



Notifiable Data Breach Form

Getting started

About this form

This form is used to inform the Australian Information Commissioner of an 'eligible data breach' where required by the *Privacy Act 1988*.

Part one is the 'statement' about a data breach required by section 26WK of the *Privacy Act*. If you are required to notify individuals of the breach, in your notification to those individuals you must provide them with the information you have entered into part one of the form.

The OAIC encourages entities to voluntarily provide additional information about the eligible data breach in part two of this form. Part two of the form is optional, but the OAIC may need to contact you to seek further information if you do not complete this part of the form.

Before completing this form, we recommend that you read our resource *What to include in an eligible data breach statement* (<https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/what-to-include-in-an-eligible-data-breach-statement>).

If you are unsure whether your entity has experienced an eligible data breach, you may wish to review the *Identifying eligible data breaches* (<https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches>) resource.

The OAIC will send an acknowledgement of your statement about an eligible data breach on receipt with a reference number.

You can save this form at any point and return to complete it within 3 days. To save your form, click on the **Save and Close** button on the top right-hand corner of this form. If you do not submit your saved form within 3 days, your saved information will be permanently erased.

Refreshing your browser will clear any information that you have not saved. If you need to refresh your browser while completing this form and wish to keep your changes, please save the form first.

Your personal information

We will handle personal information collected in this form (usually only your name and contact details) in accordance with the Australian Privacy Principles (<https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles>).

We collect this information to consider and respond to your breach notification. We may use it to contact you.

More information about how the OAIC handles personal information is available in our privacy policy (<https://www.oaic.gov.au/about-us/corporate-information/key-documents/privacy-policy-summary>).

Part one - Statement about an eligible data breach

The information that you provide to the OAIC in Part One of this form must also be included in your notification to individuals (if notification is required).

Organisation / agency details

You must complete this section

Organisation / agency name *

The Department of Home Affairs

Phone *

s.22(1)(a)(ii)

Email *

s.22(1)(a)(ii)

☐

International address

Address Line1 *

5 Chan Street

Address Line2

Suburb *

BELCONNEN

State *

ACT

Postcode *

2616

Other contact details

s. 47E(d)@homeaffairs.gov.au

Description of the eligible data breach

An eligible data breach arises when the following three criteria are satisfied:

1. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds (see What is a 'Data Breach' (<https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-1-data-breaches-and-the-australian-privacy-act/#what-is-a-data-breach?>))
2. this is likely to result in serious harm to one or more individuals (see Is Serious Harm Likely? (<https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/#is-serious-harm-likely>)), and
3. the entity has not been able to prevent the likely risk of serious harm with remedial action (see Preventing Serious Harm with Remedial Action (<https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/#preventing-serious-harm-with-remedial-action>))

This document is about the threshold at which an incident is considered an 'eligible data breach' that will be notifiable under the scheme unless an exception applies. Assessing a Suspected Data Breach (<https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/#assessing-a-suspected-data-breach>) provides guidance to entities about the process to follow when carrying out an assessment of 'whether there are reasonable grounds to suspect that there may have been an eligible data breach of the entity' under s 26WH.

Step 1- Is there an eligible data breach?

See s. 26WE(2) Privacy Act 1988 (Cth)

Step 2- Is serious harm likely?

- From the perspective of a reasonable person, would the data breach be likely to result in

- serious harm to an individual whose personal information was part of the data breach?
- 'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm

Further information on these two steps can be found here: identifying eligible data breaches (<https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/#identifying-eligible-data-breaches>)

You must complete this section

Please provide a description of the eligible data breach addressing the above steps in your response *

Voluntary Notification of Third-Party Breach

s. 47G(1)(a) occurred by a third party s. 47G(1)(a) in the s. 47G(1)(a) is an approved panel clinic and is part of the Departments offshore network its immigration medical examinations for Australian visa applicants s. 47G(1)(a) are not a contracted service provider.

s. 47G(1)(a) have advised of a suspected breach of its webserver which may have compromised visa applicant personal information.
The facts of the breach:

- s. 47G(1)(a) notified the Department on the 19th of January 2024 that their webserver had been compromised and the personal information of Australian Visa Applicants had been accessed.
- The personal information of applicants that accessed the webserver between 22 November 2023 to 9 January 2024 may have been compromised.
- SLEC became aware of the compromise on the 18th of January 2024 when they were alerted to the fact that an email had been sent to 182 applicants requesting credit card information.
- SLEC contacted all 182 applicants via phone advising them of the breach & requesting that they do not respond to the email. Of the 182 applicants, 16 were identified as Australian Visa applicants.
- s. 47G(1)(a) immediately notified their IT department and after further investigation, it was found that the information of 1831 Australian Visa applicants was accessed on the webserver, however, there was no evidence that their information had been downloaded.
- Notification letters were sent to all 1831 applicants, and a follow-up letter was sent to the 182 email recipients re-iterating the advice provided by phone.
- The online registration system of s. 47G(1)(a) collects clients' name, date of birth, gender, mother's middle name, civil status, nationality, contact number, complete address, email address, passport details, TRN or HAP ID, visa subclass, appointment date and time, and their agency name if applicable.
- The IT department of s. 47G(1)(a) has completely restricted access to the webserver and cyber security is monitoring all systems.

Based on the type of personal information collected, serious harm (potential identity fraud) may be likely.

Information involved in the data breach

The specific circumstances of the data breach are relevant when assessing whether there is a risk of serious harm to an individual. This may include consideration of the kinds of personal information involved in the data breach and the sensitivity of that information.

Further information can be found here:

- What is personal and sensitive information? (<https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information/#SensitiveInfo>)
- What is health information? (<https://www.oaic.gov.au/privacy/health-information/what-is-health-information/>)

You must complete this section

Kind or kinds of personal information involved in the data breach *

The online registration system of s. 47G(1)(a) collects clients' name, date of birth, gender, mother's middle name, civil status, nationality, contact number, complete address, email address, passport details, TRN or HAP ID, visa subclass, appointment date and time, and their agency name if applicable.

In addition, please select any categories that apply

- ☐ Financial details
(e.g. credit card number, transaction history, credit report)
- ☐ Tax file number TFN
- ☒ Identity information
(e.g. Date of Birth, Government Identifier such as Medicare, Centrelink Reference, passport, or driver license number)
- ☒ Contact information
(e.g. home address, phone number, email address)
- ☐ Health information
(see s. 6FA of the Privacy Act 1988 (Cth))
- ☐ Consumer Data Right (CDR) information
(e.g. information about banking customers sent/received via the CDR regime)
- ☐ Other sensitive information
(e.g. sexual orientation, political or religious views)

Recommended steps

You must complete this section

Steps your organisation/agency recommends that individuals take to reduce the risk that they experience serious harm as a result of this data breach *

s. 47G(1)(a) have contacted the affected individuals and requested that they do not release any financial information including credit card information.

The Department of Home Affairs Immi Account access is only accessible by username & password, which has not been compromised as a result of the s. 47G(1)(a) data breach.

Other entities affected

Key points

- The NDB scheme recognises that entities often hold personal information jointly. For example, one entity may have physical possession of the information, while another has legal control or ownership.
- In these circumstances, an eligible data breach of one entity will also be considered an eligible data breach of other entities that hold the affected information. Both will have obligations under the NDB scheme.
- In general, compliance by one entity will also be taken as compliance by each of the entities that hold the information. As such, only one entity needs to take the steps required by the NDB scheme. The NDB scheme leaves it up to the entities to decide which of them should do so.
- OAIC suggests that, in general, the entity with the most direct relationship with the individuals affected by the data breach should carry out notification.

For further information please refer to the following guidance: Data breaches involving more than one entity (<https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/#data-breaches-involving-more-than-one-entity>).

This section is optional

If the data breach described above was also a data breach of another organisation/agency, you may provide their identity and contact details to further assist individuals.

Was another organisation / agency affected?

