Australian Government
Office of the Australian Information Commissioner

'KA' and Commonwealth Bank of Australia Limited [2016] AICmr 80 (25 November 2016)

Determination and reasons for determination of Australian Privacy Commissioner, Timothy Pilgrim

Complainant:	**'KA'**
Respondent:	**Commonwealth Bank of Australia Limited (ACN 123 123 124)**
Decision date:	**25 November 2016**
Application number:	**CP14/03139**
Catchwords:	**Privacy — Privacy Act —National Privacy Principles — *Privacy Act 1988* (Cth) s 52 —NPP 2 —Use or disclosure of personal information— NPP 4 — Date security — Compensation awarded — Non-economic loss — Aggravated damages not awarded**

Contents

Findings

1. Commonwealth Bank of Australia Limited (**the CBA**) interfered with the complainant's privacy by:

    - disclosing her personal information to the principal of a Commonwealth Bank Mortgage Innovation agency (**MIA**) for a purpose other than the primary purpose of collection, in breach of National Privacy Principle (**NPP**) 2.1 of the *Privacy Act 1988* (Cth) (**Privacy Act**), and

    - failing to take reasonable steps under NPP 4.1 to protect her personal information from misuse and loss and from unauthorised access, modification or disclosure.

2. To redress this interference, the CBA shall:

    a) within 6 weeks of this determination issue an apology to the complainant acknowledging its interference with the complainant's privacy

    b) pay the complainant $10,000 for non-economic loss caused by the interference with the complainant's privacy, and

    c) review its information handling policies, particularly with respect to access to customer information where there is an acknowledged, or potential conflict of interests, and report back to me within 6 months about the findings of this review.

Background

3. The complainant is a former employee of an MIA.[1]

[1] The Commonwealth Bank Mortgage Innovation is a licensee/agency business structure where contracted, commission only sales people sell CBA financial products. For further information Commonwealth Bank Mortgage Innovation agencies see: https://www.commbank.com.au/about-us/news/media-releases/2004/251104-news-sales-force.html.

4. The complainant is also a customer of the CBA.

5. In June 2011, the complainant's employment with the MIA was terminated by its principal (**the principal**).

6. The complainant submits that in response to the termination, she took action against the principal in the Fair Work Commission (**FWC**).[2]

7. The complainant alleges that during the FWC proceedings, the principal and two employees of the MIA (**the employees**) improperly accessed her customer profile through the CBA's customer management software 'CommSee'.[3] CommSee enables authorised users to access a single view of the customer: including all accounts the customer holds and the status of recent interactions the customer has had with the Bank.[4]

8. The complainant alleges that the principal and the employees repeatedly accessed her CommSee profile during the FWC proceedings for the purpose of assisting the principal to advance his defence in those proceedings. In particular, she alleges that that the principal accessed her CommSee profile for the purpose of tracking her 'worsening financial position', and this 'not only allowed him to settle the legal matter for a significantly lower sum of money than [the principal] expected but also emotionally wore [the complainant] down and traumatised [the complainant] diminishing [her] will to continue the legal fight.'[5]

9. CommSee maintains a 'Client Access Report' (**access report**) that tracks and records the details of all accesses. CommSee records, on the individual CommSee profile, the date and time of access along with the name and department of the person who obtained access.

10. On 24 October 2011, the complainant advised the CBA she had become aware that the principal had accessed her CommSee profile on at least one occasion.[6] The complainant asked the CBA to provide her with a copy of her access report dating from the date of her termination, June 2011, or alternatively,

---

2 The complainant's complaint dated 1 July 2014. The Fair Work Commission was Fair Work Australia at the time of the complainant's Fair Work matter.

3 The complainant's complaint dated 1 July 2014.

4 Commonwealth Bank, 'Commonwealth Bank rolls out new customer service platform in Tasmania' (Media Release, 13 February 2004) https://www.commbank.com.au/about-us/news/media-releases/2004/130204-news-customer-service-tasmania.html.

5 The complainant's final submissions dated 2 June 2016 – page 22.

6 The complainant's email to the CBA dated 24 October 2011, in which she advised the CBA that the principal had accessed her CommSee profile on 27 September 2011.

assure her that the principal's access was a 'once off'.[7] The complainant advised the CBA she considers that 'a breach of privacy of this nature is extremely serious…'.

