

**From:** s47F  
**To:** s47F  
**Subject:** FW: Notification of Data Compromise [DLM=For-Official-Use-Only]  
**Date:** Friday, 1 December 2017 10:42:05 AM  
**Attachments:** [Letter to OAIC.PDF](#)

---

**From:** HOBDEN, Tracy  
**Sent:** Monday, 23 October 2017 9:34 PM  
**To:** enquiries@oaic.gov.au  
**Cc:** DILLEY, Scott <Scott.DILLEY@dss.gov.au>  
**Subject:** Notification of Data Compromise [DLM=For-Official-Use-Only]

Good evening

Please find attached a letter detailing a data compromise within the Department of Social Services.

A hard copy of the letter will also be provided.

Kind regards

Tracy

---

**Tracy Hobden**

**Branch Manager**

Financial Management and Procurement

Department of Social Services

**P:** 02 6146 3887 | **M:** s47F

| **E:** [tracy.hobden@dss.gov.au](mailto:tracy.hobden@dss.gov.au)

DSS acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

---



**Australian Government**  
**Department of Social Services**

Mr Timothy Pilgrim PSM  
Privacy Commissioner  
Office of the Australian Information Commissioner  
GPO Box 5218  
Sydney NSW 2001

By email: [enquiries@oaic.gov.au](mailto:enquiries@oaic.gov.au)

Dear Mr Pilgrim

**Notification of privacy breach**

The Department of Social Services (Department) was notified of a compromise of credit card data on 3 October 2017 and immediate action was taken to contain the incident. Details of the incident and response are noted below.

**Breach incident**

1. On Tuesday 3 October 2017, the Department was notified by the Australian Signals Directorate (ASD) of a compromise related to legacy credit card data held by Business Information Services, a contracted services provider (provider). Under guidance from ASD the provider subsequently secured the data later that day.
2. The compromise resulted from a misconfigured provider controlled server and was not a breach of the Department controlled IT environment.
3. The data compromised included credit card transactions, credit card numbers, employee names (current and former), Australian Government Service numbers and expired system passwords, for the period 2004 to 2015. The information had been provided by the Department to enable a data migration process by the provider. The data had been on the misconfigured server since approximately June 2016.
4. There is no evidence of improper use of the Department's credit cards to date and effective credit card controls have been maintained throughout the period of potential exposure. There is also no evidence of broader misuse of the compromised data.

**Breach response**

5. An investigation of the breach was undertaken in consultation with the provider. This included an impact assessment, root cause analysis, resolution identification and remedial action to prevent a repeat of the incident.

6. The provider has reviewed their security processes and engaged an independent security consulting company to undertake an independent review. A quarterly security report and annual security audit report will be provided to the Department.
7. The Department has considered relevant factors, set out in the OAIC's Guide to Data Breach Notification, including whether notification of individuals is appropriate in the circumstances of this breach.

### Contact with individuals

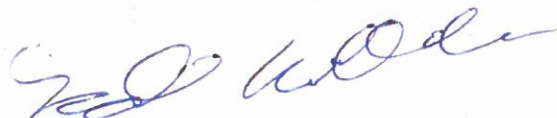
8. The Department has conducted an assessment of risk and has determined that the compromise relates to personal information as well as departmental data and could be considered a breach of Australian Privacy Principles 6 and 11.
9. However, based on:
  - the nature and volume of the personal information disclosed;
  - the steps taken by the Department and the provider to acknowledge and rectify the breach and mitigate further damage; and
  - the steps taken to prevent future breaches from occurring;

the Department considers that:

- the risk of further privacy infringement flowing from the current breach is low;
  - the probability of serious harm to individuals is low; and
  - there are limited additional measures available to individuals to mitigate the potential harm.
10. Given this, notification of affected current or former employees could lead to undue anxiety and desensitisation to future necessary notifications. The Department will continue to monitor the risk of harm to individuals, with consideration to the extent of further notification.
  11. Any complaints made in the first instance to the Department will be handled and responded to on a case-by-case basis in accordance with the Department's standard complaint handling processes.