Yes	No
-----	----

Part two - Additional information

The OAIC encourages entities to provide additional information to assist us in understanding the eligible data breach. Part two of the form is optional, but the OAIC may need to contact you to seek further information if you do not complete this part of the form. The OAIC recommends you complete as many questions as possible, but you may leave a field blank if the answer is not known.

The information that you provide on part two of the form does not need to be included in your notification to individuals, and you may request that it be held in confidence by the OAIC.

Your contact details

Title

s.22(1)(a)

Given name

s.22(1)(a)(ii)

Family name

s.22(1)(a)(ii)

Phone

s.22(1)(a)(ii)

Email

s.22(1)(a)(ii)

Breach details

Date the breach occurred

You may provide your best estimate if the exact date is not known.

11 Jan 2024

Date the breach was discovered

You may provide your best estimate if the exact date is not known

19 Jan 2024

Primary cause of the data breach

- ☒ **Malicious or criminal attack**
A malicious or criminal attack deliberately crafted to exploit known vulnerabilities for financial or other gain.
- ☐ **System fault**
A business or technology process error not caused by direct human error.
- ☐ **Human error**
An unintended action by an individual directly resulting in a data breach, for example inadvertent disclosure caused by sending a document containing personal information to the incorrect recipient.
- ☐ **Other**
- ☐ **Currently unknown**

Please provide more detail by selecting one of the following:

- ☐ **Theft of paperwork or data storage device**
- ☐ **Social engineering/impersonation**
An attack that relies heavily on human interaction to manipulate people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations.
- ☐ **Rogue employee/insider threat**
An attack by an employee or insider acting against the interests of their employer or other entity.
- ☒ **Cyber incident**
A cyber incident targets computer information systems, infrastructures, computer networks, or personal computer devices.

Please provide more detail by selecting one of the following:

- ☐ **Malware**
Software which is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.
- ☐ **Brute-force attack (compromised credentials)**
Automated software is used to generate a large number of consecutive guesses as to the value of the desired data, for example passwords.
- ☐ **Ransomware**
A type of malicious software designed to block access to data or a computer system until a sum of money is paid or other conditions are met.
- ☐ **Phishing (compromised credentials)**
An attack in which the target is contacted by email or text message by someone posing as a legitimate institution to lure individuals into providing personal information, sensitive information or passwords
- ☐ **Compromised credentials (method unknown)**
Credentials are compromised or stolen by methods unknown.
- ☒ **Hacking**
Exploiting a software or security weakness to gain access to a system or network, other than by way of phishing, brute-force attack or malware.
- ☐ **Other**

Number of individuals whose personal information is involved in the data breach

- ☐ 1
- ☐ 2 - 10
- ☐ 11 - 100
- ☐ 101 - 1,000
- ☒ 1,001 - 5,000
- ☐ 5,001 - 10,000
- ☐ 10,001 - 25,000
- ☐ 25,001 - 50,000
- ☐ 50,001 - 100,000
- ☐ 100,001 - 250,000
- ☐ 250,001 - 500,000
- ☐ 500,001 - 1,000,000
- ☐ 1,000,001 - 10,000,000
- ☐ 10,000,001 or more

Exact number of individuals whose personal information is involved in the data breach

Please provide your best estimate

1831

Number of individuals in **Australia** whose personal information is involved in the data breach

- ☒ 1
- ☐ 2 - 10
- ☐ 11 - 100
- ☐ 101 - 1,000
- ☐ 1,001 - 5,000
- ☐ 5,001 - 10,000
- ☐ 10,001 - 25,000
- ☐ 25,001 - 50,000
- ☐ 50,001 - 100,000
- ☐ 100,001 - 250,000
- ☐ 250,001 - 500,000
- ☐ 500,001 - 1,000,000
- ☐ 1,000,001 - 10,000,000
- ☐ 10,000,001 or more

Exact number of individuals in **Australia** whose personal information is involved in the data breach

Please provide your best estimate

0

Description of how the data breach occurred

Please provide any additional information about how the eligible data breach occurred that you did not provide above in section 1.

Cyber incident to the webserver of s. 47G(1)(a) became aware when affected individuals notified them that they had received an email with a link to obtain credit card payment. 182 individuals received the credit card payment link email.

Description of any action, including remedial action, you have taken, or you are intending to take, to assist individuals whose personal information was involved in the data breach

s. 47G(1)(a) have sent notification letters to all 1831 individuals who have had their information accessed. Of those 1831, 182 individuals have also been contacted by phone to advise of the incident. Passwords for all individuals have been reset.

Description of any action you have taken, or you are intending to take, to prevent reoccurrence.

s. 47G(1)(a) have ceased access to the webserver and are implementing further security measures.

How do you intend to notify individuals who are likely to be at risk of serious harm as a result of the data breach? When will this occur?

If you do not intend to notify individuals because of an exception under s 26WN or s 26WP, please provide your reasons for relying on the relevant exception.

Further information can be found here:

- *Notifying individuals about an eligible data breach (<https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/#notifying-individuals-about-an-eligible-data-breach>)*
- *What to include in an eligible data breach statement (<https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/#what-to-include-in-an-eligible-data-breach-statement>)*
- *Exceptions to notification obligations (<https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/#exceptions-to-notification-obligations>)*

s. 47G(1)(a)

have sent notification letters to 1831 individuals and follow up letters to the 182 individuals contacted via phone.

List any other data protection authorities, law enforcement bodies or regulatory bodies that you have reported this data breach to *

- ☐ Australian Cyber Security Centre (ACSC)
- ☐ Australian Taxation Office (ATO)
- ☐ Australian Prudential Regulation Authority (APRA)
- ☐ Australian Securities and Investments Commission (ASIC)
- ☐ Other

You may wish to separately report an incident (<https://www.acsc.gov.au/incident.html>) to the Australian Cyber Security Centre if it raises cyber security concerns.

Additional information

Is there any other information you wish to provide at this stage, or any matters that you wish to draw to the OAIC's attention?

You can provide additional information below, or attach supporting documents when you submit this form.

If you wish to provide further information or documents after you submit the form, you may email them to enquiries@oaic.gov.au.

Please find attached copies of the sample notifications sent by E-47G(1)(a) to the affected individuals.

You may attach other relevant information that supports your notification by using the "upload file" button below.

*Files you attach **must**:*

- be in *.pdf, *.docx, *.doc, *.txt, *.jpg, *.gif or *.png format
- be no more than five files
- in total be no larger than 20MB.

[Sample Letter - 1831 \(002\).pdf](#)

[Sample Letter - 182 \(002\).pdf](#)

Inconfidence Request

The OAIC will respect the confidence of commercially or operationally sensitive information provided voluntarily in support of a data breach notification, and will only disclose this information after consulting with you, and with your agreement or where required by law.



I request that the information provided in Part Two of this form is held by the OAIC in confidence

Please provide further information to support the request *

I request that the information provided in part two of this form is held by the OAIC in confidence.

Submission

Submitting your form

Please review the information that you have provided about the data breach. If you would like to change anything, you can return to the relevant section by using the **Go Back** button.

Once you are ready to submit your form, click the **Submit** button below.

Once you submit your form, you will be taken to a confirmation page. This page will provide a receipt number for your submission, and you will be able to download a copy of your completed form or have a copy sent to an email address of your choice.

1/25/24, 12:03 PM

s. 47G(1)(a)

s. 47G(1)(a)

s. 47G(1)(a)

Notification Letter

1 message

s. 47G(1)(a)

Wed, Jan 17, 2024 at 11:31 PM

To: s. 47G(1)(a)@gmail.com

Confidential and Privileged Communication

17 January 2024

Dear s. 47G(1)(a) Patron,

s. 47G(1)(a)

On January 15, 2024, we have determined an event where an unauthorized incident gained access to s. 47G(1)(a). This system is entirely separate and not related to our main hospitals. We have not found evidence that your information was taken or acquired. We note that when you registered, you provided your name, alias, date of birth, gender, mother's maiden name, civil status, contact number, complete address, email address, passport details, s. 47G(1)(a) case number, visa category and interview date, covid vaccine details, date of previous x-ray and s. 47G(1)(a) medical exam, appointment date and time, and possibly decryptable passwords (for those who created accounts). Your medical results for tests conducted by s. 47G(1)(a) were not included in the involved information.

