice commenced display at the entrance of relevant stores.[161]

151. The respondent noted that on 7 October 2021, communications were sent to the relevant stores instructing the replacement of store signage with the Entry Notice referenced at paragraph [149].

152. Further, the respondent assessed its use of the FRT system against the Minimum Standards, which included an assessment of privacy issues.[162] These assessments were completed by the respondent periodically from September 2021 and documented in its Compliance Checklists.[163]

153. The respondent's Compliance Checklists refer to 'Facial Recognition Technology customer notices' as a requirement of the Minimum Standards and specify the parameters for compliance with the framework, which are that:

    'The division must be transparent about its use of the Facial Identification system. This includes providing clear notices for customers in-store (such as at entrances or service

---

[159] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice pp.13 and 16.
[160] R1.1.A9 – Appendix 9 to R1.1: Location and position of respondent's conditions of entry store signage; R1.1.A8 – Appendix 8 to R1.1: Respondent's conditions of entry store signage p.1.
[161] R2.1.A1 – Appendix 1 to R2.1: Answers to the questions in the OAIC notice p.6.
[162] R2.1.A1 – Appendix 1 to R2.1: Answers to the questions in the OAIC notice p.13.
[163] R2.1.A1 – Appendix 1 to R2.1: Answers to the questions in the OAIC notice p.13; R2.1.A4.1 – Appendix 4.1 to R2.1: FRT compliance plan checklist dated September 2021.

desks) and in its privacy policy that facial recognition technology is being used, the purpose(s) for which it is being used and which third parties may be provided with that data. The division must provide similar confirmation in response to a request by a customer or other key stakeholder and have appropriate processes in place to deal with any requests for a review or complaints.'[164]

154. According to the respondent's September 2021 Compliance Checklist, it assessed itself as being non-compliant with the Minimum Standards for notice in the following respects:

    a. no notice provided in current test sites advising on FRT use; and

    b. no processes defined or documented for managing requests to review facial identification and managing complaints related to facial identification.[165]

155. The progress notes in the respondent's September 2021 Compliance Checklist noted remedial action was required which included:

    a. incorporating wording into current CCTV signage; and

    b. 'add into Privacy compliance program – EA' managing requests to review facial identification and managing complaints relating to facial identification.[166]

156. In October 2021, the Compliance Checklist was updated and noted that the 'current conditions of entry sign have been updated to include FRT'.[167] However, the deficiency identified at paragraph [155.b] remained outstanding until approximately March 2022.[168] Similarly, the November 2021 iteration of the respondent's FRT Guide indicated that signage had not yet been implemented in relevant stores.[169]

157. The FRT system was operational in 5 relevant stores before October 2021.[170] Of note, the FRT system had been in place in 1 relevant store since 22 June 2020, a period of approximately 15 months.[171] On balance, it is unlikely that the Entry Notice was displayed at these 5 stores at the time the FRT system was already operating. Therefore, a reasonable inference can be made that the individuals who entered those stores prior to October 2021 would not have known or been made aware that the FRT system was operating, let alone that their sensitive information was being collected by the respondent, the purpose of that collection and the ways in which the respondent would use or disclose their information.

158. This assessment is supported by the fact that the respondent's FRT Guide explicitly stated that 'under no circumstances should any Team Members disclose or advise customer on the use of this technology'.[172]

---

[164] R2.1.A4.1 – Appendix 4.1 to R2.1: FRT compliance plan checklist dated September 2021 pp.7-8, item 3b; R2.1.A4.2 – Appendix 4.2 to R2.1: FRT compliance plan checklist dated October 2021 pp.7-8, item 3b; R2.1.A4.3 – Appendix 4.3 to R2.1: FRT compliance plan checklist dated November 2021 pp.7-8, item 3b.

[165] R2.1.A4.1 – Appendix 4.1 to R2.1: FRT compliance plan checklist dated September 2021 pp.7-8, item 3b.

[166] R2.1.A4.1 – Appendix 4.1 to R2.1: FRT compliance plan checklist dated September 2021 pp.7-8, item 3b.

[167] R2.1.A4.2 – Appendix 4.2 to R2.1: FRT compliance plan checklist dated October 2021 pp.7-8, item 3b.