11. On 15 November 2011, the CBA responded to the complainant through its Senior Legal Counsel advising her that the access to her CommSee profile 'was done in the normal course of [the principal's] management of [her] (at that time) non-performing loan accounts with the Bank'.[8]

Privacy Complaint and the remedy sought

12. On 2 July 2014, the complainant lodged a complaint against the CBA with the Office of the Australian Information Commissioner (**OAIC**) under s 36 of the Privacy Act.[9]

13. The complainant alleges that the CBA interfered with her privacy by improperly disclosing her personal information to third parties, the principal and the employees, and by not taking reasonable steps to protect her personal information from misuse and loss, and from unauthorised access, modification or disclosure. The complainant contends that the CBA had full knowledge of the FWC proceedings, and in these circumstances the CBA should have blocked the MIA's access to her CommSee profile.[10]

14. On 15 October 2014, the OAIC opened an investigation into the complainant's allegations under s 40(1) of the Privacy Act. The written submissions provided by both the complainant and the CBA have been considered.

15. The matter was not able to be resolved through conciliation and I decided to determine the matter under s 52 of the Privacy Act.

16. Section 52(1) provides that, after investigating the complaint, I may make a determination dismissing the complaint (s 52(1(a)); or finding the complaint substantiated and make a determination that includes one or more of the following declarations:

    (i) that the respondent has engaged in conduct constituting an interference with privacy of an individual and must not repeat or continue such conduct (s 52(1)(b)(i)(B))

---

7 The complainant's email to the CBA dated 24 October 2011.

8 By letter dated 15 November 2011.

9 The complainant's complaint dated 1 July 2014.

10 The substance of the complainant's complaint dated 1 July 2014.

(ii) that the respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant

(iii) that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint (s52(1)(b)(iii))

(iv) it would be inappropriate for any further action to be taken in the matter.

17. The complainant is seeking a declaration by me that the CBA interfered with her privacy, and she is seeking compensation for that interference. She also asks that I impose penalties on the CBA for the interference, and for the CBA providing 'misleading statements and fraudulent/falsified documents' to the OAIC during the complaint investigation.

The Law

18. At the time of the alleged breaches, the NPPs were the standards for handling personal information which private sector organisations subject to the Privacy Act were obliged to uphold. *The Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Privacy Amendment Act), which substantively took effect on 12 March 2014, replaced the NPPs with the Australian Privacy Principles.

19. I have considered the complaint under the provisions of the Privacy Act including the NPPs in effect at the relevant time.

20. Section 13A of the Privacy Act held that an act or practice that breached an NPP in relation to personal information was for the purposes of the Act an interference with the privacy of the individual who the information was about. Section 16A required an organisation not do an act or engage in a practice that breaches the NPPs.

21. Personal information was defined in s 6 of the Privacy Act as:

> ... information or opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion.[11]

[11] 'Personal information' under the post 12 March 2014 regime is defined to mean: 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.

22. The complainant's CommSee profile identifies the complainant. Therefore, it contains information that is about her, and thus it is her personal information for the purposes of s 6 of the Privacy Act.

23. 'Organisation' was defined under s 6C of the Privacy Act to include:

    (a) An individual; or

    (b) A body corporate; or

    (c) A partnership; or

    (d) Any other unincorporated association; or

    (e) A trust

    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.

24. The CBA is a publicly listed corporation; therefore it is an 'organisation' within the meaning of s 6C(b) of the Privacy Act.

25. NPP 2.1 provided that:

    An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:

    …

    (f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities…

26. The term 'use' is not defined in the Privacy Act. However, the *Guidelines to the National Privacy Principles* issued by the then Office of the Federal Privacy Commissioner in September 2001 explain that '…use of personal information refers to the handling of personal information within an organisation'.

27. The guidelines to the APPs, which replaced the NPPs on 12 March 2014, explain that an organisation 'uses' personal information, where, for example, it accesses and reads the personal information.

28. NPP 4 required organisations to take reasonable steps to protect an individual's personal information from misuse and loss and from unauthorised access, modification or disclosure. NPP4 has been replaced

by APP 11 which now imposes similar obligations on organisations to protect personal information under APP 11.1.[12]

Alleged breach of NPP 2

29. The complainant alleges a breach of NPP 2 on the basis that the CBA improperly used and disclosed her personal information to the principal and the employees of the MIA. The complainant contends the CBA cannot rely on any exceptions under the Act.[13]

30. The CBA does not now dispute that it disclosed the complainant's personal information to the principal and the employees, but it contends that the disclosure was not in breach of the NPPs.[14]

31. The CBA had initially contended that only the principal had accessed the complainant's CommSee profile, and during the course of the complaint investigation the CBA had submitted an access report to the OAIC that purported to support that contention.[15]

32. However, during the course of the complaint investigation, the complainant submitted evidence to the OAIC that supported her position that the employees had also accessed her CommSee profile. The complainant's evidence appeared to show that the copy of the access report, as submitted by the CBA, was incomplete.

