

8

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 found that 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 eight (8) separate occasions by accessing Centrelink online customer records, eg Income Support Information System (ISIS) concerning S22 47F your ex husband on 18/05/2009. S 22/47F, your sister, on 11/03/2009 and 20/04/2009. 22/47F, your sister's ex husband, on 16/01/2008, 02/10/2008 and 18/11/2008. 22/47F, your ex husband's sister, on 14/08/2008 and 21/01/2009.
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;
 - (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.

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

- 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. Privacy Incident Investigation Report dated 26/08/2009. 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;
 - b. copy of a Declaration of Confidentiality form signed and dated by you on 07/05/2007;
 - c. Electronic Declaration of Confidentiality signed by you on 07/05/2008 and 07/05/2009.

REPORT OF THE DECISION MAKER ON
SUSPECTED BREACH OF THE CODE OF CONDUCT
BY S 22 / 47E

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. 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

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

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...

10. 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.

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

11. 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.
12. 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~~

13. 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.
14. 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....
15. 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.
16. There is no record of access for you in the Inadvertent Access Register.

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 07/02/2007, you were engaged as an ongoing employee of Centrelink. You are now a Customer Service Advisor at the APS 4 level, working in S 47F

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

19. In summary, you have worked at Centrelink for a period of 3 years and 1 month. I note as at the date of the last suspected unauthorised access on 18/05/2009, you had worked at Centrelink for a period of 2 years and 3 months.
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.

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

24. On 07/05/2007 you attended a Centrelink Privacy/Disciplinary Awareness Session in S 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. On 07/05/2007 you signed a form to indicate that you had received the Confidentiality Booklet. You undertook to read the Confidentiality Booklet and to abide by the rules it contained. 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 07/05/2007 you signed a form to indicate that you had received the Confidentiality Booklet. 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.
27. On 16 February 2007, an email was sent to all employees regarding an incident in the media involving possible release of Centrelink customer information. Given this email was sent as an 'important.information' email bcc to the inbox of each Centrelink employee, I am satisfied on the balance of probabilities that you received this information. This email reminded employees that unauthorised access to, use or disclosure of customer information is an offence which may attract a period of imprisonment.
- 'It is very important that all staff are clear that the unauthorised disclosure of protected customer information is a very serious breach of confidentiality, and the obligation to maintain the confidentiality of protected information continues even after an employee leaves Centrelink. Any unauthorised access to, use or disclosure of protected customer information is an offence which may attract a period of imprisonment.'
28. On 5 April 2007, an email was sent to all employees regarding the issue of access to customer records and conflict of interest. Given this email was sent as an 'important.information' email bcc to the inbox of each Centrelink employee, I am satisfied on the balance of probabilities that you received this information. This email advised employees of the following:
- 'Our policy is to avoid conflicts of interest all together, but having said that, there are some obvious situations where rather than just avoid a customer, the conflict of interest needs to be and can be managed.
- There are procedures in place that allow you to deal with these situations by declaring the relationship to your team leader or manager prior to accessing or assessing the customer's record. You can find these in the Chief Executive Instruction (CEI 20), and in the Privacy and Confidentiality Manual.'
29. On the basis of this evidence, I am satisfied that you knew, or ought to have known, that:
- accessing records and processing activities concerning you, your family and/or acquaintances is not permitted by Centrelink;