[168] R2.1.A4.4 – Appendix 4.4 to R2.1: FRT compliance plan checklist dated March 2022 pp.7-8, item 3b.

[169] R1.1.A7.1 – Appendix 7.1 to R1.1: ShrinK 365: FRT Guide dated November 2021 p.14.

[170] R1.1.A3 – Appendix 3 to R1.1: List of FRT stores.

[171] R1.1.A3 – Appendix 3 to R1.1: List of FRT stores.

[172] R1.1.A7.1 – Appendix 7.1 to R1.1: ShrinK 365: FRT Guide dated November 2021 p.14; R1.1.A7.2 - Appendix 7.2 to R1.1: ShrinK 365: FRT National Office Guide dated April 2022 p.18.

Privacy Poster

159. The respondent submitted that at certain stores it also displayed a privacy poster at entry points which directed customers to its privacy policy on its website and stated:[173]

> ***'Privacy***
>
> *Kmart is committed to protecting your privacy.*
>
> *You may be asked for personal information for a variety of reasons such as seeking a refund without a receipt, store delivery services or providing feedback.*
>
> *Any personal information collected will only be used for the purposes it was provided unless you have agreed to otherwise. Kmart will handle your personal information securely and carefully.*
>
> *To view details of the Kmart privacy policy.*
>
> *(Including how to request access your personal information we hold)*
>
> *Please visit www.kmart.com.au or contact our customer service Centre on [phone numbers indicated].'*[174]

160. The respondent submitted that the privacy poster was implemented at the relevant stores during the relevant period. For all relevant stores, except one, the privacy poster was 'confirmed in place' between 15 November to 22 December 2021. That is, the date in which a LP Partner of the respondent confirmed that the privacy poster was in effect, which the respondent anticipates that in most or all cases was later than the actual date it was installed. The privacy poster was in effect in the relevant stores until at least 15 July 2022, being the date in which the respondent paused its use of the FRT system.[175]

Privacy Policy

161. The respondent relied on its privacy policy, three iterations of which were in force during the relevant period and available on its website, to support its argument that it used a layered approach to notification under APP 5.1.[176] These privacy policies were effective during the following periods: [177]

    a. **Privacy policy 1** – 2018 and November 2021[178]

    b. **Privacy policy 2** – November 2021 and May 2022[179]

    c. **Privacy policy 3** – May 2022 and 15 July 2022[180]

162. Privacy policy 1 does not expressly or impliedly refer to the respondent's use of FRT to collect individuals' personal information, including metadata and biometric information, nor did the policy provide any information which would address any of the other APP 5.2 matters in relation to the respondent's use of FRT.[181] Instead, the policy

---

[173] R2.1.A1 – Appendix 1 to R2.1: Answers to the questions in the OAIC notice p.5.
[174] R1.1.A8 – Appendix 8 to R1.1: Respondent's conditions of entry store signage p.2; R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.13.
[175] R3.1 – Letter from the respondent to the OAIC dated 10 April 2025 pp.4-6.
[176] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice pp.12 and 16.
[177] R1.1.A1 – Appendix 1 to R1.1: Answers to the questions in the OAIC notice p.12.
[178] R1.1.A11.1 – Appendix 11.1 to R1.1: Respondent's privacy policy dated 2018 – November 2021.
[179] R1.1.A11.2 – Appendix 11.2 to R1.1: Respondent's privacy policy dated November 2021 – May 2022.
[180] R1.1.A11.3 – Appendix 11.3 to R1.1: Respondent's privacy policy dated May 2022 – 15 July 2022.
[181] R1.1.A11.1 – Appendix 11.1 to R1.1: Respondent's privacy policy dated 2018 – November 2021.

broadly stated that the respondent collected and used information to 'protect against fraud and theft'.[182]

163. By contrast, privacy policies 2 and 3 state that the respondent may collect individuals' personal information including 'images from facial recognition software' which it may use for 'loss prevention and store safety purposes'.[183] Both policies also provided that the respondent may disclose personal information to 'third parties necessary to assist [it] in investigating and preventing any potential, suspected or actual breaches of policy or law, fraudulent activities, loss prevention activities'.[184]

164. Prior to November 2021, 10 relevant stores were operating the FRT system, with a further 11 relevant stores commencing operation of the FRT system in November 2021.[185] Accordingly, individuals who entered those stores prior to November 2021 would not have knowledge or been made aware of the respondent's use of FRT, even if they viewed the respondent's privacy policy.

