5

# FINAL REPORT OF THE DECISION MAKER ON SUSPECTED BREACH OF THE CODE OF CONDUCT BY S 22 / 47F

1. As selected in accordance with paragraph 2 of the Procedures for Determining Breaches of the Code of Conduct (the Code of Conduct Procedures), by Mark le Dieu, National Manager, People Services Branch, and as referred to me by S 22/47F National Manager, Section 47F, I am required to:

   a. investigate an allegation that you may have breached the Australian Public Service Code of Conduct;

   b. determine whether you did breach the Code of Conduct; and

   c. in the event that I find you did breach the Code of Conduct, make a recommendation on what, if any, sanction(s) should be imposed.

## SUSPECTED BREACH OF THE CODE OF CONDUCT

2. It is suspected that you may have failed to comply with laws relating to unauthorised access to Centrelink information and failed to comply with Centrelink 'unauthorised access' policies on four (4) separate occasions by accessing Centrelink's online customer records through the Income Support Information System (ISIS) and On-Line Search facility (OLS), concerning:

   - yourself; on three (3) separate occasions from 1 December 2009 to 4 February 2010; and,
   - your fathe S 22 / 47F rs; on one (1) occasion on 15 December 2009.

3. My task is to establish whether your suspected conduct occurred and if so, whether it was a breach of the Code of Conduct.

4. I suspect that your conduct may be in breach of the following elements of the Code of Conduct.

   (1) An APS employee must behave honestly and with integrity in the course of APS employment;

   (2) An APS employee must act with care and diligence in the course of APS employment;

   (4) An APS employee, when acting in the course of APS employment, must comply with all applicable Australian laws. For this purpose, Australian law means:

   (a) any Act (including the Public Service Act 1999), or any instrument made under an Act; or

   (b) any law of a State or Territory, including any instrument made under such law.

   (5) An APS employee must comply with any lawful and reasonable direction given by someone in the employee's Agency who has authority to give the direction.

   (7) An APS employee must disclose, and take reasonable steps to avoid, any conflict of interest (real or apparent) in connection with APS employment;

   (11) An APS employee must at all times behave in a way that upholds the APS Values and the integrity and good reputation of the APS.

**LEGISLATION/POLICY/INSTRUCTIONS**

5. In conducting this investigation I have had regard to the following legislation, policy and instructions.

   a. Code of Conduct, section 13 of the *Public Service Act 1999* (the 1999 Act). The Code of Conduct has applied since 5 December 1999 and sets out the standards of conduct required of APS employees.

   b. subsection 203(1) of the *Social Security (Administration) Act 1999*, which has applied since 20 March 2000 and has been amended from time to time. Effectively, this provision makes it an offence for a person to intentionally access protected information in Centrelink records if the person is not authorised to obtain that information and knows that the information is protected information.

   c. subsection 204(1) of the *Social Security (Administration) Act 1999*, which has applied since 20 March 2000 and has been amended from time to time. Effectively, this provision makes it an offence for an unauthorised person to intentionally use, record or disclose protected information in Centrelink records if the person knows that the information is protected information.

   d. Centrelink Privacy and Confidentiality Manual Chapter 3, titled 'Storage and Security of Personal/Protected Information', which has applied since January 2003 and has been amended from time to time. This Chapter of the Manual states that a person whose information is held by Centrelink has a right to expect that Centrelink will hold it securely, and will ensure that access to the information is permitted only for legitimate purposes.

   e. Centrelink 'Declaration of Confidentiality/Privacy, Security, Fraud Awareness and Conduct Responsibilities' booklet (previously known as the 'Declaration of Confidentiality/Security and Privacy Responsibilities' booklet or the 'Rules for the Handling of Personal/Protected Information' booklet), which is referred to in this report as the Confidentiality Booklet. The Confidentiality Booklet is provided to employees who undertake training in privacy or information security awareness. The Confidentiality Booklet contains a summary of the 'unauthorised access' rules and a Declaration of Confidentiality, which is signed by each employee who receives the Confidentiality Booklet.

   f. Chief Executive's Instruction 20, 'Unauthorised Access to Centrelink Customer Records and the Personnel Records of Centrelink Employees', which has applied since 2 December 2005 and has been amended from time to time. This Instruction provides direction to employees regarding access, use and/or disclosure of personal or protected information, and conflict of interest matters.