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

- 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

- 30. Attached to this draft report is a Privacy Incident Investigation Report dated 26/08/2009. 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 are not included in my report. Arrangements can be made for you to view these if you wish.
- 31. The Privacy Incident Investigation Report describes and analyses evidence which tends to suggest that you have accessed online customer records concerning your ex husband, your sister, your sister's ex husband and your ex husband's sister.
- 32. I propose to adopt the content of the Privacy Incident Investigation Report as my findings of fact in relation to your access to customer records concerning your ex husband, your sister, your sister's ex husband and your ex husband's sister.
- 33. There was no evidence that you accesses the Inadvertent Access Register.
- 34. Customer Record Access Monitor (CRAM) reports indicate that you accessed the Centrelink records of 22 / 47F, your ex husband. 22 / 47F, your sister. 22 / 47F, your sister's ex husband and 22/47F, your ex husbands sister between 16 January 2008 to 18 May 2009. You acknowledge accessing your sister 22/47F's Centrelink record and also performing a transaction resulting in the issue of S 47F forms. You have stated that you don't remember accessing 22/47F, your ex husband's, Centrelink record, however the CRAM report clearly shows that you have keyed in his surname, first name and date of birth into the name search facility, this indicates that the access of this record was deliberate and not accidental. The PED screen was accessed and there was no documentation to indicate why this record was accessed. Your statement in relation to the access of 22/47F, your sisters ex husband, Centrelink record indicates that this access would have been part of your duties, however CRAM report demonstrates that you accessed 22/47F record on three different occasions using the name search facility by keying in nis surname, first initial and date of birth. On two occasions 22/47F record was not documented with why the record was accessed. The PED, CH and FTS screens were accessed. On one occasion a document was created stated that the customer contacted the S 47F regarding a Section 47F. The PED, ATOSW, FRCS and FLSC screens were accessed. Given the size of the organisation it is unlikely that in a 10 month period you would have been randomly selected to take the enquiry of your sister's ex husband on 3 separate occasions. You stated that you do not know 22/47F, however she is the sister of your ex husband. You also said that access to her record would have been during your normal working duties. You accessed your ex sister in law record on 14/08/2008 and navigated to the PED, FIPY, PS and DOC. The document stated that the customer contacted regarding future payment. Your access to 22/47F record on the 21/01/2009 was gained through several attempts. You keying in surname 22/47F and first initial 47F in the name search. You then keyed in S 22 / 47F's name, 22/47F husband as well as her daughter S 22/47F name. You accessed the PED and FID screens and did not document

REPORT OF THE DECISION MAKER ON
SUSPECTED BREACH OF THE CODE OF CONDUCT
BY S 22 / 47E

the record regarding why this accessed occurred. On the balance of the evidence and facts established in this case my view is that you have breached the elements of the APS Code of Conduct outlined in point 4.

35. Based on the evidence contained in the Privacy Incident Investigation Report, it is my conclusion that you did access Centrelink's records concerning your sister and her ex husband and your ex husband and his sister 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

36. 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.**

37. 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.**

38. 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**

39. 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.

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

- (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.
40. 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
41. 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 your sister, her ex husband, your ex husband and his sister.. 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.
42. I am satisfied that your conduct, particularly your ongoing pattern of disregarding 'unauthorised access' Centrelink policies, represents a failure to uphold the APS Values, which are set out in section 10 of the 1999 Act.
43. 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 your sister, her ex husband, your ex husband and his sister at all. You did not behave in this way and thus demonstrated a failure to behave ethically in relation to those records.

SANCTION

44. 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).
45. I note that you are 47F years of age and have worked in Centrelink since 07/02/2007. 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.
46. I note that you have failed to comply with Centrelink's 'unauthorised access' rules on 8 occasions over a period of 21/10/2008 to 18/05/2009. Your actions related to the records of your sister, her ex husband, your ex husband and his sister.
47. I note that you not only made unauthorised access to customer records, but you also performed transactions including sending out S 47F forms to your sister. Your actions may have caused you or a Centrelink customer to derive a benefit to which they would not otherwise have been entitled. I do not propose to make any 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

REPORT OF THE DECISION MAKER ON
SUSPECTED BREACH OF THE CODE OF CONDUCT
BY § 47F

also unauthorised manipulation of Centrelink data as a serious matter and as an aggravating factor.

48. 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 propose to recommend that the sanction of a reduction in salary of 5% for a period of six months be applied.
49. I am of the opinion that this sanction is appropriate in the circumstances, because of the seriousness of your case and the fact that you performed a transaction on your sister, § 47F Centrelink record. The fact that your statement regarding this matter contains misleading information about your relationship with your ex sister in law has influenced the recommended sanction. I have no confidence that if a lesser sanction available under subsection 15(1) of the *Public Service Act 1999*, such as a reprimand were applied, you would not again misuse Centrelink records in the future, if it suited you to do so.
50. I do not consider that a lesser sanction would be an adequate response to the gravity of your conduct.

§ 47F

Investigating Officer

§ 47F

30/03/2010