33. On 13 March 2015, the OAIC sought an explanation from the CBA as to why it had omitted information relevant to the complaint investigation by providing an incomplete access report.

34. On 13 March 2015, the CBA advised the OAIC that an administrative error had occurred while preparing the access report, and parts of the access report were inadvertently missed. The CBA provided a revised copy of the access report. At this time, the CBA also conceded that the employees, in addition to the principal, had in fact accessed the complainant's CommSee profile.

35. The access report[16] records that the principal accessed the complainant's profile on 15 June 2011, 1 July 2011, 4 July 2011, 14 July 2011, 2 August 2011 and 14 September 2011.

---

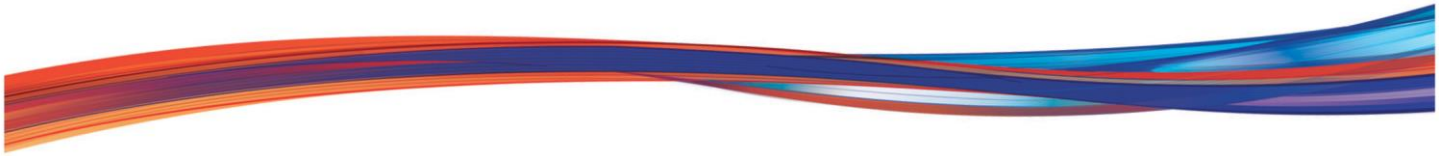
12 APP 11.1 obliges an APP entity to take reasonable steps to protect the information from misuse, interference and loss (APP 11.1(a)); and from unauthorised access, modification or disclosure (APP 11.1(b)).

13 The complainant's complaint dated 1 July 2014.

14 The CBA's submissions dated 16 May 2016.

15 By email on 5 January 2015.

16 The revised, resubmitted version



36. The access report records that the employees accessed the complainant's profile on 28 June 2011, 29 June 2011 and 20 September 2011. [17]

37. The access report records that there are multiple instances of access to the complainant's customer profile on the dates listed above.

38. I note that the complainant contends that the revised access report is also incomplete and that there are further unreported accesses additional to those listed above.[18]

39. I accept the revised access report as evidence that the principal and the employees accessed the complainant's CommSee profile during the FWC proceedings.

40. The CBA contends that the 'accesses and use of the information were consistent with legitimate CBA business purposes and therefore there was no unauthorised access or use which might lead to a breach of National Privacy Principle 2'.[19]

41. The complainant alleges that all the accesses were improper and that the CBA should have restricted the MIA's access to her customer profile during the period in which she was in FWC proceedings with its principal. In that regard, I note that on 14 July 2011, the principal sent an email to the CBA requesting that the complainant's loans be removed from the MIA's loan book for the reason that he 'would prefer not to be managing this relationship moving forward as there may be a conflict of interest'.[20] It is apparent that a number of the accesses occurred subsequent to that date.

42. Initially to the complainant, and subsequently to the OAIC the CBA has given various reasons addressing why, in its view, the accesses I have listed above at [35] - [36] are not an interference with the complainant's privacy. Specifically, the CBA has said the accesses were:

    - for the management of the complainant's, at that time, non-performing loans
    - for reasons of further lending

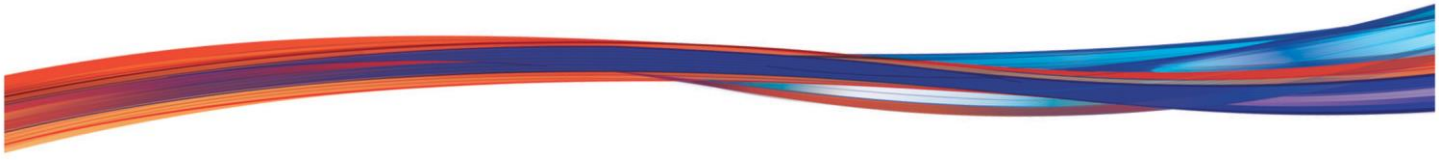
---

17 The revised, resubmitted version.

18 In her final submissions dated 2 June 2016, the complainant contends that the report is missing two days, 9 and 10 July 2011, over which the complainant alleges 22 accesses occurred.

19 In its letter to the OAIC dated 16 May 2016.

20 Email from the principal to the CBA dated 14 July 2011 at 9:34 AM.



- in accordance with the MIA service agreement to maintain a continuous client relationship, including client maintenance and service, addressing general product enquiries on the products introduced to the CBA
- for the purpose of investigating suspected unlawful activity, and
- made in relation to the investigation of alleged fraud.