I would be grateful for your acknowledgement of this letter and look forward to your response. The contact officer for this matter is <sup>s47F</sup> Principal Lawyer, who can be contacted on <sup>s47F</sup>

Yours sincerely,



Scott Dilley  
Chief Finance Officer and Group Manager  
Finance and Services Group

23 October 2017

**From:** Enquiries  
**To:** s47F  
**Cc:** [HOBDEN, Tracy](#)  
**Subject:** FW: DBN17/00129 Notification of Data Compromise [DLM=For-Official-Use-Only]  
**Date:** Tuesday, 24 October 2017 8:28:32 AM  
**Attachments:** [Letter to OAIC.PDF](#)

---

Our reference: DBN17/00129

Dear s47F

Thank you for your correspondence notifying the [Office of the Australian Information Commissioner](#) (the OAIC) of a possible data breach by DSS - Department of Social Services.

We have referred your correspondence to the OAIC's Dispute Resolution Branch for consideration. An officer from the relevant Dispute Resolution team will be in contact with you shortly.

In the meantime, you may wish to review the OAIC's published [Data Breach Notification Guide to handling personal information security breaches](#).

Should you wish to follow up on this matter, please contact the *OAIC Enquiries Line* on 1300 363 992 and quote the reference number at the top of this email.

Yours sincerely

Trish  
Enquiries Officer  
Office of the Australian Information Commissioner

**From:** HOBDEN, Tracy [mailto:Tracy.HOBDEN@dss.gov.au]  
**Sent:** Monday, 23 October 2017 9:34 PM  
**To:** Enquiries <enquiries@oaic.gov.au>  
**Cc:** DILLEY, Scott <Scott.DILLEY@dss.gov.au>  
**Subject:** DBN17/00129 Notification of Data Compromise [DLM=For-Official-Use-Only]

Good evening

Please find attached a letter detailing a data compromise within the Department of Social Services.

A hard copy of the letter will also be provided.

Kind regards

Tracy

---

**Tracy Hobden**

**Branch Manager**

Financial Management and Procurement

Department of Social Services

**P:** 02 6146 3887 | **M:** s47F | **E:** [tracy.hobden@dss.gov.au](mailto:tracy.hobden@dss.gov.au)

DSS acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

---

\*\*\*\*\*  
WARNING: The information contained in this email may be confidential.  
If you are not the intended recipient, any use or copying of any part  
of this information is unauthorised. If you have received this email in  
error, we apologise for any inconvenience and request that you notify  
the sender immediately and delete all copies of this email, together  
with any attachments.  
\*\*\*\*\*

**From:** Natalie Le  
**To:** s47F  
**Subject:** DBN17/00129 [DLM=Sensitive]  
**Date:** Tuesday, 31 October 2017 10:12:29 AM

---

Our reference: DBN17/00129

Ms s47F

Department of Social Services

s47F

Dear Ms s47F

I refer to the Department Of Social Services notification to the OAIC of 23 October 2017 regarding a data breach incident.

I attempted to phone you earlier today, however you were not available - I would appreciate it if you could contact me on the details below to discuss this matter further.

Kind regards,

**Natalie Le** | Assistant Director | Dispute Resolution Branch  
**Office of the Australian Information Commissioner**  
GPO Box 5218 Sydney NSW 2001 | [www.oaic.gov.au](http://www.oaic.gov.au)  
**Phone** (02) 8231 4206 | **Email** [natalie.le@oaic.gov.au](mailto:natalie.le@oaic.gov.au)

*Protecting information rights – advancing information policy*



\*\*\*\*\*

**WARNING:** The information contained in this email may be confidential.  
If you are not the intended recipient, any use or copying of any part of this information is unauthorised. If you have received this email in error, we apologise for any inconvenience and request that you notify the sender immediately and delete all copies of this email, together with any attachments.

\*\*\*\*\*

**From:** s47F  
**To:** "Natalie Le"  
**Subject:** RE: DBN17/00129 [DLM=Sensitive]  
**Date:** Thursday, 2 November 2017 11:22:23 AM  
**Attachments:** [Credit card data compromise DLMFor-Official-Use-Only \(9.12 KB\).msg](#)

---

Hi Natalie – I've left a voice mail message with you.