We immediately conducted actions to contain and mitigate the situation, including making the website server completely inaccessible externally, resetting passwords, and permanent disabling of features that are enabled by a client's password. As we prioritize the protection of your personal information and the preservation of your privacy, we have conducted a thorough investigation and taken prompt action to address the matter.

For further assistance or additional information regarding this incident, please do not hesitate to contact our dedicated support team at s. 47G(1)(a).

In your service,

s. 47G(1)(a)

Confidentiality Notice:

The contents of this email and any attachments are confidential and/or legally privileged and are intended solely for the addressee. If you received this email message in error, please immediately notify the sender by reply email and delete this message and its attachments. Any use, reproduction, or dissemination of this transmission by persons or entities other than the intended recipient is strictly prohibited.



s. 47G(1)(a)

to [REDACTED]

Thu, Jan 11, 7:38 PM

**STRICTLY CONFIDENTIAL**

January 11, 2024

[REDACTED]

Dear Sir/Madam:

Thank you for taking the time to answer our call. As discussed over the phone, online credit card payment services for s. 47G(1)(a) website are currently unavailable. We would like to offer an alternative solution should you wish to make payments via credit card. You are welcome to visit our clinic in person to facilitate the payment from 8:00 AM to 4:00 PM Mondays to Fridays. Our friendly staff will be more than happy to assist you with the payment process.

We apologize for any inconvenience this may cause and appreciate your understanding and cooperation during this time. As such, please be aware that we will not send any communication directing you to provide your credit card information online. If you have any questions or require further assistance, please do not hesitate to contact our clinic at s. 47G(1)(a) for US applicants or at s. 47G(1)(a) for Australia, Canada, New Zealand or South Korea applicants or via email at s. 47G(1)(a)

Thank you.

Sincerely,

s. 47F(1)

Vice-President and Head

s. 47G(1)(a)

Privacy and Confidentiality

This message, its thread, and any attachments are private and confidential. Except for the legitimate purpose of this message, no part of this message or identity of a person may be disclosed, reproduced or exhibited in any form or manner without the consent of the sender. In case of wrongful receipt of or unauthorized access to this message, please immediately inform the sender and permanently delete all wrongfully received copies.

↩ Reply

➦ Forward



Australian Government

Office of the Australian Information Commissioner

Our reference: DBN24/00149

Thank you for your statement notifying the Information Commissioner of a data breach.

If you have not done so already, please provide a copy of the notification that you have sent to affected individuals to databreaches@oaic.gov.au. This will assist our staff when assessing your notification.

If we require any further information, we will be in contact. If we receive a complaint from individuals affected by the incident, we will deal with that complaint on its merits.

Further resources

Entities covered by the *Privacy Act 1988* (Cth) 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. APP 6 also limits the circumstances in which an APP entity is permitted to disclose the personal information it holds. Please visit our website for more information on the [APPs](#).

The OAIC's [Guide to securing personal information](#) contains information about reasonable steps APP entities should consider taking to protect the personal information as required by APP 11 of the Privacy Act.

You may also find the OAIC's [Data breach preparation and response: a guide to managing data breaches in accordance with the Privacy Act 1988 \(Cth\)](#) useful in preparing for and responding to future data breaches.

If the breach you have reported is a cyber-security incident, you could also [report it to the Australian Cyber Security Centre](#) (ACSC). The ACSC can provide advice to organisations that have experienced a data breach, and reports to the ACSC help build the Australian Government's understanding of the cyber threat environment.

Yours sincerely

Office of the Australian Information Commissioner

6 February 2024

s.22(1)(a)(ii)

From: s.22(1)(a)(ii)@industry.gov.au
Sent: Tuesday, 6 February 2024 4:27 PM
To: s.22(1)(a)(ii)
Subject: Form Receipt - (Automated Notification) - Office of the Australian Information Commissioner [SEC=OFFICIAL:Sensitive]
Attachments: OAIC-NDB-130913.pdf



Reference
Code:
**OAIC-
NDB-
130913**

YOU SUBMITTED A FORM CALLED: NOTIFIABLE DATA BREACH FORM

Your form reference code is: **OAIC-NDB-130913**

To check the progress of your submission and/or confirm it has been received you should contact the agency that provides the form. These details are displayed below.

Please see the attached PDF for a copy of your form submission.

Office of the Australian Information Commissioner

<https://www.oaic.gov.au> | [1300 363 992](tel:1300363992) | enquiries@oaic.gov.au

GPO Box 5218, Sydney NSW 2001

Note: Please do not reply to this auto-generated email.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

March 19, 2024

Dear Values Client:

We hope this letter finds you well.

We are sending you this email to raise awareness about data protection and cybersecurity.

In January 2024, you were notified about an incident involving unauthorized access to the s. 47G(1)(a) s. 47G(1)(a). Since the incident, s. 47G(1)(a) has fortified its system security and engaged the services of a cybersecurity specialist to prevent similar incidents from happening in the future. Rest assured that the incident had no effect on your medical examination for an Australian visa.

When you registered online, you provided your name, date of birth, gender, mother's maiden name, civil status, contact number, complete address, email address, passport detail, and possibly your covid vaccine details, date of previous chest x-ray, and date of previous medical exam at s. 47G(1)(a). Up to this time, there has been no evidence that your personal information was taken or acquired but we still want to share the following tips to help protect your personal information:

DATA PROTECTION AND CYBERSECURITY TIPS

1. If you think your password is compromised, change it. Use a strong password or passphrase and, whenever applicable, use multi-factor authentication.
2. Be careful when checking your emails. Do not click on suspicious attachments, particularly those coming from strangers.
3. Avoid sharing your personal details, account information, or financial data by email or through phone.
4. If you do online banking, go to your bank's website by typing their web address directly into your web browser.
5. Monitor your bank or credit card account transactions for suspicious activity. Report unauthorized transactions to your bank immediately.
6. If you think you are a victim of identity theft, notify the National Privacy Commission.

Should you require further assistance, please do not hesitate to contact us via email at s. 47G(1)(a). Our team is available to answer any questions you may have and provide guidance on how to protect yourself from potentially fraudulent activity.

We are here as your partner both in healthcare and in protecting your personal information.

Sincerely yours,

s. 47G(1)(a)

s.22(1)(a)(ii)

From: s.22(1)(a)(ii)
Sent: Monday, 25 March 2024 4:27 PM
To: OAIC - Data Breaches
Cc: s. 47E(d) @homeaffairs.gov.au
Subject: CM: RE: Data breach notification involving the Department of Home Affairs - Our Ref: DBN24/00149 [SEC=OFFICIAL]
Attachments: Follow-up Notification.pdf

OFFICIAL

Good Afternoon s.22(1)(a)(i)

For further clarification, s. 47G(1)(a) is a member of the Australian Panel Network and not a contracted Service Provider for the Department, we therefore, have no contractual obligations with s. 47G(1)(a). The data breach notification was a voluntary notification on behalf of the panel clinic.

The Department of Home Affairs has been in contact with s. 47G(1)(a) to obtain a response in relation to the preliminary enquiries regarding the data breach and has obtained the following responses:

1. Specify what 'further security measures' s. 47G(1)(a) intends to implement to prevent future recurrence of a cyber-attack?

The following steps have been taken since the incident:

S. 47E(d)

Released by Department of Home Affairs
 under the Freedom of Information Act 1982

In relation to the 182 affected individuals that received the phishing emails, s. 47G(1)(a) has confirmed that in their original phone contact with each recipient, they had established that no one had accessed the link in the email or provided their credit card information, although, they will also receive a copy of the supplementary notification.

Thank you for your assistance and patience whilst we obtained the further information.