**EVIDENCE AND OTHER MATERIAL**

6. In the course of my investigation I have considered the following evidence and material:

   a. Information from your Personal Employment File, such as your public service history and declaration of confidentiality etc;

   b. Information from your Infolink Personnel Record, such as personal details, date specifications, pay levels and organisational assignments etc;

c. Privacy Incident Investigation Report dated 11 March 2010. Please note that any personal information contained in the Privacy Incident Investigation Report which is not relevant to the matter being investigated has been redacted;

d. copy of an electronic Declaration of Confidentiality acknowledged by you on 26 June 2009;

e. Confirmation of your attendance at a Centrelink Privacy/Disciplinary Awareness Session at Section 47F on 9 February 2009.

**CENTRELINK'S 'UNAUTHORISED ACCESS' RULES**

7. I am satisfied that Centrelink has provided staff with clear guidance about accessing customer records in circumstances where there may be a conflict of interest. In particular, Centrelink has unequivocally instructed staff not to handle cases concerning ex-partners, family, relatives or friends and/or acquaintances, and not to access their own customer records.

8. I am also satisfied that, to the extent that they provide direction to employees, the Chief Executive's Instructions I have referred to in this report constitute lawful and reasonable directions given by someone in Centrelink (or its predecessor, the Department of Social Security) who had authority to give the direction.

9. Chief Executive's Instruction 20 relevantly states:

> 20.01 When accessing personal information held in the records of Centrelink, all employees must comply with Centrelink's privacy and confidentiality policy regarding access, use and/or disclosure of personal or protected information set out in:
>
> (a) Centrelink Privacy Awareness Kit
>
> (b) The Declaration of Confidentiality booklet that contains the 'Rules for Handling Personal/Protected Information'
>
> 20.02 In all their dealings with customers and/or other staff, employees must ensure that they deal with conflicts of interest, real or apparent, in accordance with the policy set out in:
>
> (a) Centrelink Privacy Awareness Kit
>
> (b) Centrelink People Management Handbook
>
> (c) Centrelink Ethics Resource Kit

10. Chapter 3 of the Privacy and Confidentiality Manual relevantly states:

> 3.061 Being a Centrelink employee does not automatically authorise an individual to access protected information. Employees are given access to Centrelink computer and paper records in order for them to carry out their prescribed duties. Access to protected information is not provided for private use therefore employees must not access computer or paper records of customers or employees out of personal interest or curiosity...
>
> 3.063 Some examples of browsing include accessing:
>
> - your own customer record;
> - the customer database or Infolink to:
>
> - obtain a friend's birth date and/or address to send a greeting card;

- obtain a friend or relative's telephone number which may be unlisted in order to contact them on a social/personal basis etc;

- the records of people reported in the press;
- neighbours records out of curiosity;
- the records of friends and relatives to find out what their income or assets might be;
- a customer record on behalf of a friend or relative;
- a friend's records to see how their claim is progressing or to see if it has been assessed correctly;
- a work colleagues record at his or her request;
- using 'live' records for group training purposes; and
- a customer's record who is the subject of a tip-off if it is not part of the staff member's job to do so.

3.064 Public confidence in the integrity of the public service is vital to the proper operation of government. Where the community perceives a conflict of interest that confidence is jeopardised. A conflict of interest occurs when an employee's personal affairs, financial or other interests conflict with the performance of their official duties...

3.067 There would be as conflict of interest where the employee has a personal interest in the person whose record is being accessed. For this reason an employee must not access and/or process their own customer record or those of family, ex family, friends, close personal acquaintances, neighbours [or] work colleagues without authorisation from their team leader...

3.068 The restriction does not apply to everyone an employee knows as a casual acquaintance. The test is whether the acquaintance with the customer could be seen by a third person to be to the customer's advantage in his or her dealings with Centrelink...