Apologies for not responding until this morning – I've been unavailable. More than happy to discuss our breach notification by phone or email.

Following the risk monitoring in relation to notifying affected individuals alluded to in our notice to you, the Department has now acted to notify its current staff (email notice attached), and is proceeding to contact former staff. There are some practical difficulties involved with this as you can imagine and we are working through them, but we intend to take all reasonable steps, and I'm happy to discuss them further with you.

Kind regards,

s47F

**Principal Lawyer**  
**Corporate Law Team**  
 Legal Services Branch  
 Corporate Services Group  
 Department of Social Services

s47F

**DSS acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.**

Note: This email and any attachments may contain confidential or legally privileged information (and neither are waived or lost if this email has been sent to you by mistake). If you are not the intended recipient, you must not use, disclose, copy or retain it. If you have received it in error, please let me know by reply email and then delete this email from your system and do not retain any copy. Recipients within DSS should seek assistance from DSS Legal before disseminating this email to third parties.

**From:** Natalie Le [mailto:natalie.le@oaic.gov.au]  
**Sent:** Tuesday, 31 October 2017 10:12 AM  
**To:** s47F >  
**Subject:** DBN17/00129 [DLM=Sensitive]

Our reference: DBN17/00129

s47F

Department of Social Services

s47F

Dear s47F

I refer to the Department Of Social Services notification to the OAIC of 23 October 2017

regarding a data breach incident.

I attempted to phone you earlier today, however you were not available - I would appreciate it if you could contact me on the details below to discuss this matter further.

Kind regards,

**Natalie Le** | Assistant Director | Dispute Resolution Branch  
**Office of the Australian Information Commissioner**  
GPO Box 5218 Sydney NSW 2001 | [www.oaic.gov.au](http://www.oaic.gov.au)  
**Phone** (02) 8231 4206 | **Email** [natalie.le@oaic.gov.au](mailto:natalie.le@oaic.gov.au)

*Protecting information rights – advancing information policy*



\*\*\*\*\*

**WARNING:** The information contained in this email may be confidential.  
If you are not the intended recipient, any use or copying of any part of this information is unauthorised. If you have received this email in error, we apologise for any inconvenience and request that you notify the sender immediately and delete all copies of this email, together with any attachments.

\*\*\*\*\*



**From:** DILLEY, Scott  
**Subject:** Credit card data compromise [DLM=For-Official-Use-Only]  
**Date:** Tuesday, 31 October 2017 1:32:05 PM

---

Good afternoon,

The Department of Social Services has been notified of a data compromise relating to staff profiles held within the Department's credit card management system prior to 2016. As a holder of a profile during that time I would like to provide you with the following details of this compromise.

The compromised data included name, user name, work phone number, work email, system password, AGS number, APS classification and organisation unit.

The compromise resulted from the actions of the Department's third party providers and is not a result of any of the Department's internal systems. The data has now been secured.

There is no evidence of misuse of the data. There is also no evidence of improper use of the Department's credit cards and effective credit card acquittal processes have been maintained throughout the period of exposure.

If you use the same password across both work and personal accounts you may wish to change and strengthen your password.

Whilst all affected credit cards have expired, any cards with the same card number as an expired card will be replaced. Our credit card administrator will be in contact with you shortly to arrange replacement cards. In the meantime, it is safe for you to continue using your existing cards.

I apologise for the need to bring this to your attention.

If you have any concerns, please talk with your SES Manager or contact [enquiries@dss.gov.au](mailto:enquiries@dss.gov.au).

Regards,

Scott

---

**Scott Dilley**

Chief Finance Officer and Group Manager

Finance and Services Group

Department of Social Services

**P:** 02 61460150 **M:** **S47F**

**F:** 02 62049476 **E:** [scott.dilley@dss.gov.au](mailto:scott.dilley@dss.gov.au)

---

**From:** Natalie Le  
**To:** s47F  
**Subject:** RE: DBN17/00129 [DLM=Sensitive]  
**Date:** Monday, 13 November 2017 9:53:25 AM

---

Hi s47F

Further to our phone discussion on 2 November 2017, I would appreciate it if DSS could provide an update in relation to data breach notification to previous staff.