What steps would have been reasonable in the circumstances to comply with APP 5.1?

165. In the circumstances, I am of the view that it would have been reasonable for the respondent to have, at a minimum, taken steps to clearly and explicitly address APP 5.2(b), (d), (e) and (g) in physical notices that were prominently displayed at both the entry points and Returns Counter of the relevant stores for the entire duration of the relevant period, in sufficient size and in an accessible format, that enabled individuals to be notified or otherwise made aware of the APP 5.2 matters. Those notices should have directed individuals to more detailed information about the respondent's use of the FRT system, which could have been made available on its website and addressed those APP 5.2 matters.

Were the steps taken by the respondent to notify individuals of APP 5.2 matters reasonable in the circumstances?

166. I am of the view that the steps taken by the respondent, as outlined at paragraphs [149] – [164], were not reasonable in the circumstances because:

a. they did not, at a minimum, adequately notify individuals of the matters in APP 5.2(b), (d), (e) and (g). Accordingly, individuals who entered the relevant stores in which FRT was operating would have had little to no knowledge that their personal information was being collected at both the point of entry and at the Returns Counter via the FRT system;

b. they were not in effect for the entire relevant period, such that there was a period of time at least prior to October 2021 in which no notice of the matters in APP 5.2(b), (d), (e) and (g) was provided to individuals relating to the respondent's use of FRT; and

c. the respondent failed to display signage that adequately notified or ensured individuals who presented to the Returns Counter of a relevant store had

[182] R1.1.A11.1 – Appendix 11.1 to R1.1: Respondent's privacy policy dated 2018 – November 2021 p.3.
[183] R1.1.A11.2 – Appendix 11.2 to R1.1: Respondent's privacy policy dated November 2021 – May 2022 pp.2 and 4; R1.1.A11.3 – Appendix 11.3 to R1.1: Respondent's privacy policy dated May 2022 – 15 July 2022 pp.2 and 3.
[184] R1.1.A11.2 – Appendix 11.2 to R1.1: Respondent's privacy policy dated November 2021 – May 2022 p.4; R1.1.A11.3 – Appendix 11.3 to R1.1: Respondent's privacy policy dated May 2022 – 15 July 2022 p.3.
[185] R1.1.A3 – Appendix 3 to R1.1: List of FRT stores.

knowledge or were otherwise aware that their personal information was being collected via the FRT system.

Entry Notice and Privacy Poster

167. I am not satisfied that the Entry Notice and privacy poster displayed at the entry points to the relevant stores discharged the respondent of its APP 5.1 obligations because:

    a. stating that 'this store has 24-hour CCTV coverage, which includes facial recognition technology' does not adequately notify or otherwise ensure individuals were aware that their personal information was being collected, as required by APP 5.2(b);

    b. the respondent did not specify that the purpose for which individuals' personal information was being collected was to prevent and detect refund fraud, as required by APP 5.2(d);

    c. the respondent did not notify or ensure individuals were aware of the consequences if all or some of their personal information was not collected, as required by APP 5.2(e); and

    d. the respondent did not specify that its privacy policy contained information about how individuals could access the personal information that was held about them by the respondent for at least [Redacted] to [Redacted], or [Redacted] to [Redacted] in the case of enrolled individuals, and how those individuals could seek the correction of that information as required by APP 5.2(g).

168. Even if I were minded to accept that the Entry Notice discharged the respondent of its obligations under APP 5.1, which I do not consider to be the case, it is clear that there was a period of time before 7 October 2021 in which the FRT system was operating in a number of relevant stores and no in store notice was provided. Similarly, the respondent failed to display any in store signage at the Returns Counter where it collected individuals' facial images and metadata.

169. While the respondent stated it displayed the privacy poster at the relevant stores, it appears that the date in which it was 'confirmed in place' at some stores post-dated the time in which the FRT system was already operating. Irrespective, the privacy poster makes no mention of the respondent's collection of personal information through the use of the FRT system. Therefore, I am of the view that the respondent failed to notify or otherwise ensure individuals were aware of the APP 5.2 matters.