Kind regards

s.22(1)(a)(ii)

Assistant Director
Privacy Section
Privacy, FOI and Records Management Branch
Legal Group
Department of Home Affairs

s.22(1)(a)(ii)

OFFICIAL

From: OAIC - Data Breaches <databreaches@oaic.gov.au>
Sent: Tuesday, 12 March 2024 3:17 PM
To: s. 47E(d) @homeaffairs.gov.au>
Cc: s.22(1)(a)(ii)
Subject: Data breach notification involving the Department of Home Affairs - Our Ref: DBN24/00149 [SEC=OFFICIAL]

Our Reference: DBN24/00149

Dear s.22(1)(a)(ii)

I refer to the statement of 6 February 2024 to the Office of the Australian Information Commissioner (OAIC) about a data breach incident involving the Department of Home Affairs (DHA).

DHA advised its third party offshore network medical examination provider, s. 47G(1)(a) experienced a cyber incident which resulted in unauthorised access to data held in the webserver.

The OAIC is making preliminary inquiries under s 42(2) of the *Privacy Act 1988* (Cth) (Privacy Act) about this matter. Given the possibility of an investigation, the OAIC asks that DHA retain any records it holds or controls relating to this matter.

Information sought by the OAIC

To assist the OAIC in assessing this matter, I would appreciate if DHA could respond to the following by **COB, 19 March 2024**:

1. Specify what 'further security measures' s. 47G(1)(a) intends to implement to prevent future recurrence of a cyber-attack?
2. What measures were in place, prior to the incident, to:
 - a. Detect and prevent suspicious activities and/or cyber-attack(s) similar to this one. If any, why did these measure(s) fail in this instance?

- b. Protect the personal information it holds.

Notification requirements under the NDB scheme

Where an entity has assessed that an eligible data breach has occurred, it must notify individuals at risk of serious harm and provide a statement to the Commissioner as soon as practicable, please refer to s26WG of the Privacy Act.

Where an entity is notifying affected individuals of an eligible data breach, the notification is expected to set out the following information:

1. The identity and contact details of the entity
2. A description of the eligible data breach
3. The kind, or kinds, of personal information affected
4. **Recommended steps that individuals can take**

The notifications issued by s.47G(1)(a) to the affected individuals did not include:

- For the 182 affected individuals that received phishing emails, the kind(s) of personal information affected i.e. credit card information may have been compromised
- For the 1,831 affected individuals, recommendations about the steps individuals should take in response to the eligible data breach.

The OAIC expects practical steps to be provided to affected individuals based on the kinds of information involved. The OAIC's guidance materials [Respond to a data breach notification](#) and [identity fraud](#) contains information on providing appropriate recommendations to the affected individuals.

Based on the above information, the OAIC recommends that s.47G(1)(a)/DHA provide a supplementary notifications which meet the above notification requirements. Please **also** confirm what date and how the supplementary notifications will be issued.

The OAIC would appreciate a copy of the supplementary notification(s) and response to our inquiries by **COB, 19 March 2024** via return email.

The OAIC would appreciate a response by **COB, 19 March 2024** via return email.

Regards,



s.22(1)(a)(ii)
Investigations Officer
Office of the Australian Information Commissioner
P s.22(1)(a)(ii) E s.22(1)(a)(ii)

s.22(1)(a)(ii)

The OAIC acknowledges Traditional Custodians of Country across Australia and their continuing connection to land, waters and communities. We pay our respect to First Nations people, cultures and Elders past and present.

[Subscribe to Information Matters](#)

Notice:

The information contained in this email message and any attached files may be confidential information, and may also be the subject of legal professional privilege. If you are not the intended recipient any use,

disclosure or copying of this email is unauthorised. If you received this email in error, please notify the sender by contacting the department's switchboard on 1300 488 064 during business hours (8:30am - 5pm Canberra time) and delete all copies of this transmission together with any attachments.

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

You may go back to previous pages using the buttons below:

Submission

Submission

Please review the information that you have provided about the data breach. If you would like to change anything, you can return to the relevant section by using the navigation buttons at the top of the screen

Once you are ready to submit your form, click the Submit button below.

Once you submit your form, you will be taken to a confirmation page. This page will provide a reference code for your submission, and you will have a copy sent to the email address provided.

Part one - Statement about an eligible data breach

Fields with an Asterix () are mandatory and you will need to provide a selection or response.*

The information that you provide to the OAIC in Part One of this form must also be included in your notification to individuals (if notification is required).

Organisation / agency details

Organisation / agency name *

Department of Home Affairs

Phone *

s.22(1)(a)(ii)

Email *

s. 47E(d) homeaffairs.gov.au

International Address:

Street Address 1 *

5 Chan Street

Street Address 2

City/Suburb *

Belconnen

State *

ACT

Postcode *

2616

Other contact details

s.22(1)(a)(ii)

Description of eligible data breach

An eligible data breach arises when the following three criteria are satisfied:

1. There is unauthorized access to or unauthorized disclosure of personal information, or a loss of personal information, that an entity holds (see [What is a 'Data Breach'?](#))
2. This is likely to result in serious harm to one or more individuals (see [Is Serious Harm Likely?](#)), and
3. The entity has not been able to prevent the likely risk of serious harm with remedial action (see [Preventing Serious Harm with Remedial Action](#))

This document is about the threshold at which an incident is considered an 'eligible data breach' that will be notifiable under the scheme unless an exception applies. [Assessing a Suspected Data Breach](#) provides guidance to entities about the process to follow when carrying out an assessment of 'whether there are reasonable grounds to suspect that there may have been an eligible data breach of the entity' under s 26WH.

Step 1: Is there an eligible data breach?

See s. 26WE(2) Privacy Act 1988 (Cth)

Step 2: Is serious harm likely?

From the perspective of a reasonable person, would the data breach be likely to result in serious harm to an individual whose personal information was part of the data breach?

'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

Further information on these two steps can be found here: [identifying eligible data breaches](#)

Please provide a description of the eligible data breach addressing the above steps in your response *

On Monday 8 July 2024 a Departmental employee within s. 47E(d) sent out a 'business consult' email. The email was in relation to a s. 47E(d) s. 47E(d). Although the business consult process is standard procedure when a FOI request is received, the email was sent to various internal s. 47E(d) s. 47E(d) s. 47E(d). Upon realising the error, the responsible departmental employee requested in writing that the email be deleted as it was sent in error and re-issued the email to the correct business areas. A privacy breach report was provided to the Privacy Section in relation to the privacy breach. s. 47E(d)

s. 47E(d)

Information involved in the data breach

The specific circumstances of the data breach are relevant when assessing whether there is a risk of serious harm to an individual. This may include consideration of the kinds of personal information involved in the data breach and the sensitivity of that information.

Webform WEB-NDB-24-00073

Further information can be found here:

[What is personal and sensitive information?](#)

[What is health information?](#)

You must complete this section.

Kind or kinds of personal information involved in the data breach *

Names Departmental email addresses.

In addition, please select any categories that apply

- Financial details:
- Tax File Numbers:
- Identity information:
- Contact information: checked
- Consumer Data Right data:
- Health information:
- Other sensitive information:

Option Description

Financial details (*e.g. credit card number, transaction history, credit report*)

Identity information (*e.g. Date of Birth, Government Identifier such as Medicare, Centrelink Reference, passport, or driver license number*)

Contact information (*e.g. home address, phone number, email address*)

Health information (*see s. 6FA of the Privacy Act 1988 (Cth)*)

Consumer Data Right (CDR) Information (*e.g. information about banking customers sent/received via the CDR regime*)

Other sensitive information (*e.g. sexual orientation, political or religious views*)

Recommended steps

You must complete this section

Steps your organisation/agency recommends that individuals take to reduce the risk that they experience serious harm as a result of this data breach *

The Privacy Section made the following recommendations: - The responsible employee is provided with extra support and training, feedback and be reminded of their obligations under the Privacy Act 1988. Recommended that the incident be reported to the Security Branch. - **s. 47F(1)** **s. 47F(1)**. -The responsible Departmental employee requested in writing that the email sent in error be deleted and re-issued the email to the correct business areas. Additionally, the Privacy Section provided an assessment to both the responsible employee and **s. 47F(1)**

Other entities affected

Key points

Webform WEB-NDB-24-00073

- The NDB scheme recognises that entities often hold personal information jointly. For example, one entity may have physical possession of the information, while another has legal control or ownership.
- In these circumstances, an eligible data breach of one entity will also be considered an eligible data breach of other entities that hold the affected information. Both will have obligations under the NDB scheme.
- In general, compliance by one entity will also be taken as compliance by each of the entities that hold the information. As such, only one entity needs to take the steps required by the NDB scheme. The NDB scheme leaves it up to the entities to decide which of them should do so.
- OAIC suggests that, in general, the entity with the most direct relationship with the individuals affected by the data breach should carry out notification.