Regards,

**Natalie Le** | Assistant Director | Dispute Resolution Branch  
**Office of the Australian Information Commissioner**  
GPO Box 5218 Sydney NSW 2001 | [www.oaic.gov.au](http://www.oaic.gov.au)  
**Phone** (02) 8231 4206 | **Email** [natalie.le@oaic.gov.au](mailto:natalie.le@oaic.gov.au)

*Protecting information rights – advancing information policy*



**From:** s47F  
**Sent:** Thursday, 2 November 2017 11:22 AM  
**To:** Natalie Le <[natalie.le@oaic.gov.au](mailto:natalie.le@oaic.gov.au)>  
**Subject:** RE: DBN17/00129 [DLM=Sensitive]

Hi Natalie – I've left a voice mail message with you.

Apologies for not responding until this morning – I've been unavailable. More than happy to discuss our breach notification by phone or email.

Following the risk monitoring in relation to notifying affected individuals alluded to in our notice to you, the Department has now acted to notify its current staff (email notice attached), and is proceeding to contact former staff. There are some practical difficulties involved with this as you can imagine and we are working through them, but we intend to take all reasonable steps, and I'm happy to discuss them further with you.

Kind regards,

s47F  
**Principal Lawyer**  
**Corporate Law Team**  
Legal Services Branch  
Corporate Services Group  
Department of Social Services  
s47F

DSS acknowledges the traditional owners of country throughout Australia, and their continuing

connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

Note: This email and any attachments may contain confidential or legally privileged information (and neither are waived or lost if this email has been sent to you by mistake). If you are not the intended recipient, you must not use, disclose, copy or retain it. If you have received it in error, please let me know by reply email and then delete this email from your system and do not retain any copy. Recipients within DSS should seek assistance from DSS Legal before disseminating this email to third parties.

**From:** Natalie Le [<mailto:natalie.le@oaic.gov.au>]  
**Sent:** Tuesday, 31 October 2017 10:12 AM  
**To:** s47F >  
**Subject:** DBN17/00129 [DLM=Sensitive]

Our reference: DBN17/00129

s47F  
Department of Social Services  
s47F

Dear Ms s47F

I refer to the Department Of Social Services notification to the OAIC of 23 October 2017 regarding a data breach incident.

I attempted to phone you earlier today, however you were not available - I would appreciate it if you could contact me on the details below to discuss this matter further.

Kind regards,

**Natalie Le** | Assistant Director | Dispute Resolution Branch  
**Office of the Australian Information Commissioner**  
GPO Box 5218 Sydney NSW 2001 | [www.oaic.gov.au](http://www.oaic.gov.au)  
**Phone** (02) 8231 4206 | **Email** [natalie.le@oaic.gov.au](mailto:natalie.le@oaic.gov.au)

*Protecting information rights – advancing information policy*



\*\*\*\*\*  
**WARNING:** The information contained in this email may be confidential.  
If you are not the intended recipient, any use or copying of any part of this information is unauthorised. If you have received this email in error, we apologise for any inconvenience and request that you notify the sender immediately and delete all copies of this email, together with any attachments.

\*\*\*\*\*

\*\*\*\*\*

WARNING: The information contained in this email may be confidential.  
If you are not the intended recipient, any use or copying of any part  
of this information is unauthorised. If you have received this email in  
error, we apologise for any inconvenience and request that you notify  
the sender immediately and delete all copies of this email, together  
with any attachments.