43. I note that the CBA's responses to the complaint have been inconsistent and the CBA itself has acknowledged this fact.[21]

44. In response to the CBA's reasons, the complainant submits:

> [In relation to the management of the complainant's loans] … neither [the principal] or any of his staff were responsible for managing my non-performing loans - this was handled by another division of the Bank (the "Hardships Area") with whom I was in regular contact as I worked to get my accounts back in order.
>
> ...
>
> … clients who had arrangements in place or were in regular contact with the "Hardships Area" did not need to be contacted, nor their accounts viewed or managed.
>
> …
>
> [In relation to further lending and maintaining a continuous client relationship]. Given I was in a legal dispute with [the principal] directly, I would never have contacted either him or any of this staff for maintenance, service, product enquiries or any other banking matter. However, as the interactions show from other CBA staff, I did contact the call centre and local branches.
>
> …
>
> [In relation to investigating fraud and unlawful activity]. Given that the Bank has number departments who [sic] could investigate such activity, was [the principal] really an appropriate person to conduct an investigation?

45. The complainant also submits an email from the principal to a director of the MIA [**the director**] dated 19 September 2011. I note that in that email, the principal discusses 'being sued' and his 'preference to

---

21 In its letters to the OAIC dated 8 February 2016 and 16 May 2016.

see [the complainant] go down for fraud and lose her properties', commenting that 'at least [the principal's] wife and staff will be proud of [him]'.

46. In its final submissions to the OAIC,[22] the CBA set out the background and the findings of its investigation into the circumstances surrounding the principal and employees accessing the complainant's CommSee profile.

47. The CBA submits that its investigations show:

    - The principal's accesses on 15 June 2011, and between 4 July 2011 and 14 September 2011 were made in relation to assessing the complainant's home loan application and the provision of information to CBA Group Security. The principal prepared a cover letter and files relating to the complainant's salary and income during the relevant period.
    - It has not been able to establish a clear link to the principal's access of 1 July 2011.
    - The first employee was unable to recall why he accessed the profile on the relevant dates. However, the CBA's investigations revealed that this employee had accessed the profiles of more than 60 clients over the two days at issue.
    - The CBA has not been able to contact the second employee.

48. The CBA submits that the first employee's accesses are 'consistent with a review of a report or follow up on performance of accounts and [this] suggests that [the complainant] was not singled out', and the second employee's access appear to relate 'to either review of arrears on the account, or as part of the investigation into potential fraudulent conduct'.

49. I have examined the relevant CBA's policies that were in effect in 2011. The CBA's external privacy policy stated:

> Personal information may also be used for:
>
> - monitoring and evaluating products and services;
> - gathering and aggregating information for statistical, prudential, actuarial and research purposes;
> - assisting customers with queries; and

[22] Dated 16 May 2016.

- taking measures to detect and prevent credit loss.

50. It is apparent that the primary purpose of the CBA's collection of customer personal information is to allow CBA staff, and other authorised users, to effectively manage customers' banking business, including for protective purposes such as loss prevention. I am satisfied that the primary purpose of collection would include the review account arrears and investigations into potential fraudulent conduct. The CBA will not have interfered with the complainant's privacy if the principal and the employees accessed her CommSee profile for the purpose of reviewing account arrears, or as part of an investigation into potential fraudulent conduct.

51. In any event, by way of the operation of the exception in NPP 2.1(f), the CBA will not have interfered with the complainant's privacy, if her CommSee profile was accessed as a necessary part of an investigation into unlawful activities.

52. Throughout the complaint investigation, the CBA has maintained its position that for each access 'there was something being reviewed relating to [the complainant's] loans' and that 'access to [the complainant's] profile is compliant with National Privacy Principle 2'.[23]

Findings in relation to alleged breach of NPP 2.1

Permitted use - primary purpose

53. As I discussed above at [50], using or disclosing personal information about an individual for the primary purpose of managing a customer's banking business is not a breach of NPP 2.

54. As I discussed above at [47], the CBA's investigation show that the first employee accessed 60 separate accounts over the relevant two-day period, I agree with the CBA that it appears that the first employee had not 'singled out' the complainant's CommSee profile. I agree with the CBA that the first employee likely accessed the complainant's CommSee profile for the purpose of a review of a report or a general follow up on performance of accounts.

55. In relation to the second employee's accesses, the CBA was unable to contact this individual. However, the CBA said that the access appears to relate 'to either review of arrears on the account, or as part of the investigation into potential fraudulent conduct'. There is no evidence that would suggest that the

[23] The CBA's submissions dated 13 March 2015.

second employee has any direct involvement in the FWC proceeding, and given the passage of time this employee is now uncontactable. Further, the report indicates that this employee accessed the complainant's CommSee profile, only once.[24] For these reasons, I am satisfied that the second employee most likely accessed the complainant's CommSee profile for a proper purpose, likely for the primary purpose of reviewing the complainant's loans.