Privacy Policy

170. I have also considered whether the Entry Notice and privacy poster, when combined with the various iterations of the respondent's privacy policy that was in effect during the relevant period, sufficiently notified individuals of APP 5.2(b), (d), (e) and (g) through a 'layered' approach.

171. Privacy policy 1 failed to notify individuals that the respondent collected individuals' facial images and metadata upon entry to the store and at the Returns Counters via the FRT system, and the purpose of that collection.

172. Privacy policy 1 was in effect for approximately 17 months of the relevant period, until November 2021.[186] By that time, the FRT system had already been operating in at least 10 stores.[187]Accordingly, for at least 17 months, individuals who entered the relevant stores would not have been notified or made aware of the APP 5.2 matters as it pertained to the respondent's use of FRT.

173. Even if the respondent's privacy policy had included the relevant APP 5.2 matters, as stated by the Commissioner in *'ABR' and Civil Aviation Safety Authority (Privacy)*:

> *'the publication of a privacy policy, being a transparency mechanism and a separate obligation under the Privacy Act, is not generally, on its own, a way of complying with APP 5.'*[188]
>
> *'It is preferable for an APP entity to set out, or otherwise ensure awareness, of all the APP 5.2 matters at the point of the specific collection unless it is unreasonable to do so, rather than to rely on its APP privacy policy.'*[189]

174. There does not appear to be any reason why it was not practicable for the respondent to take steps to inform individuals of the APP 5.2 matters at the point of collection as they entered a relevant store and presented to the Returns Counters.

175. I am of the view that a reasonable person can understand, if notified, that the respondent takes images of their face in one location of a store, generates data from those images, and holds them in a database to recognise their face in another part of the store. A reasonable person can understand, if notified, that the respondent keeps a record of their facial image and biometric information (and other personal information) in the Enrolment Database for future data matching if they are suspected of refund fraud.

Finding

176. I find that the respondent breached APP 5.1, and therefore interfered with the privacy of individuals, by failing to take such steps as were reasonable in the circumstances to notify those individuals whose personal information it collected through its FRT system during the relevant period about the matters in APP 5.2(b), (d), (e) and (g).

APP 1.3 – APP Privacy Policy

177. APP 1.3 requires an APP entity to have a clearly expressed and up-to-date privacy policy about the management of personal information by the entity. The APP privacy policy must contain the information set out in APP 1.4 which includes, amongst other things:

    a. the kinds of personal information the entity collects and holds; and

    b. how the entity collects and holds personal information.

[186] The figure of 17 months is based on the period of June 2020 to November 2021. That is, the respondent commenced operating the FRT system in its first store in June 2020, and privacy policy 1 ceased effect as of November 2021.

[187] R1.1.A3 – Appendix 3 to R1.1: List of FRT stores.

[188] *'ABR' and Civil Aviation Safety Authority (Privacy)* [2022] AICmr53 (24 June 2022), [63].

[189] *'ABR' and Civil Aviation Safety Authority (Privacy)* [2022] AICmr53 (24 June 2022), [107].

178. As outlined at paragraph [161], the respondent had three privacy policies in place during the relevant period.[190]

179. Between 2018 and November 2021, privacy policy 1 made no mention of the use of the FRT system. In particular, privacy policy 1 did not include:

    a. the fact that the respondent collected and held the facial images, metadata and biometric information of all individuals who entered the relevant stores, as required by APP 1.4(a); and

    b. how the respondent collected and held that personal information, including by using CCTV cameras to capture real time facial images, which were analysed and processed in the FRT system to create metadata and biometric information, as required by APP 1.4(b).

180. Although privacy policy 1 broadly stated that the purpose for which the respondent collected personal information was to 'protect against fraud and theft',[191] it failed to specify that it was to detect and prevent refund fraud via the FRT system. I am of the view that including those details would have led to greater transparency. Nonetheless, I am inclined to accept that the information required by APP 1.4(c), being the 'purpose' for which the respondent collected, held, used and disclosed personal information was addressed in privacy policy 1.