For further information please refer to the following guidance: [Data breaches involving more than one entity.](#)

This section is optional

If the data breach described above was also a data breach of another organisation/agency, you may provide their identity and contact details to further assist individuals.

Was another organisation / agency affected?

No

Part two - Additional information

Fields with an Asterix () are mandatory and you will need to provide a selection or response.*

The OAIC encourages entities to provide additional information to assist us in understanding the eligible data breach. Part two of the form is optional, but the OAIC may need to contact you to seek further information if you do not complete this part of the form. The OAIC recommends you complete as many questions as possible, but you may leave a field blank if the answer is not known.

The information that you provide on part two of the form does not need to be included in your notification to individuals, and you may request that it be held in confidence by the OAIC.

Your contact details

Title

s.22(1)(a)(ii)

Given name

s.22(1)(a)(ii)

Family name

s.22(1)(a)(ii)

Phone

s.22(1)(a)(ii)

Email

s.22(1)(a)(ii)

Breach details

Webform WEB-NDB-24-00073

Date the breach occurred

You may provide your best estimate if the exact date is not known.

08/Jul/2024

Date the breach was discovered

You may provide your best estimate if the exact date is not known.

09/Jul/2024

Primary cause of data breach

In the selection field below please choose the Primary cause of the data breach where:

Malicious or criminal attack is 'a malicious or criminal attack deliberately crafted to exploit known vulnerabilities for financial or other gain.'

System fault is 'a business or technology process error not caused by direct human error.'

Human error is 'an unintended action by an individual directly resulting in a data breach, for example inadvertent disclosure caused by sending a document containing personal information to the incorrect recipient.'

Primary cause of data breach

Human error

Please provide more details in the selection field below where:

Personal information sent to wrong recipient (email) is 'an unintended action by an individual directly resulting in a data breach, for example inadvertent disclosure caused by sending a document containing personal information to the incorrect recipient.'

Personal information sent to wrong recipient (fax) is where 'personal information is sent to the wrong recipient via facsimile machine, for example, as a result of fax number incorrectly entered or wrong fax number on file.'

Personal information sent to wrong recipient (mail) is where 'personal information is sent to the wrong recipient via postal mail, for example, as a result of transcribing error or wrong address on files.'

Personal information sent to wrong recipient (other) is where 'personal information is sent to the wrong recipient via channels other than email, fax or mail, for example, delivery by hand or uploading to web portal.'

Failure to use BCC when sending email is where 'sending an email to a group by including all recipient emails addresses in the 'To' or 'CC' field, thereby disclosing all recipient email address to all recipients.'

Insecure disposal is 'disposing of personal information in a manner that could lead to its unauthorised disclosure, for example, using a public rubbish bin to dispose of customer records instead of a secure document disposal bin.'

Loss of paperwork or data storage device is 'loss of a physical asset(s) containing personal information, for example, leaving a folder or a laptop on a bus.'

Unauthorised disclosure (failure to redact) if 'failure to effectively remove or de-identify personal information from a record before disclosing it.'

Unauthorised disclosure (verbal) is 'disclosing personal information without authorisation, verbally for

Webform WEB-NDB-24-00073

example, calling it out in a waiting room.'

Unauthorised disclosure (unintended release or publication) is 'unauthorised disclosure of personal information in a written format, including paper documents or online.'

Data Breach Details

PI sent to wrong recipient (email)

Number of individuals whose personal information is involved in the data breach

2 - 10

Exact number of individuals whose personal information is involved in the data breach

Please provide your best estimate

5

Number of individuals in **Australia** whose personal information is involved in the data breach

2 - 10

Exact number of individuals in **Australia** whose personal information is involved in the data breach

Please provide your best estimate

5

Description of how the data breach occurred

Please provide any additional information about how the eligible data breach occurred that you did not provide above in section 1

s. 47E(d)

During the process of sending out a 'business consult' email, the s. 47F(1) included group mailboxes and individual recipients s. 47F(1)) to which the email should not have been circulated to. s. 47F(1)

There were no attachments and the Content Manager (TRIM Link) has security access controls in place.

Description of any action, including remedial action, you have taken, or you are intending to take, to assist individuals whose personal information was involved in the data breach

The Privacy Section provided a privacy breach assessment s. 47E(d)

s. 47E(d)

The assessments concluded that a privacy breach had occurred, s. 47E(d)

s. 47E(d)

s. 47E(d)

Actions taken include: - Requesting all

recipients of the email delete and not further disseminate the information received -Provided s. 47F(1)

s. 47F(1) with information in relation to support services.

Description of any action you have taken, or you are intending to take, to prevent reoccurrence.

- Recommendations have been made for additional training and a reminder of obligations under the Privacy Act 1988. - Review of auditing processes prior to sending out 'business consult' emails in relation to FOI requests.

How do you intend to notify individuals who are likely to be at risk of serious harm as a result of the data breach? When will this occur?

If you do not intend to notify individuals because of an exception under s 26WN or s 26WP, please provide your reasons for relying on the relevant exception.

Further information can be found here:

- [Notifying individuals about an eligible data breach](#)

- [What to include in an eligible data breach statement](#)

s. 47E(d)

List any other data protection authorities, law enforcement bodies or regulatory bodies that you have reported this data breach to *

- Australian Cyber Security Centre (ACSC):
- Australian Taxation Office (ATO):
- Australian Prudential Regulation Authority (APRA):
- Australian Securities and Investments Commission (ASIC):
- Other: checked

Please specify *

This has not been reported to any other data protection authorities, law enforcement bodies or regulatory bodies.

You may wish to separately [report an incident](#) to the Australian Cyber Security Centre if it raises cyber security concerns.

Additional Information

Is there any other information you wish to provide at this stage, or any matters that you wish to draw to the OAIC's attention?

You can provide additional information below, or attach supporting documents when you submit this form.

If you wish to provide further information or documents after you submit the form, you may email them to databreaches@oaic.gov.au.

Included with this submission is a statement from the affected ABF Officer.

You may attach other relevant information that supports your notification by using the "upload file" button below.

Files you attach must:

*be in *.pdf, *.docx, *.doc, *.txt, *.jpg, *.gif, or *.png format*

be no more than five files

in total be no larger than 20MB

- Statement from affected ABF Officer (843.53 kB) Created date: 22/Jul/2024 09:15 AM

Inconfidence Request

The OAIC will respect the confidence of commercially or operationally sensitive information provided voluntarily in support of a data breach notification, and will only disclose this information after consulting with you, and with your agreement or where required by law.

I request that the information provided in Part Two of this form is held by the OAIC in confidence: checked

Please provide further information to support the request *

Webform WEB-NDB-24-00073

All necessary steps have been taken to redact information however, as this submission includes a statement **S. 47F(1)**, could you please seek permission from the Department in the event that on disclosure is required.



Australian Government

Office of the Australian Information Commissioner

Our reference: DBN24/00944

Thank you for your statement notifying the Information Commissioner of a data breach.

If you have not done so already, please provide a copy of the notification that you have sent to affected individuals to databreaches@oaic.gov.au. This will assist our staff when assessing your notification.

If we require any further information, we will be in contact. If we receive a complaint from individuals affected by the incident, we will deal with that complaint on its merits.

Further resources

Entities covered by the *Privacy Act 1988* (Cth) 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. APP 6 also limits the circumstances in which an APP entity is permitted to disclose the personal information it holds. Please visit our website for more information on the [APPs](#).