56. In relation to the principal's accesses, as I discussed above at [47], the CBA submits that its investigations show that the principal's accesses were related to assessing the complainant's home loan application and the provision of information to CBA Group Security. In effect, preliminary investigations relating to the propriety of the complainant's loan application.

57. As I discussed above at [44], the complainant questions whether, in the surrounding circumstance of the FWC proceedings, the principal would be an appropriate person to conduct such an investigation. The complainant contends that the CBA has a number of internal departments that could investigate such activity.

58. I agree with the complainant. The principal of an external mortgage agency, with whom the complainant in currently involved in a FWC dispute, would not be an appropriate person to conduct such an investigation. Particularly given, as I discussed above at [41], that the principal himself identified a potential conflict of interests on 14 July 2011 and he has asked the CBA to remove the complainant's loans from the MIA's loan book. In this case, it is apparent that the principal continued to access the complainant's CommSee profile for a further two months from that date, on multiple occasions through to 14 September 2011. The access report records that the principal's accesses occurred on a number of occasions after hours and for extended periods of time. One access, on 10 July 2011 lasted for over three hours.

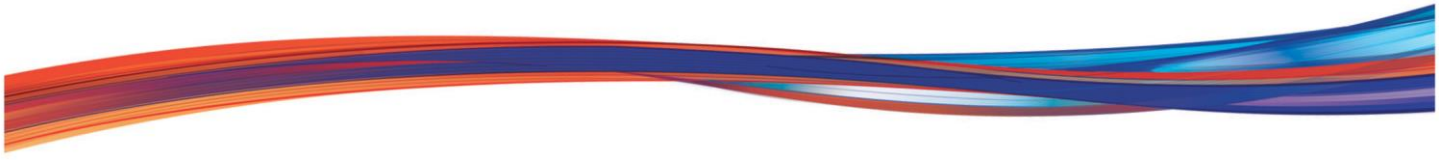
59. Given the apparently acrimonious relationship between the principal and the complainant during the FWC proceedings, as evidenced by the email referred to in paragraph 45 above,[25] I do not accept that the principal was properly accessing the complainant's CommSee profile on each occasion during that time.

60. From the evidence before me, I am not satisfied that the CBA has demonstrated that on the balance of probabilities, all of the principal's accesses to the complainant's CommSee profile were for the primary purpose. In particular, I do not accept that the principal accessed the profile for the purpose of

---

24 On 20 September 2011.

25 As I discussed above at [45].



investigating alleged fraud. Given that the CBA has its own department for such investigations, I agree with the complainant that it would have been inappropriate for the principal to be involved in such an investigation, particularly given the nature of the FWC dispute at the time and the principal's recognition of the conflict of interest the dispute had created. I do not accept the CBA's submissions that the principal accessed the complainant's CommSee profile for primary purpose of managing the complainant's banking business, this too appears unlikely in the circumstances. I note particularly that the CBA has been unable to explain at least one access.[26] I agree with the complainant that in disclosing her personal information to the principal, the CBA used her personal information for an improper secondary purpose.

61. For these reasons, I am satisfied that the CBA improperly used and disclosed the complainant's personal financial information to the principal when it gave the principal access to the complainant's CommSee profile at a time when the principal and the complainant where in a FWC dispute with each other.

Exception NPP 2.1(f) Unlawful activity

62. The guidelines to the NPPs explain that NPP 2.1(f) acknowledges that one of an organisation's legitimate functions is to investigate and report on suspected unlawful activity. [27]

63. The CBA contends the disclosure was permitted under NPP 2.1(f) as the CBA had reason to suspect that unlawful activity had been engaged in, and disclosing the personal information was a necessary part of its investigation.[28]

64. Given my findings that the CBA gave the principal access the complainant's CommSee profile for an improper secondary purpose, a secondary purpose that is not the purpose of investigating an alleged fraud, it is unnecessary for me to consider whether the exception under NPP 2.1(f) applied.

Alleged Breach of NPP 4.1

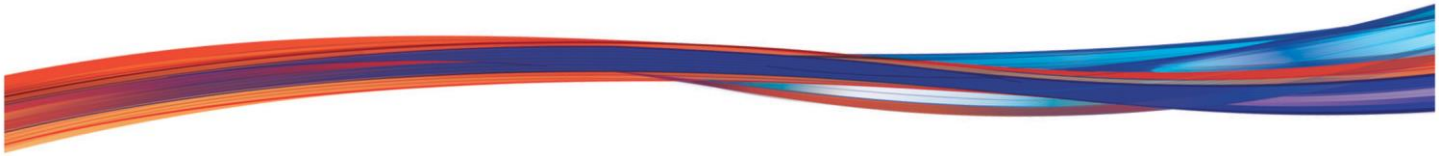
65. The complainant alleges a breach of NPP 4.1 by the CBA failing to take reasonable steps to protect her personal information from misuse, loss and from unauthorised, access, modification, use or disclosure.