3.071 If circumstances make it unavoidable for an employee to access the record of a friend, relative or acquaintance, the problem of conflict of interest can be overcome by advising his or her team leader/manager of the need **before** accessing the record. With the team leader's permission, the record may then be accessed and/or assessed. A record of this authorisation will need to be kept, possibly in a DOC created by the team leader on the customer record [or] in a secure office register signed by the team leader...

3.072 **A customer cannot authorise an employee** to access their record when such an access would be contrary to Centrelink practice. For example, an employee's mother cannot authorise them to look at her record because Centrelink instructions clearly state that an employee must not access or assess the records of family members....

3.101 A Centrelink employee may inadvertently access the customer record of a family member, friend, close personal acquaintance, neighbour etc. If this happens the employee must immediately speak with their team leader or manager and explain the situation. The team leader or manager must make a note of the 'inadvertent' access in a secure office register...

11. The Confidentiality Booklet relevantly states:

Access to personal information is on a 'need to know' basis in order for you to perform your duties. It is not provided for your personal use. You do not have to disclose the information to someone else, just looking at a customer or employee's record when you are not authorised is an offence under various legislation Centrelink administers. This is commonly known as **browsing.**

You are not authorised to access and/or process your own customer record or those of family, friends or other people where there may be, or may be perceived to be, a **conflict of interest.** This also includes people with whom you may have had or are having a dispute.

While it is acceptable for you to receive a request from a friend, relative or acquaintance for information or advice about the person's dealings with Centrelink, you should not be involved in processing the matter including accessing the customer's or Centrelink employee's record. **A customer (including a colleague who is a customer) cannot authorise you to access their record** where such access would be contrary to Centrelink practice. For example, your mother cannot authorise you to look at her record because Centrelink instructions clearly state that you cannot access or assess the records of family members.

There are severe penalties for employees who breach the confidentiality provisions. These include penalties under various legislation (including the *Crimes Act 1914*) of up to two years imprisonment. Ongoing and non-ongoing employees may also face sanctions under the *Public Service Act 1999* which may attract disciplinary measures such as fines, demotions or dismissal.

12. I have reproduced the above quotes to establish the basis for my finding that Centrelink has provided guidance on these matters. In making my findings, I have relied on the whole of the above quoted Chief Executive's Instructions, along with the other legislation, policy and instructions referred to in this document.

13. I am satisfied that:

    a. Centrelink had specifically prohibited you from accessing customer records concerning you and your immediate family, and/or acquaintances; and

    b. Centrelink had expressly indicated that a failure to follow these rules might result in disciplinary action.

**ACTION REQUIRED BY YOU IN RESPONSE TO INADVERTENT ACCESS**

14. The Confidentiality Booklet relevantly states:

> If you are concerned about a possible conflict of interest you should speak to your Team Leader **before** dealing with that person or accessing their record. The Team Leader can authorise you to deal with the matter or reassign the case to another employee.

15. Centrelink's Privacy and Confidentiality Manual relevantly states:

> 3.071 If circumstances make it unavoidable for an employee to access the record of a friend, relative or close personal acquaintance, the problem of conflict of interest can be overcome by advising his or her team leader/line manager of the need before accessing the record. With the team leader/line manager's permission, the record may then be accessed and/or assessed. A record of this authorisation must be made by the team leader/line manager who has authorised the access. To do this the team leader/line manager must access the customer record themselves and record an

'AAA' enquiry type DOC on the customer's record containing the authorised employee's logon id details and the date of the access they are approving. The DOC automatically records the logon id of the authorising team leader/line manager when it is applied.

3.101 A Centrelink employee may inadvertently access the customer record of a family member, friend, close personal acquaintance, neighbour etc. If this happens, the employee must remove themselves from the situation, notify their team leader/line manager and explain the situation, then record the incident in the Inadvertent Access Register, accessed from the Privacy and Information Access section homepage....

16. Since July 2007, a national online register has been in operation enabling employees to directly report occasions of inadvertent access. Prior to this, employees were required to notify their team leader/manager who would appropriately record the report and the action taken.