181. Between November 2021 to July 2022, the respondent implemented privacy policies 2 and 3, which referred to the collection of the following kinds of personal information:

    a. '*images from video surveillance, body cameras and other cameras used in and around our stores (including in car parks, pick up areas, store entrances and publicly accessible spaces)*'; and

    b. *'images from facial recognition software'*.[192]

182. While privacy policies 2 and 3 specified some of the kinds of personal information that was collected by the FRT system, the policies failed to inform individuals that the collection involved the generation of additional information from such facial images, specifically metadata, and that this constitutes individuals' biometric information, being their sensitive information. As a result, I am of the view that the respondent failed to stipulate the 'kinds' of personal information it collected and held. As such, I am not satisfied that the respondent has included the information required by APP 1.4(a).

183. Privacy policies 2 and 3 also specified that the respondent collected personal information '…through our security cameras, body cameras or other cameras used in our stores (including in car parks, pick up areas, store entrances and publicly accessible areas)'.[193]

184. Although the privacy policies articulate that personal information is collected through cameras, it failed to articulate, even in generic terms, the fact that such personal information was collected via the FRT system. Consequently, the respondent has failed to include the information required by APP 1.4(b).

---

[190] R1.1.A11.1 – Appendix 11.1 to R1.1: Respondent's privacy policy dated 2018 – November 2021; R1.1.A11.2 – Appendix 11.2 to R1.1: Respondent's privacy policy dated November 2021 – May 2022; R1.1.A11.3 – Appendix 11.3 to R1.1: Respondent's privacy policy dated May 2022 – 15 July 2022.

[191] R1.1.A11.1 – Appendix 11.1 to R1.1: Respondent's privacy policy dated 2018 – November 2021 p.3.

[192] R1.1.A11.2 – Appendix 11.2 to R1.1: Respondent's privacy policy dated November 2021 – May 2022 p.2; R1.1.A11.3 – Appendix 11.3 to R1.1: Respondent's privacy policy dated May 2022 – 15 July 2022 p.2.

[193] R1.1.A11.2 – Appendix 11.2 to R1.1: Respondent's privacy policy dated November 2021 – May 2022 p.2; R1.1.A11.3 – Appendix 11.3 to R1.1: Respondent's privacy policy dated May 2022 – 15 July 2022 p.2.

Finding

185. I find that during the relevant period, the respondent failed to include in its privacy policies information about the kinds of personal information that it collected and held, and how it collected and held that personal information, as required by APP 1.4(a) and 1.4(b). Therefore, I find that the respondent did not have a clearly expressed and up-to-date APP privacy policy which contained the information required by APP 1.4 and as a result, breached APP 1.3.

Declarations

186. As I have found that the respondent interfered with the privacy of individuals, I have a discretion under s 52(1A) of the Privacy Act to make one or more declarations. Consequently, I have made declarations at paragraph [3] of this determination.

Carly Kind
Privacy Commissioner

26 August 2025

Review rights

Section 96 of the *Privacy Act 1988* (Cth) states that a party may make an application to the Administrative Review Tribunal (**ART**) to have a decision under s 52(1) or (1A) to make a determination reviewed. The ART provides independent merits review of administrative decisions and has power to set aside, vary, or affirm a privacy determination. An application to the ART must be made within 28 days after the day on which the person is given the privacy determination (s 18(1) of the *Administrative Review Tribunal Act 2024* (Cth); r 5(3) of the *Administrative Review Tribunal Rules 2024* (Cth)). An application fee may be payable when lodging an application for review to the ART. Further information is available on the ART's website (art.gov.au) or by telephoning 1800 228 333.

A party may also apply under s 5 of the *Administrative Decisions (Judicial Review) Act 1977* (Cth) to have the determination reviewed by the Federal Circuit and Family Court of Australia or the Federal Court of Australia. The Court may refer the matter back to the OAIC for further consideration if it finds the Information Commissioner's decision was wrong in law or the Information Commissioner's powers were not exercised properly. An application to the Court must be lodged within 28 days of the date of the determination. An application fee may be payable when lodging an application to the Court. Further information is available at https://www.fcfcoa.gov.au/gfl and www.federalcourt.gov.au/.