---

26 The principal's access of 1 July 2011.

27 *Guidelines to the National Privacy Principles*, pages 40-41.

28 In its response of 19 December 2014.



66. The complainant alleges that the CBA did not take adequate security measures when it continued to allow the MIA access to her CommSee profile once it had knowledge of the FWC proceedings and the potential conflict between her interests and the interests of the principal.

67. The guidelines to the NPPs explain that '[i]n general terms an organisation discloses personal information when it releases information to others outside the organisation'.[29]

68. In relation to 'reasonable steps', the NPP guidelines explain:

> What are reasonable steps to secure personal information will depend on the organisation's particular circumstances. Some relevant factors include:
>
> - The sensitivity of the personal information the organisation holds
> - The harm that is likely to result to people if there is a breach of security
> - How the organisation stores, processes, and transmits the personal information (for example, paper-based or electronic records), and
> - The size of the organisation (the larger the organisation, the greater the level of security likely to be needed.[30]

Findings in relation to alleged breach of NPP 4.1

69. As I discussed above at [40], throughout the privacy investigation, the CBA has not acknowledged that it interfered with the complainant's privacy. Rather, it has maintained its position that the principal's accesses to complainant's CommSee profile were consistent with CBA business purposes.

70. The CBA has the largest customer base of any Australian bank and it employs 52,000 people within the Commonwealth Bank Group.[31] CommSee gives authorised users access to customers' financial information.

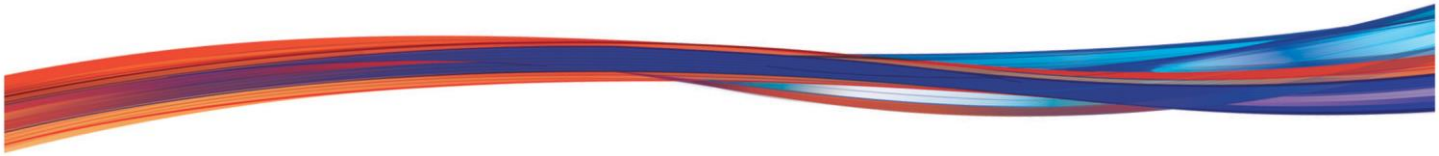
71. Given the size of the organisation, and the sensitivity of the information stored on CommSee, I consider that, at a minimum, the CBA should have processes in place to restrict a user's access to a CommSee

---

29 *Guidelines to the National Privacy Principles*, page 28.

30 *Guidelines to the National Privacy Principles*, pages 44-45.

31 Commonwealth Bank, *Commonwealth Bank overview* https://www.commbank.com.au/about-us/our-company/overview.html.



profile immediately when it becomes aware of a potential conflict of interests between the customer and the user.

72. In this case, the principal maintained his access to the complainant's CommSee profile, and in fact continued to access the complainant's personal financial information for a period of three months subsequent to the date he informed the CBA of the potential conflict of interests.

73. I am therefore of the view that the CBA's data security practices were not reasonable in this instance. I am satisfied that the CBA has not met its obligations under NPP 4.1.

Finding on damages

74. I have found that the CBA breached NPP 2.1 and NPP 4.1

75. Having found the complaint substantiated, I have the discretion under s 52(1)(b)(iii) of the Privacy Act to award compensation for 'any loss or damage suffered by reason of' the interference with privacy'. Section 52(1A) states that loss or damage can include 'injury to the complainant's feelings or humiliation suffered by the complainant'.

76. I am guided by the principles on awarding compensation summarised by the Administrative Appeals Tribunal in *EQ and Office of the Australian Information Commissioner*[32] and *Rummery and Federal Privacy Commissioner*.[33] I have discussed the principles in *Rummery* in a number of previous determinations, including *'IR' and NRMA Insurance, Insurance Australia Limited*[34] and *'HW' and Freelancer International Pty Limited*.[35]

77. I have also had regard to amounts awarded in other privacy determinations. I have previously summarised these in *'IY' and Business Services Brokers Pty Ltd t/a TeleChoice*[36] and *'IQ' and NRMA Insurance, Insurance Australia Limited*.[37]

---

32 *EQ and Office of the Australian Information Commissioner (Freedom of information)* [2016] AATA 785.

33 *Rummery and Federal Privacy Commissione*r [2004] AATA 1221 [32].

34 *'IR' and NRMA Insurance, Insurance Australia Limited* [2016] AICmr 37 [97].