**YOUR KNOWLEDGE OF CENTRELINK'S 'UNAUTHORISED ACCESS' RULES**

17. I have considered what knowledge you had, or should have had, of Centrelink's rules concerning accessing customer records concerning you, your family and/or acquaintances, including other Centrelink employees.

18. Personnel records indicate on 9 February 2009, you were engaged as an ongoing employee of Centrelink. You are now a Customer Service Advisor at the APS 3.2 level, working in Section 47F.

19. In summary, you have worked at Centrelink for a period of approximately fourteen (14) months. I note that as at the date of the last suspected unauthorised access on 4 February 2010, you had worked at Centrelink for a period of just under one (1) year.

20. Since 1992, Centrelink (and its predecessor, the Department of Social Security) has displayed computer messages on access to the Customer database to remind employees of their responsibilities concerning access to records concerning immediate family members, friends and/or acquaintances. From November 1994 to August 2005, the Centrelink mainframe randomly generated 25 messages, five of which directly relate to Centrelink's 'unauthorised access' rules. The text of these messages is set out below.

    a. Protecting client information is your responsibility. Accessing client or staff information when it is not required as part of your job is an offence. Penalties include fines, imprisonment and disciplinary action. All access to computer records is logged.

    b. Protecting client information is your responsibility. You may be approached by friends, relatives or a close personal acquaintance who knows that you work for the department. They may ask you to amend FA/FAS entitlement records or the like. Staff may not access friends' files (even in the course of your duties). This can lead to a clash of interest. Friends and family should be told to approach the office through the proper channels. If files of any of the above are given to you as part of your workload tell your supervisor who will reassign them to another staff member.

    c. Avoiding Conflict of Interest is your responsibility. Staff may not access their personal departmental client files nor those of their family and friends. This can lead to a Conflict of Interest.

d. The price of privacy is eternal vigilance.

e. Confidentiality is your responsibility. You may only access records necessary in the performance of your duties. Browsing is a criminal offence. All computer access is logged. The department can now tell if you have accessed a record.

21. The above messages have been supplemented by the following messages, launched in October 1998.

a. Browsing: you don't have to give out the information to someone else, just looking at customer or staff records when you are not authorised is an offence.

b. Family & friends deserve privacy too! You are not authorised to access the records of family, friends & close associates.

22. The above messages have also been supplemented by the following message, launched in March 1999.

a. Staff are not authorised to access or assess their own customer record.

23. All employees are obliged and reminded to lock their keyboard every time they leave their desk. In any case, an unattended computer keyboard will lock after 10 minutes. I am satisfied that during your employment with Centrelink the above-mentioned messages will have provided you with daily reminders of your obligation to comply with Centrelink's 'unauthorised access' policies.

24. On 9 February 2009 you attended a Centrelink Privacy/Disciplinary Awareness Session in Section 47F. The session addressed a range of issues about access to customer records, including unauthorised browsing and conflicts of interest. The session also addressed the consequences of failing to comply with Centrelink's 'unauthorised access' rules.

25. Since January 2008, Centrelink officers have received an email annually on their commencement anniversary advising them that there is a Declaration of Confidentiality to acknowledge in the Inbox of their Infolink Personnel record. Officers are required to log into Infolink, select the Electronic Declaration of Confidentiality action item and acknowledge that they have read, understood and agree to abide by the rules contained in the Declaration of Confidentiality - Privacy, Security, Fraud Awareness and Conduct Responsibilities booklet. The CEO has directed that all officers must electronically acknowledge their obligations annually on their commencement anniversary. Your Infolink Personnel record indicates that on 26 June 2009, you electronically acknowledged Declarations of Confidentiality - Privacy, Security, Fraud Awareness and Conduct Responsibilities. By doing so, you certified that you had read and understood Parts A (Privacy and Confidentiality), B (Security Responsibilities) and C (Fraud Awareness and Conduct Responsibilities) of the Confidentiality Booklet and undertook to read Part D (Legislation and Definitions). You also agreed to abide by the rules set out in the booklet. The Confidentiality Booklet clearly establishes that employees are not entitled to access their own records and the records concerning family and/or acquaintances.