\*\*\*\*\*

**From:** s47F  
**To:** "Natalie Le"  
**Cc:** GRINSELL-JONES, Alan  
**Subject:** RE: DBN17/00129 [DLM=Sensitive]  
**Date:** Monday, 13 November 2017 4:36:29 PM

---

Dear Natalie

Thanks for your email. I can confirm the following:

- The distribution of notices by post to all former DSS/FaHCSIA/FaCS staff between 2004 and 2015 who:
  - had a credit card profile (i.e. this is more staff than had a credit card); and
  - whose last known residential address is available to the department;
 was completed last week and 6598 letters were sent out on Monday 6 November 2017.
- The letters stated:

*The Department of Social Services has been notified of a data compromise relating to staff profiles within the Department's credit card management system prior to 2016. As a holder of a profile during that time I would like to provide you with the following details about this compromise.*

*The compromised data included name, user name, work phone number, work email, system password, AGS number, APS classification and organisation unit. The compromise resulted from the actions of the Department's third party provider and is not a result of any of the Department's internal systems. The data has now been secured.*

*There is no evidence of misuse of the data. There is also no evidence of improper use of the Department's credit cards and effective credit card acquittal processes have been maintained throughout the period of the compromise.*

*If you have used the same password across both work and personal accounts you may wish to change and strengthen your password.*

*I apologise for the need to bring this to your attention. If you have any concerns, please email my team on [enquiries@dss.gov.au](mailto:enquiries@dss.gov.au).*

[Signed]  
 Scott Dilley  
 Chief Finance Officer and Group Manager  
 Finance and Services Group

- I understand that a very small number of enquiries were received in response to the internal notice sent on 31 October 2017 (<10). It is too early to gauge the level of response to the external notice.

If you have any other questions about this breach and the Department's notification response, please don't hesitate to contact me.

Kind regards,

s47F

**Principal Lawyer**  
**Corporate Law Team**  
Legal Services Branch  
Corporate Services Group  
Department of Social Services  
s47F

DSS acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

Note: This email and any attachments may contain confidential or legally privileged information (and neither are waived or lost if this email has been sent to you by mistake). If you are not the intended recipient, you must not use, disclose, copy or retain it. If you have received it in error, please let me know by reply email and then delete this email from your system and do not retain any copy. Recipients within DSS should seek assistance from DSS Legal before disseminating this email to third parties.

**From:** Natalie Le [mailto:natalie.le@oaic.gov.au]  
**Sent:** Monday, 13 November 2017 9:53 AM  
**To:** s47F  
**Subject:** RE: DBN17/00129 [DLM=Sensitive]

Hi s47F

Further to our phone discussion on 2 November 2017, I would appreciate it if DSS could provide an update in relation to data breach notification to previous staff.

Regards,

**Natalie Le** | Assistant Director | Dispute Resolution Branch  
**Office of the Australian Information Commissioner**  
GPO Box 5218 Sydney NSW 2001 | [www.oaic.gov.au](http://www.oaic.gov.au)  
**Phone** (02) 8231 4206 | **Email** [natalie.le@oaic.gov.au](mailto:natalie.le@oaic.gov.au)

*Protecting information rights – advancing information policy*



**From:** s47F  
**Sent:** Thursday, 2 November 2017 11:22 AM  
**To:** Natalie Le <[natalie.le@oaic.gov.au](mailto:natalie.le@oaic.gov.au)>  
**Subject:** RE: DBN17/00129 [DLM=Sensitive]

Hi Natalie – I've left a voice mail message with you.

Apologies for not responding until this morning – I've been unavailable. More than happy to discuss our breach notification by phone or email.

Following the risk monitoring in relation to notifying affected individuals alluded to in our notice to you, the Department has now acted to notify its current staff (email notice attached), and is proceeding to contact former staff. There are some practical difficulties involved with this as you can imagine and we are working through them, but we intend to take all reasonable steps, and I'm happy to discuss them further with you.

Kind regards,

s47F

**Principal Lawyer**  
**Corporate Law Team**  
 Legal Services Branch  
 Corporate Services Group  
 Department of Social Services  
 s47F

**DSS acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.**

Note: This email and any attachments may contain confidential or legally privileged information (and neither are waived or lost if this email has been sent to you by mistake). If you are not the intended recipient, you must not use, disclose, copy or retain it. If you have received it in error, please let me know by reply email and then delete this email from your system and do not retain any copy. Recipients within DSS should seek assistance from DSS Legal before disseminating this email to third parties.