35 *'HW' and Freelancer International Pty Limited* [2015] AICmr 86 [351].

36 *'IY' and Business Services Brokers Pty Ltd t/a TeleChoice* [2016] AICmr 44 [53]-[56].

37 *'IQ' and NRMA Insurance, Insurance Australia Limited* [2016] AICmr 36 [65]-[69].

Economic loss

78. In *EQ and Office of the Australian Information Commissioner*, the AAT discusses that damages for economic loss are awarded to restore an individual to 'the same position as he would have been in if he had not sustained the wrong for which he is now getting his compensation';[38] and the relevant principles in relation to causation are:

    a) causation is ultimately a question of common sense and experience, determined on the facts of each case;

    (b) in law, causation is a question identifying where legal responsibility should lie, rather than examine the cause of event from a scientific or philosophical viewpoint, policy issues and value judgements have a role to play in determining whether, for legal purposes, a circumstances we found to be causative of loss;

    (c) a' but for' analysis is not a sufficient test causation, although it may be a guide; and

    (d) where there are multiple elements, each one sufficient on its own to have caused the loss, the causation test may be considered satisfied by each one of them.[39]

79. The complainant asserts that the principal benefited by at least $100,000 by misusing his access to her financial information during the FWC case.[40] The complainant has submitted an email between the director and the principal dated 5 October 2011 (**the email**) in which the principal said: 'I am also happy to take the loan book for which I would pay $100k to [the complainant] and legal fees (total cost say $130k)'.

80. On the basis of the email, the complainant asserts that the principal used his knowledge of her financial position during FWC settlement negotiations to effect a settlement of $100,000 less that she would otherwise have agreed to.

81. I do not agree with the complainant that, in this case a causal link is made out. It is not clear to me that in the email the principal is referring to a settlement in the FWC proceedings. Likewise, I do not think it can

---

38 *EQ and Office of the Australian Information Commissioner (Freedom of information)* [2016] AATA 785 [41] and [47].

39 *EQ and Office of the Australian Information Commissioner (Freedom of information)* [2016] AATA 785 [47] from *March v Stramare (E and MH) Pty Ltd* [1991] HCA 12; (1991) 171 CLR 506.

40 The complainant's letter to the OAIC of 2 June 2016.

be said that if the principal had not accessed the complainant's CommSee profile, the complainant would now be in a position of having received from him an additional $100,000.

82. Similarly, in my view it cannot be said that on a common sense approach, the principal's access to the complainant's CommSee profile caused her to receive a lesser settlement amount in the FWC proceedings. Nor, it is apparent that 'but for' the principal's access the complainant would have been able to negotiate a greater settlement figure.

83. In these circumstances, I am satisfied that there is no basis for awarding compensation for economic loss.

Non-economic loss

84. The complainant submits that she has 'gained over 25kgs as a result of ongoing chronic stress' and her 'quality of life has suffered significantly' by the disclosure of her personal information.[41] She claims that with live access to her bank account information and transactions, 'it would be very easy for CBA staff to pinpoint' her location at any moment, 'even to this day.' These incidents have raised concerns for her personal safety and she still has the same 'intense screaming nightmares' now that she suffered during the FWC proceedings.

85. The complainant has not submitted any other evidence, beyond her own statements, to support her claims that she has suffered physical effects, anxiety and nightmares as a result of the breach of the CBA. However, I have considered and given substantial weight to her statements.

86. I am satisfied that the manner in which CBA has handled the complainant's personal information has caused the complainant considerable distress and that an award of damages is consequently appropriate. In particular, I consider that when the principal informed the CBA on the 14 July 2011 that he may have a conflict of interest, the CBA should have immediately acted to restrict his access to the complainant's CommSee profile.

87. I have also had regard to the type of information that has been disclosed by the CBA, the complainant has submitted, and I accept that the principal had access to the complainant's individual bank account transactions for the previous two years. He had access to her financial position; and her income and expenditure, both historically and in near real time.

---

41 The complainant's letter to the OAIC of 2 November 2015.

88. After consideration of the above factors, I consider it appropriate to award the complainant $10,000 in compensation for non-economic loss.

Aggravated damages

89. The power to award damages in s 52 of the Privacy Act includes the power to award aggravated damages in addition to general damages.[42]

90. I have previously made reference to two principles which provide useful guidance in determining whether such an award is warranted:[43]

- aggravated damages may be awarded where the respondent behaved 'high-handedly, maliciously, insultingly or oppressively in committing the act of discrimination'[44]
- the 'manner in which a defendant conducts his or her case may exacerbate the hurt and injury suffered by the plaintiff so as to warrant the award of additional compensation in the form of aggravated damages.'