26. On the basis of this evidence, I am satisfied that you knew, or ought to have known, that:

a. accessing records and processing activities concerning you, your family and/or acquaintances is not permitted by Centrelink;

b. accessing records and processing activities concerning you, your family and/or acquaintances might constitute a conflict of interest; and

c. such conduct might result in disciplinary action.

**YOUR SUSPECTED CONDUCT**

27. Attached to the draft report that was hand delivered to you by S 22 / 47F on 3 May 2010 was a Privacy Incident Investigation Report dated 11 March 2010. When provided to me, the Privacy Incident Investigation Report annexed CRAM Reports. The relevant details from the CRAM Reports are set out in the Privacy Incident Investigation Report. Accordingly the CRAM Reports were not included in my draft report. Arrangements were however made for you to view these, had you wished to do so.

28. The Privacy Incident Investigation Report describes and analyses evidence which tends to suggest that you have accessed online customer records concerning you and your father. Specifically, it appears you accessed your own Centrelink record on three (3) separate occasions from 1 December 2009 to 4 February 2010 and also that of your father, S 22 / 47F, on one (1) occasion on 15 December 2009 at which time, you issued an income statement to him.

29. On 11 March 2010, you provided a signed statement to the Privacy Officer, S 22/47F. In your statement, you acknowledged making unauthorised access to your own record and that of S 22 / 47F.

30. In your statement, you explained that you had searched for your own record on 1 December 2009, 1 February 2010, and 4 February 2010, and accessed your record on the latter two dates. You stated that you undertook these searches simply to obtain your own Customer Reference Number (CRN) because you wanted to set up Self Service, which you have since done. You noted that once you had accessed your record, you did not go beyond the first screen, instead clearing out of the record once you had recorded your CRN.

31. In your statement, you also acknowledged searching for, and accessing the record of, your father, S 22 / 47F. You explained that you did this at his request, in order to send him an Income Statement. You noted that you did not undertake any further actions on this record.

32. Chapter 3 of the Privacy and Confidentiality Manual relevantly states that *'being a Centrelink employee does not automatically authorise an individual to access protected information. Employees are given access to Centrelink computer and paper records in order for them to carry out their prescribed duties'*. The Privacy and Confidentiality Manual also states that *'a customer cannot authorise an employee to access their record when such an access would be contrary to Centrelink practice. For example, an employee's mother cannot authorise them to look at her record because Centrelink instructions clearly state that an employee must not access or assess the records of family members...'*.

33. Further, the Confidentiality Booklet states that *'you are not authorised to access and/or process your own customer record or those of family, friends or other people where there may be, or may be perceived to be, a conflict of interest'.*

34. Regardless of the your intentions, your actions were contrary to Centrelink's browsing policy, including Chief Executive Instruction 20 *Unauthorised Access to Centrelink Customer Records and the Personnel Records of Centrelink Employees*, which states that when accessing personal information held in the records of Centrelink, all employees must comply with Centrelink's privacy and confidentiality policy regarding access, use and/or disclosure of personal or protected information.

35. In light of the fact that you failed to respond to the draft report, I have adopted the content of the Privacy Incident Investigation Report as my findings of fact in relation to your accesses to customer records concerning you and your father, S 22 / 47F.

36. Based on the evidence contained in the Privacy Incident Investigation Report, it is my conclusion that you did access Centrelink's records concerning you and your father and you knew, or ought to have known, that in the circumstances:

    a. your conduct was unauthorised and a breach of Centrelink policy;

    b. your conduct represented a failure to comply with Social Security legislation concerning authorised access to information; and

    c. your conduct constituted a conflict of interest, and it was incumbent upon you to take steps to avoid that conflict of interest.

**CONDUCT CONSTITUTED A BREACH OF THE CODE OF CONDUCT**

37. Having regard to all of the evidence, I have formed an opinion that your conduct was in breach of the APS Code of Conduct. A discussion of this finding in relation to each of the elements of the Code follows.