**From:** Natalie Le [<mailto:natalie.le@oaic.gov.au>]

**Sent:** Tuesday, 31 October 2017 10:12 AM

**To:** s47F >

**Subject:** DBN17/00129 [DLM=Sensitive]

Our reference: DBN17/00129

Ms s47F

Department of Social Services

s47F

Dear Ms s47F

I refer to the Department Of Social Services notification to the OAIC of 23 October 2017 regarding a data breach incident.

I attempted to phone you earlier today, however you were not available - I would appreciate it if you could contact me on the details below to discuss this matter further.

Kind regards,

**Natalie Le** | Assistant Director | Dispute Resolution Branch  
**Office of the Australian Information Commissioner**  
GPO Box 5218 Sydney NSW 2001 | [www.oaic.gov.au](http://www.oaic.gov.au)  
**Phone** (02) 8231 4206 | **Email** [natalie.le@oaic.gov.au](mailto:natalie.le@oaic.gov.au)

*Protecting information rights – advancing information policy*



\*\*\*\*\*  
WARNING: The information contained in this email may be confidential.  
If you are not the intended recipient, any use or copying of any part  
of this information is unauthorised. If you have received this email in  
error, we apologise for any inconvenience and request that you notify  
the sender immediately and delete all copies of this email, together  
with any attachments.  
\*\*\*\*\*

\*\*\*\*\*  
WARNING: The information contained in this email may be confidential.  
If you are not the intended recipient, any use or copying of any part  
of this information is unauthorised. If you have received this email in  
error, we apologise for any inconvenience and request that you notify  
the sender immediately and delete all copies of this email, together  
with any attachments.  
\*\*\*\*\*



**From:** Natalie Le  
**To:** s47F  
**Subject:** DBN17/00129 [DLM=Sensitive]  
**Date:** Friday, 17 November 2017 8:14:23 AM

---

Our reference: DBN17/00129

Ms s47F

Department Of Social Services

s47F

Dear Ms s47F

### Data Breach Notification by the Department of Social Services

Thank you for notifying the Office of the Australian Information Commissioner (OAIC) about a data breach incident involving the Department of Social Services (DSS).

DSS advise that on 3 October 2017, it became aware that personal information held by a contracted service provider (CSP) was held on an insecure server for approximately 16 months. The personal information affected in this incident included employee names, Australian Government Service numbers and expired systems passwords.

#### Response to the data breach

In response to the incident, DSS took steps to investigate the incident including an impact assessment, root cause analysis, resolution identification and remedial action and found that there is no evidence of improper use of the data. DSS also advise that the CSP has reviewed its security processes and engaged an independent security consulting company to undertake an independent review.

DSS has also taken steps to notify all current staff members of the incident and 6598 former DSS, FaHCSIA and FaCS staff between 2004 and 2015 who had a credit card profile and whose last known residential address is available to the department. The notification included the following statement:

If you have used the same password across both work and personal accounts you may wish to change and strengthen your password.

#### OAIC guidance

Organisations covered by the Privacy Act 1988 (Cth)(the Privacy Act) have obligations under Australian Privacy Principle (APP) 11 to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and unauthorised access, modification or disclosure.

The OAIC's [Guide to securing personal information](#) (the PI Security Guide) contains information about reasonable steps APP entities should consider taking to protect the personal information they hold from misuse, interference, loss and from unauthorised access, use, modification or disclosure, as required by APP 11 of the Privacy Act.

**Next steps**

In light of the steps DSS has taken in response to the data breach, the OAIC does not intend to take any action in response to your data breach notification at this time.

However, if we receive a complaint from individuals affected by the incident, we will deal with that complaint on its merits and will refer to the information provided in your notification.