The OAIC's [Guide to securing personal information](#) contains information about reasonable steps APP entities should consider taking to protect the personal information as required by APP 11 of the Privacy Act.

You may also find the OAIC's [Data breach preparation and response: a guide to managing data breaches in accordance with the Privacy Act 1988 \(Cth\)](#) useful in preparing for and responding to future data breaches.

If the breach you have reported is a cyber-security incident, you could also [report it to the Australian Cyber Security Centre](#) (ACSC). The ACSC can provide advice to organisations that have experienced a data breach, and reports to the ACSC help build the Australian Government's understanding of the cyber threat environment.

Yours sincerely

Office of the Australian Information Commissioner

22 July 2024

You may go back to previous pages using the buttons below:

Submission

Submission

Please review the information that you have provided about the data breach. If you would like to change anything, you can return to the relevant section by using the navigation buttons at the top of the screen

Once you are ready to submit your form, click the Submit button below.

Once you submit your form, you will be taken to a confirmation page. This page will provide a reference code for your submission, and you will have a copy sent to the email address provided.

Part one - Statement about an eligible data breach

Fields with an Asterix () are mandatory and you will need to provide a selection or response.*

The information that you provide to the OAIC in Part One of this form must also be included in your notification to individuals (if notification is required).

Organisation / agency details

Organisation / agency name *

Department of Home Affairs

Phone *

s.22(1)(a)(ii)

Email *

s. 47E(d) homeaffairs.gov.au

International Address:

Street Address 1 *

5 Chan Street

Street Address 2

City/Suburb *

Belconnen

State *

ACT

Postcode *

2616

Other contact details

s.22(1)(a)(ii)

Description of eligible data breach

An eligible data breach arises when the following three criteria are satisfied:

1. There is unauthorized access to or unauthorized disclosure of personal information, or a loss of personal information, that an entity holds (see [What is a 'Data Breach'?](#))
2. This is likely to result in serious harm to one or more individuals (see [Is Serious Harm Likely?](#)), and
3. The entity has not been able to prevent the likely risk of serious harm with remedial action (see [Preventing Serious Harm with Remedial Action](#))

This document is about the threshold at which an incident is considered an 'eligible data breach' that will be notifiable under the scheme unless an exception applies. [Assessing a Suspected Data Breach](#) provides guidance to entities about the process to follow when carrying out an assessment of 'whether there are reasonable grounds to suspect that there may have been an eligible data breach of the entity' under s 26WH.

Step 1: Is there an eligible data breach?

See s. 26WE(2) Privacy Act 1988 (Cth)

Step 2: Is serious harm likely?

From the perspective of a reasonable person, would the data breach be likely to result in serious harm to an individual whose personal information was part of the data breach?

'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

Further information on these two steps can be found here: [identifying eligible data breaches](#)

Please provide a description of the eligible data breach addressing the above steps in your response *

s. 47E(d)

s. 47E(d)

s. 47E(d)

s. 47E(d)

We believe that a reasonable person could conclude that there is a likelihood of serious harm (s 26WG(g)) s. 47F(1)

Information involved in the data breach

The specific circumstances of the data breach are relevant when assessing whether there is a risk of serious harm to an individual. This may include consideration of the kinds of personal information involved in the data breach and the sensitivity of that information.

Webform WEB-NDB-24-00098

Further information can be found here:

[What is personal and sensitive information?](#)

[What is health information?](#)

You must complete this section.

Kind or kinds of personal information involved in the data breach *

Name Contact information (email, phone number) Visa application details

In addition, please select any categories that apply

- Financial details:
- Tax File Numbers:
- Identity information:
- Contact information: checked
- Consumer Data Right data:
- Health information: checked
- Other sensitive information:

Option Description

Financial details (*e.g. credit card number, transaction history, credit report*)

Identity information (*e.g. Date of Birth, Government Identifier such as Medicare, Centrelink Reference, passport, or driver license number*)

Contact information (*e.g. home address, phone number, email address*)

Health information (*see s. 6FA of the Privacy Act 1988 (Cth)*)

Consumer Data Right (CDR) Information (*e.g. information about banking customers sent/received via the CDR regime*)

Other sensitive information (*e.g. sexual orientation, political or religious views*)

Recommended steps

You must complete this section

Steps your organisation/agency recommends that individuals take to reduce the risk that they experience serious harm as a result of this data breach *

We have recommended that the affected individual change their passwords to their ImmiAccount and place a 'block' to stop information from being 'imported' to other ImmiAccounts The Privacy Section has engaged with the responsible business area and recommended they provide further support to the affected individual

Other entities affected

Key points

- The NDB scheme recognises that entities often hold personal information jointly. For example, one entity may have physical possession of the information, while another has legal control or

Webform WEB-NDB-24-00098

ownership.

- In these circumstances, an eligible data breach of one entity will also be considered an eligible data breach of other entities that hold the affected information. Both will have obligations under the NDB scheme.
- In general, compliance by one entity will also be taken as compliance by each of the entities that hold the information. As such, only one entity needs to take the steps required by the NDB scheme. The NDB scheme leaves it up to the entities to decide which of them should do so.
- OAIC suggests that, in general, the entity with the most direct relationship with the individuals affected by the data breach should carry out notification.

For further information please refer to the following guidance: [Data breaches involving more than one entity.](#)

This section is optional

If the data breach described above was also a data breach of another organisation/agency, you may provide their identity and contact details to further assist individuals.

Was another organisation / agency affected?

No

Part two - Additional information

Fields with an Asterix () are mandatory and you will need to provide a selection or response.*

The OAIC encourages entities to provide additional information to assist us in understanding the eligible data breach. Part two of the form is optional, but the OAIC may need to contact you to seek further information if you do not complete this part of the form. The OAIC recommends you complete as many questions as possible, but you may leave a field blank if the answer is not known.

The information that you provide on part two of the form does not need to be included in your notification to individuals, and you may request that it be held in confidence by the OAIC.

Your contact details

Title

s.22(1)(a)(ii)

Given name

s.22(1)(a)(ii)

Family name

s.22(1)(a)(ii)

Phone

s.22(1)(a)(ii)

Email

s.22(1)(a)(ii)

Breach details

Date the breach occurred

You may provide your best estimate if the exact date is not known.

Webform WEB-NDB-24-00098

04/Apr/2024

Date the breach was discovered

You may provide your best estimate if the exact date is not known.

24/Jun/2024

Primary cause of data breach

In the selection field below please choose the Primary cause of the data breach where:

Malicious or criminal attack is 'a malicious or criminal attack deliberately crafted to exploit known vulnerabilities for financial or other gain.'

System fault is 'a business or technology process error not caused by direct human error.'

Human error is 'an unintended action by an individual directly resulting in a data breach, for example inadvertent disclosure caused by sending a document containing personal information to the incorrect recipient.'

Primary cause of data breach

Human error

Please provide more details in the selection field below where:

Personal information sent to wrong recipient (email) is 'an unintended action by an individual directly resulting in a data breach, for example inadvertent disclosure caused by sending a document containing personal information to the incorrect recipient.'

Personal information sent to wrong recipient (fax) is where 'personal information is sent to the wrong recipient via facsimile machine, for example, as a result of fax number incorrectly entered or wrong fax number on file.'

Personal information sent to wrong recipient (mail) is where 'personal information is sent to the wrong recipient via postal mail, for example, as a result of transcribing error or wrong address on files.'

Personal information sent to wrong recipient (other) is where 'personal information is sent to the wrong recipient via channels other than email, fax or mail, for example, delivery by hand or uploading to web portal.'

Failure to use BCC when sending email is where 'sending an email to a group by including all recipient emails addresses in the 'To' or 'CC' field, thereby disclosing all recipient email address to all recipients.'

Insecure disposal is 'disposing of personal information in a manner that could lead to its unauthorised disclosure, for example, using a public rubbish bin to dispose of customer records instead of a secure document disposal bin.'

Loss of paperwork or data storage device is 'loss of a physical asset(s) containing personal information, for example, leaving a folder or a laptop on a bus.'