91. As I discussed above at [17], the complainant asks that I impose penalties on the CBA for the interference with her privacy, and for the CBA providing 'misleading statements and fraudulent/falsified documents' to the OAIC during the complaint investigation.

92. The complainant has provided extensive submissions addressing why, in her view the CBA has behaved poorly during the investigation of her privacy complaint. I have carefully considered these submissions. While it is unnecessary for me to go into the submissions in detail, in summary the complainant seeks that the CBA be penalised for the way in which it has dealt with her complaint.

93. I note that the complainant initially sought only either a copy of her access report or alternatively, its assurance that that the principal's access to her CommSee profile was a 'once off'. In response to that initial complaint, the CBA response was a brief letter from its Senior Legal Counsel that did not provide

---

42 *Rummery and Federal Privacy Commissioner and Anor* [2004] AATA 1221, [32].

43 *'D' v Wentworthville Leagues Club* [2001] AICmr 9 [50]; *'S' v Veda Advantage Information Services and Solutions Limited* [2012] AICmr 33 [93]; '*BO' v AeroCare Pty Ltd* [2014] AICmr 37 [57]; *'HW' v Freelancer International Pty Limited* [2015] AICmr 86 [379].

44 *Hall v A & A Sheiban Pty Ltd* [1989] FCA 72 [75].

access or address the substance of her complaint. In my view it would be preferable if the CBA had sought to resolve the complainant's concerns in the first instance.

94. I further note that the CBA was inconsistent with its responses to both the complainant and the OAIC, and that it continues to deny that it has breached the NPPs. I also note that the CBA provided the OAIC with a potentially misleading document during the course the privacy investigation (the partial access report). I accept that the CBA's approach to the privacy investigation has caused the complainant additional work, delays and frustration, and the additional work, delays and frustration is likely to have caused the complainant some distress.

95. However, I do not consider the way in which the CBA has conducted its case is overall high-handed, malicious, insulting or oppressive. Overall I do not consider CBA's behaviour was so inappropriate as to justify an award of aggravated damages.

Determination

96. I declare in accordance with s 52(1(b)(i)(B) of the Privacy Act that the CBA:

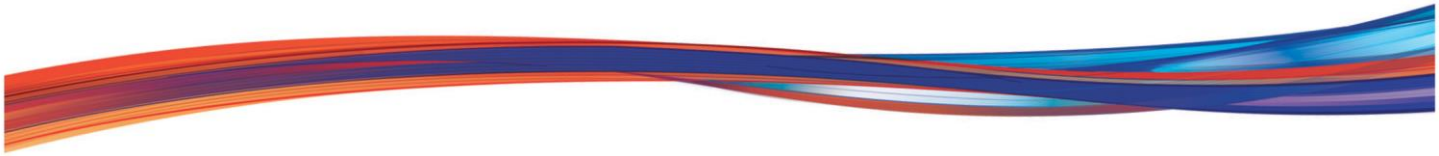
- the complainant's complaint is substantiated
- the CBA has breached NPP 2 by improperly disclosing personal information about the complainant to the principal
- the CBA had breached NPP 4 by failing to take reasonable steps to protect the complainant's personal information from misuse.

97. I declare in accordance with s 52(1)(b)(ii) of the Privacy Act that the CBA:

- must issue a written apology to the complainant within six weeks of this determination, acknowledging its interference with the complainant's privacy.

98. I declare in accordance with s 52(1)(b)(ia) that the CBA must:

- review its information handling policies, particularly in respect of access to customer information where there is an acknowledged, or potential conflict of interest, and
- report back to me within 6 months about the findings of this review.



99. I declare in accordance with s 52(1)(b)(iii) that the complainant is entitled to $10,000 for the non-economic loss suffered as a result of CBA's interference with her privacy.

Timothy Pilgrim
Australian Privacy Commissioner

25 November 2016

Review rights

A party may apply under s 96 of the *Privacy Act 1988* to have a decision under s 52(1) or (1A) to make a determination reviewed by the Administrative Appeals Tribunal (AAT). The AAT provides independent merits review of administrative decisions and has power to set aside, vary, or affirm a privacy determination. An application to the AAT must be made within 28 days after the day on which the person is given the privacy determination (s 29(2) of the Administrative Appeals Tribunal Act 1975). An application fee may be payable when lodging an application for review to the AAT. Further information is available on the AAT's website (www.aat.gov.au) or by telephoning 1300 366 700.

A party may also apply under s 5 of the *Administrative Decisions (Judicial Review) Act 1977* to have the determination reviewed by the Federal Circuit Court 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 on the Court's website (http://www.federalcourt.gov.au/) or by contacting your nearest District Registry.