**(1) An APS employee must behave honestly and with integrity in the course of APS employment.**

38. Centrelink employed you in a position of trust. Centrelink trusted and required you to comply with the 'unauthorised access' rules and inform other Centrelink staff of any circumstance in which a conflict of interest might arise. You knew, or should have known, that you should not have accessed records or processed any activities for yourself, your family and/or acquaintances. You also knew, or should have known, to inform your Team Leader/Senior Officer or Privacy Officer if you inadvertently accessed such records. It appears that you chose not to abide by Centrelink's clear directions to you about how you were to behave. I regard your behaviour as displaying a fundamental lack of honesty and integrity.

**(2) An APS employee must act with care and diligence in the course of APS employment.**

39. Your failure to comply with Centrelink's 'unauthorised access' rules represents a serious shortcoming in the performance of your basic duties. The fact that you have been reminded on many occasions about the 'unauthorised access' rules and your duty to take steps to avoid conflicts of interest reinforces the extent of your shortcomings. I find that your conduct demonstrated a lack of care and diligence in the performance of your duties.

**(4) An APS employee must comply with applicable Australian laws**

40. Your failure to comply with Centrelink's 'unauthorised access' rules led you to fail to comply with applicable Australian laws, specifically a failure to comply with the social security laws about accessing, using, recording and disclosing protected customer information described under the heading 'Legislation/Policies/Instructions', above. I make no finding that you are guilty of an offence under the applicable provisions, but I am satisfied on the balance of probabilities that you did not comply with those provisions.

**(5) An APS employee must comply with any lawful and reasonable direction given by someone in the employee's Agency who has authority to give the direction.**

41. The Chief Executive's Instructions referred to in this report set out a series of lawful and reasonable directions, which for the sake of convenience I have described in this report as Centrelink's 'unauthorised access' rules. I find that your failure to comply with Centrelink's 'unauthorised access' rules breached this aspect of the Code of Conduct.

**(7) An APS employee must disclose, and take reasonable steps to avoid, any conflict of interest (real or apparent) in connection with APS employment**

42. As noted above, I am satisfied that you did not disclose the conflict between your personal connections with the people whose records you accessed and your duty as a Centrelink employee not to access records concerning you and your father. Nor did you take any steps to avoid the apparent conflict. I am satisfied that you have breached this aspect of the Code of Conduct.

**(11) An APS employee must at all times behave in a way that upholds the APS Values and the integrity and good reputation of the APS.**

43. I am satisfied that your conduct, particularly your ongoing pattern of disregarding Centrelink's 'unauthorised access' policies, represents a failure to uphold the APS Values, which are set out in section 10 of the 1999 Act.

44. In particular, I consider that in behaving as you did, you failed to uphold the APS Value that provides 'the APS has the highest ethical standards'. Ethical conduct, in this situation, demanded that you not access the records concerning you and your father at all. You did not behave in this way and thus demonstrated a failure to behave ethically in relation to those records.

**SANCTION**

45. In considering what sanction to recommend, I am mindful of the fact that the imposition of a sanction is for the purposes of protecting the APS and deterring similar conduct and not for the purpose of punishment (although the imposition of a sanction may be detrimental to an employee).

46. I note that you are 47F years of age and have worked in Centrelink since 9 February 2009. I note that you presently work as a Customer Service Advisor in S 47F . As an employee whose duties require regular access to Centrelink customer records, I consider that you have a high degree of responsibility to treat those records in an appropriate way. I regard the fact that you failed to do so as very serious.

47. I note that you have failed to comply with Centrelink's 'unauthorised access' rules on four (4) occasions over a period of a little over two (2) months from 1 December 2009 to 4 February 2010. Your actions related to the records of you and your father.

48. The fact that you have a small number of 'browses', all of which occurred in a confined period, and the fact that you have not previously been the subject of misconduct investigations indicates to me that your misconduct in this instance was out of character. Because your misconduct appears to have been out of character, I regard it as less serious than I would regard similar conduct engaged in by a Centrelink employee with a documented history of disregarding Centrelink policies - whether in relation to browsing or any other matter.