Unauthorised disclosure (failure to redact) is 'failure to effectively remove or de-identify personal information from a record before disclosing it.'

Unauthorised disclosure (verbal) is 'disclosing personal information without authorisation, verbally, for example, calling it out in a waiting room.'

Unauthorised disclosure (unintended release or publication) is 'unauthorised disclosure of personal information in a written format, including paper documents or online.'

Data Breach Details

Unauthorised disclosure (verbal)

Number of individuals whose personal information is involved in the data breach

1

Exact number of individuals whose personal information is involved in the data breach

Please provide your best estimate

1

Number of individuals in **Australia** whose personal information is involved in the data breach

1

Exact number of individuals in **Australia** whose personal information is involved in the data breach

Please provide your best estimate

1

Description of how the data breach occurred

Please provide any additional information about how the eligible data breach occurred that you did not provide above in section 1

s. 47E(d)

s. 47E(d)

s. 47F(1)

s. 47F(1)

s. 47F(1)

Description of any action, including remedial action, you have taken, or you are intending to take, to assist individuals whose personal information was involved in the data breach

s. 47F(1)

Description of any action you have taken, or you are intending to take, to prevent reoccurrence.

Recommendations have been made to provide additional training and support to call centre staff.

Reminder of their obligations under the Privacy Act 1988 Review of identify check, audit and ensuring that individuals are authorised to access certain ImmiAccounts, regardless if they are migration agents.

How do you intend to notify individuals who are likely to be at risk of serious harm as a result of the data breach? When will this occur?

If you do not intend to notify individuals because of an exception under s 26WN or s 26WP, please provide your reasons for relying on the relevant exception.

Further information can be found here:

- [Notifying individuals about an eligible data breach](#)
- [What to include in an eligible data breach statement](#)
- [Exceptions to notification obligations](#)

The affected individual is already aware as they notified the Department. Regardless, a formal letter will be emailed.

List any other data protection authorities, law enforcement bodies or regulatory bodies that you

Webform WEB-NDB-24-00098

have reported this data breach to *

- Australian Cyber Security Centre (ACSC):
- Australian Taxation Office (ATO):
- Australian Prudential Regulation Authority (APRA):
- Australian Securities and Investments Commission (ASIC):
- Other: checked

Please specify *

No other authorities or law enforcement bodies have been contacted

You may wish to separately [report an incident](#) to the Australian Cyber Security Centre if it raises cyber security concerns.

Additional Information

Is there any other information you wish to provide at this stage, or any matters that you wish to draw to the OAIC's attention?

You can provide additional information below, or attach supporting documents when you submit this form.

If you wish to provide further information or documents after you submit the form, you may email them to databreaches@oaic.gov.au.

You may attach other relevant information that supports your notification by using the "**upload file**" button below.

*Files you attach **must**:*

*be in *.pdf, *.docx, *.doc, *.txt, *.jpg, *.gif, or *.png format*

be no more than five files

in total be no larger than 20MB

Inconfidence Request

The OAIC will respect the confidence of commercially or operationally sensitive information provided voluntarily in support of a data breach notification, and will only disclose this information after consulting with you, and with your agreement or where required by law.

I request that the information provided in Part Two of this form is held by the OAIC in confidence:



Australian Government

Office of the Australian Information Commissioner

Our reference: DBN24/00971

Thank you for your statement notifying the Information Commissioner of a data breach.

If you have not done so already, please provide a copy of the notification that you have sent to affected individuals to databreaches@oaic.gov.au. This will assist our staff when assessing your notification.

If we require any further information, we will be in contact. If we receive a complaint from individuals affected by the incident, we will deal with that complaint on its merits.

Further resources

Entities covered by the *Privacy Act 1988* (Cth) 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. APP 6 also limits the circumstances in which an APP entity is permitted to disclose the personal information it holds. Please visit our website for more information on the [APPs](#).

The OAIC's [Guide to securing personal information](#) contains information about reasonable steps APP entities should consider taking to protect the personal information as required by APP 11 of the Privacy Act.

You may also find the OAIC's [Data breach preparation and response: a guide to managing data breaches in accordance with the Privacy Act 1988 \(Cth\)](#) useful in preparing for and responding to future data breaches.

If the breach you have reported is a cyber-security incident, you could also [report it to the Australian Cyber Security Centre](#) (ACSC). The ACSC can provide advice to organisations that have experienced a data breach, and reports to the ACSC help build the Australian Government's understanding of the cyber threat environment.

Yours sincerely

Office of the Australian Information Commissioner

29 July 2024



Australian Government

Department of Home Affairs

29 July 2024

s. 47F(1)

By email: **s. 47F(1)**

Dear **s. 47F(1)**

Thank you for notifying the Department that there has been unauthorised access to your personal information.

The Department takes its obligations under the *Privacy Act 1988* (Privacy Act) seriously. Your complaint was provided to our Privacy Section to review and investigate.

The investigation has found that your personal information was accessed on, or around 4th of April 2024 and included your name, date of birth, residential address, phone number, email and government issued identifiers.

The Department apologises for any distress this incident has caused and wishes to assure you that this incident is taken very seriously.

The Department recommends you change your password to your ImmiAccount and consider placing a block on your current application. If you require assistance with your ImmiAccount or would like to arrange a block on your application, you can contact the Global Feedback Unit on 131 881 within Australia between 9am and 5pm Monday to Friday (excluding Australian National Public holidays). Alternatively, you can email feedback@homeaffairs.gov.au

If you require help with translating and interpretation you can contact The Translating and Interpreting Service within Australia (TIS) 131 450

For crisis and ongoing support please contact:

s. 47F(1)

- 13 11 14 – Lifeline crisis support and suicide prevention.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

We consider this breach meets the requirements for notification to the Office of the Australian Information Commissioner (OAIC) under the Notifiable Data Breach Scheme. This notification to OAIC of this incident did not include your name or contact information.

If you are dissatisfied with the way the Department has managed your privacy complaint you can lodge a complaint directly with the OAIC

- on their website <https://www.oaic.gov.au/privacy/privacy-complaints/>
- email, send it to enquiries@oaic.gov.au
- mail, send it to GPO Box 5218, Sydney NSW 2001
- fax, send it to 02 9284 9666

If you have further concerns about the incident or should you wish to discuss this matter, please do not hesitate to contact me on the details below.

Yours sincerely

Privacy Section

Department of Home Affairs

s.22(1)(a)(ii)

From: s. 47E(d)
 Subject: Notification of Data Breach s. 47F(1)
 Attachments: Form 929.pdf s. 47F(1) otification Data Breach Letter s. 47F(1).docx

From: s.22(1)(a)(ii)
 Sent: M
 To: s. 47F(1)
 Cc: s. 47E(d) @homeaffairs.gov.au>
 Subject: Notification of Data Breach s. 47F(1) SEC=OFFICIAL]

OFFICIAL

Dear s. 47F(1)

Thank you for notifying the Department that there has been unauthorised access to your personal information.

The investigation has found that your personal information was accessed on, or around 4th of April 2024 and included your name, date of birth, residential address, phone number, email and government issued identifiers.

The Department apologises for any distress this incident has caused and wishes to assure you that this incident is taken very seriously.

Please see the attached document for more information in relation to your query. Please also find attached a personal details update form if you wish to update your information with the department.

Thank you

Kind regards

s.22(1)(a)(ii)

Manager | Student Program Delivery SA
 Temporary Visa and Travel Exemptions Branch | Immigration Programs Division
 Immigration and Settlement Services Group | Department of Home Affairs



The Department of Home Affairs and the Australian Border Force acknowledge the Traditional Custodians throughout Australia and their continuing connection to land, sea and the community. We pay respect to all Aboriginal and Torres Strait Islander peoples, their cultures and to their Elders past and present.

OFFICIAL

Released by Department of Home Affairs
 under the Freedom of Information Act 1982

You may go back to previous pages using the buttons below:

Submission

Submission

Please review the information that you have provided about the data breach. If you would like to change anything, you can return to the relevant section by using the navigation buttons at the top of the screen

Once you are ready to submit your form, click the Submit button below.