Regards,

**Natalie Le** | Assistant Director | Dispute Resolution Branch  
**Office of the Australian Information Commissioner**  
GPO Box 5218 Sydney NSW 2001 | [www.oaic.gov.au](http://www.oaic.gov.au)  
**Phone** (02) 8231 4206 | **Email** [natalie.le@oaic.gov.au](mailto:natalie.le@oaic.gov.au)

*Protecting information rights – advancing information policy*



\*\*\*\*\*  
**WARNING: The information contained in this email may be confidential.**  
If you are not the intended recipient, any use or copying of any part of this information is unauthorised. If you have received this email in error, we apologise for any inconvenience and request that you notify the sender immediately and delete all copies of this email, together with any attachments.  
\*\*\*\*\*

**From:** s47F  
**To:** [Natalie Le](#)  
**Subject:** RE: DBN17/00129 [DLM=Sensitive]  
**Date:** Tuesday, 21 November 2017 4:39:29 PM

---

Many thanks Natalie – much appreciated.

s47F

**Principal Lawyer**  
**Corporate Law Team**  
 Legal Services Branch  
 Corporate Services Group  
 Department of Social Services  
 s47F

DSS acknowledges the traditional owners of country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to them and their cultures, and to elders both past and present.

Note: This email and any attachments may contain confidential or legally privileged information (and neither are waived or lost if this email has been sent to you by mistake). If you are not the intended recipient, you must not use, disclose, copy or retain it. If you have received it in error, please let me know by reply email and then delete this email from your system and do not retain any copy. Recipients within DSS should seek assistance from DSS Legal before disseminating this email to third parties.

**From:** Natalie Le [mailto:natalie.le@oaic.gov.au]  
**Sent:** Friday, 17 November 2017 8:14 AM  
**To:** s47F  
**Subject:** DBN17/00129 [DLM=Sensitive]

Our reference: DBN17/00129

Ms s47F  
 Department Of Social Services  
 s47F

Dear s47F

### Data Breach Notification by the Department of Social Services

Thank you for notifying the Office of the Australian Information Commissioner (OAIC) about a data breach incident involving the Department of Social Services (DSS).

DSS advise that on 3 October 2017, it became aware that personal information held by a contracted service provider (CSP) was held on an insecure server for approximately 16 months. The personal information affected in this incident included employee names, Australian Government Service numbers and expired systems passwords.

#### Response to the data breach

In response to the incident, DSS took steps to investigate the incident including an impact assessment, root cause analysis, resolution identification and remedial action and found that there is no evidence of improper use of the data. DSS also advise that the CSP has reviewed its security processes and engaged an independent security consulting company to undertake an independent review.

DSS has also taken steps to notify all current staff members of the incident and 6598 former DSS, FaHCSIA and FaCS staff between 2004 and 2015 who had a credit card profile and whose last known residential address is available to the department. The notification included the following statement:

If you have used the same password across both work and personal accounts you may wish to change and strengthen your password.

### OAIC guidance

Organisations covered by the Privacy Act 1988 (Cth)(the Privacy Act) have obligations under Australian Privacy Principle (APP) 11 to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and unauthorised access, modification or disclosure.

The OAIC's [Guide to securing personal information](#) (the PI Security Guide) contains information about reasonable steps APP entities should consider taking to protect the personal information they hold from misuse, interference, loss and from unauthorised access, use, modification or disclosure, as required by APP 11 of the Privacy Act.

### Next steps

In light of the steps DSS has taken in response to the data breach, the OAIC does not intend to take any action in response to your data breach notification at this time.

However, if we receive a complaint from individuals affected by the incident, we will deal with that complaint on its merits and will refer to the information provided in your notification.

Regards,

**Natalie Le** | Assistant Director | Dispute Resolution Branch  
**Office of the Australian Information Commissioner**  
GPO Box 5218 Sydney NSW 2001 | [www.oaic.gov.au](http://www.oaic.gov.au)  
**Phone** (02) 8231 4206 | **Email** [natalie.le@oaic.gov.au](mailto:natalie.le@oaic.gov.au)

*Protecting information rights – advancing information policy*



\*\*\*\*\*

WARNING: The information contained in this email may be confidential.  
If you are not the intended recipient, any use or copying of any part  
of this information is unauthorised. If you have received this email in  
error, we apologise for any inconvenience and request that you notify  
the sender immediately and delete all copies of this email, together  
with any attachments.

\*\*\*\*\*