49. I note that you not only made unauthorised access to customer records, but you also performed a transaction by way of issuing an incoming statement to your father. Your actions may have caused you or a Centrelink customer to derive a benefit to which they would not otherwise have been entitled. I make no finding that your actions did cause you or a Centrelink customer to derive some benefit, but I do regard the fact that your conduct involved not only unauthorised access but also unauthorised transactions as a serious matter and as an aggravating factor.

50. I note that in your statement, you stated that *'I recall receiving privacy training; however I was not aware of how strict the privacy and confidentiality policy is. I knew I was not permitted to make any changes to my record or my father's record, but I thought it would be OK just to access the record if I did not make any changes'.* You added that *'I am sorry for having made these accesses. I now realise that accessing these records for any reason can be considered to be browsing, and I will ensure I do not make any unauthorised accesses in the future'.* I conclude that you genuinely regret your actions and believe that you have learned a lot about your responsibilities as a result of this investigation. This learning is a positive outcome for you and for Centrelink. I believe that your remorse for your actions is a mitigating factor in this instance.

51. Having considered the evidence, facts and mitigating and aggravating circumstances of this case, and in accordance with section 15 of the *Public Service Act 1999*, I recommend that the sanction of deductions from salary, by way of a fine of $600.00, be applied.

52. I am of the opinion that this sanction is appropriate in the circumstances as it aims to ensure the integrity of Centrelink's data is protected and provides you with an understanding that Centrelink takes situations involving unauthorised access to protected information very seriously. An officer with approximately fourteen (14) months experience, you have been employed by Centrelink during a period of heightened privacy awareness in Centrelink. The aforementioned staff instructions and policies have been supported by training programs at various times. You attended a Privacy Awareness Session during your induction on 9 February 2009. On 26 June 2009, you electronically acknowledged a Declarations of Confidentiality - Privacy, Security, Fraud Awareness and Conduct Responsibilities, which outlines employees' privacy and confidentiality responsibilities and includes a declaration that employees will undertake to read and abide by the policies contained within. I conclude that you have, therefore, been regularly made aware of your privacy and confidentiality responsibilities in a variety of different ways, and yet on a number of occasions, chose to ignore them.

53. I considered that a reprimand was too lenient a sanction, as I believe your breaches of the Code of Conduct were serious, and committed with knowledge of Centrelink's policies relating to Privacy and Confidentiality. The Australian public needs to have a high level of trust in Centrelink's ability to manage and protect personal information. Your unauthorised accesses to protected information are very serious in that they compromise our ability to maintain public confidence in these aspects of public service. The protection and management of customer information is at the core of the everyday business activities of the majority of Centrelink's employees, and any actions which impact on our ability to guarantee privacy and confidentiality to customers must be viewed as grave offences. Further, your actions have clear potential impacts on the reputation and standing of Centrelink in the community. The prohibitions on staff conduct exist both to ensure and to maintain the appearance of fair and ethical professional conduct. Your actions have the potential to erode both of these aspects of public confidence in Centrelink.

54. I have no confidence that if a lesser sanction were applied under subsection 15(1) of the *Public Service Act 1999*, you would not again misuse Centrelink records in future, if it suited you to do so. In searching for your own Centrelink customer record and that of your father, you failed to act in accordance with Centrelink policies, despite the fact that your connection to this customer meant that you were not authorised to access these records. I therefore do not consider that a lesser sanction would be an adequate response to the gravity of your conduct.

55. Finally, I considered that the sanctions of demotion, reassignment of duties and termination of employment were too harsh. Other than the one access to your father's record, whereby you issued an income statement, your unauthorised accesses appear to be primarily for the purpose of browsing. Whilst these accesses were unauthorised, they do not appear to have been made for the purpose of obtaining a benefit or an advantage for yourself or any other person. I conclude, on balance, that your awareness of Centrelink's 'unauthorised access' rules will develop and improve as a result of this process and you will become very aware of your obligations. I therefore believe that it is extremely unlikely you will commit a breach of privacy at any time in the future.

56. I have therefore decided that deductions from salary, by way of a fine of $600.00, as the most appropriate sanction. It represents a significant sum of money and thereby reflects the gravity of this offence.

s 47F
Professional Standards Officer
People Support
s 47F

18 May 2010