Once you submit your form, you will be taken to a confirmation page. This page will provide a reference code for your submission, and you will have a copy sent to the email address provided.

Part one - Statement about an eligible data breach

Fields with an Asterix () are mandatory and you will need to provide a selection or response.*

The information that you provide to the OAIC in Part One of this form must also be included in your notification to individuals (if notification is required).

Organisation / agency details

Organisation / agency name *

Department of Home Affairs

Phone *

s.22(1)(a)(ii)

Email *

s. 47E(d) omeaffairs.gov.au

International Address:

Street Address 1 *

5 Chan Street

Street Address 2

City/Suburb *

Belconnen

State *

ACT

Postcode *

2616

Other contact details

s.22(1)(a)(ii)

Description of eligible data breach

An eligible data breach arises when the following three criteria are satisfied:

1. There is unauthorized access to or unauthorized disclosure of personal information, or a loss of personal information, that an entity holds (see [What is a 'Data Breach'?](#))
2. This is likely to result in serious harm to one or more individuals (see [Is Serious Harm Likely?](#)), and
3. The entity has not been able to prevent the likely risk of serious harm with remedial action (see [Preventing Serious Harm with Remedial Action](#))

This document is about the threshold at which an incident is considered an 'eligible data breach' that will be notifiable under the scheme unless an exception applies. [Assessing a Suspected Data Breach](#) provides guidance to entities about the process to follow when carrying out an assessment of 'whether there are reasonable grounds to suspect that there may have been an eligible data breach of the entity' under s 26WH.

Step 1: Is there an eligible data breach?

See s. 26WE(2) Privacy Act 1988 (Cth)

Step 2: Is serious harm likely?

From the perspective of a reasonable person, would the data breach be likely to result in serious harm to an individual whose personal information was part of the data breach?

'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

Further information on these two steps can be found here: [identifying eligible data breaches](#)

Please provide a description of the eligible data breach addressing the above steps in your response *

Based on information provided to the Department by a Visa client, the Department initiated an 'interrogation' of the visa clients ImmiAccount. The interrogation uncovered that there may have been unauthorised access to the clients ImmiAccount by two registered Migration Agents. There is no record indicating that either migration agent was authorised to access the ImmiAccount. One of these migration agents is acting for the s. 47F(1). The migration agents imported personal information belonging to the affected individual into their accounts s. 47F(d)

s. 47E(d)

s. 47E(d)

s. 47F(1)

s. 47F(1)

s. 47F(1)

s. 47E(d)

s. 47E(d)

Information involved in the data breach

Webform WEB-NDB-24-00136

The specific circumstances of the data breach are relevant when assessing whether there is a risk of serious harm to an individual. This may include consideration of the kinds of personal information involved in the data breach and the sensitivity of that information.

Further information can be found here:

[What is personal and sensitive information?](#)

[What is health information?](#)

You must complete this section.

Kind or kinds of personal information involved in the data breach *

Name DOB Contact information (Email, home address, phone number) Government issued identifiers
In addition, please select any categories that apply

- Financial details:
- Tax File Numbers:
- Identity information: checked
- Contact information:
- Consumer Data Right data:
- Health information:
- Other sensitive information:

Option Description

Financial details (*e.g. credit card number, transaction history, credit report*)

Identity information (*e.g. Date of Birth, Government Identifier such as Medicare, Centrelink Reference, passport, or driver license number*)

Contact information (*e.g. home address, phone number, email address*)

Health information (*see s. 6FA of the Privacy Act 1988 (Cth)*)

Consumer Data Right (CDR) Information (*e.g. information about banking customers sent/received via the CDR regime*)

Other sensitive information (*e.g. sexual orientation, political or religious views*)

Recommended steps

You must complete this section

Steps your organisation/agency recommends that individuals take to reduce the risk that they experience serious harm as a result of this data breach *

• Change passwords to their ImmiAccount • If the two migration agents are authorised to access the ImmiAccount, this authorisation must be provided via Form 956A

Other entities affected

Key points

- The NDB scheme recognises that entities often hold personal information jointly. For example, one

Webform WEB-NDB-24-00136

entity may have physical possession of the information, while another has legal control or ownership.

- In these circumstances, an eligible data breach of one entity will also be considered an eligible data breach of other entities that hold the affected information. Both will have obligations under the NDB scheme.
- In general, compliance by one entity will also be taken as compliance by each of the entities that hold the information. As such, only one entity needs to take the steps required by the NDB scheme. The NDB scheme leaves it up to the entities to decide which of them should do so.
- OAIC suggests that, in general, the entity with the most direct relationship with the individuals affected by the data breach should carry out notification.

For further information please refer to the following guidance: [Data breaches involving more than one entity.](#)

This section is optional

If the data breach described above was also a data breach of another organisation/agency, you may provide their identity and contact details to further assist individuals.

Was another organisation / agency affected?

No

Part two - Additional information

Fields with an Asterix () are mandatory and you will need to provide a selection or response.*

The OAIC encourages entities to provide additional information to assist us in understanding the eligible data breach. Part two of the form is optional, but the OAIC may need to contact you to seek further information if you do not complete this part of the form. The OAIC recommends you complete as many questions as possible, but you may leave a field blank if the answer is not known.

The information that you provide on part two of the form does not need to be included in your notification to individuals, and you may request that it be held in confidence by the OAIC.

Your contact details

Title

s.22(1)(a)(ii)

Given name

s.22(1)(a)(ii)

Family name

s.22(1)(a)(ii)

s.22(1)(a)(ii)

Email

s.22(1)(a)(ii)

Breach details

Date the breach occurred

Webform WEB-NDB-24-00136

You may provide your best estimate if the exact date is not known.

08/May/2024

Date the breach was discovered

You may provide your best estimate if the exact date is not known.

11/Jul/2024

Primary cause of data breach

In the selection field below please choose the Primary cause of the data breach where:

Malicious or criminal attack is 'a malicious or criminal attack deliberately crafted to exploit known vulnerabilities for financial or other gain.'

System fault is 'a business or technology process error not caused by direct human error.'

Human error is 'an unintended action by an individual directly resulting in a data breach, for example inadvertent disclosure caused by sending a document containing personal information to the incorrect recipient.'

Primary cause of data breach

System fault

Please provide more detail in by selecting one of the following:

Data Breach Details

Unintended access

Number of individuals whose personal information is involved in the data breach

1

Exact number of individuals whose personal information is involved in the data breach

Please provide your best estimate

1

Number of individuals in **Australia** whose personal information is involved in the data breach

1

Exact number of individuals in **Australia** whose personal information is involved in the data breach

Please provide your best estimate

1

Description of how the data breach occurred

Please provide any additional information about how the eligible data breach occurred that you did not provide above in section 1

S. 47F(1)

s. 47F(1)

s. 47E(d)

s. 47E(d)

Multiple attempts have been made to contact the affected individual to confirm whether they had authorised either migration agent to access their ImmiAccount. These attempts have been unsuccessful in reaching the affected individual.

Description of any action, including remedial action, you have taken, or you are intending to take, to assist individuals whose personal information was involved in the data breach

s. 47F(1)

s. 47F(1)

s. 47E(d)

s. 47E(d)

• A block has been placed on the affected

individuals ImmiAccount to prevent further unauthorised access. • Recommended that client of interest (COI) notes are placed on both the affected individual and s. 47F(1) account in the event that either contact GSU, the individual who takes the call, will be fully informed s. 47F(1)

s. 47F(1) and to take extra care when dealing with the information held by the Department. • s. 47F(1)

s. 47F(1)

s. 47F(1)

s. 47F(1) section have attempted to contact the affected individual to verify and confirm that they authorised the two migration agents to access their account – no response to date. • All attempts by the Department to contact the affected individual have been unsuccessful.

Description of any action you have taken, or you are intending to take, to prevent reoccurrence.

s. 47E(d)

How do you intend to notify individuals who are likely to be at risk of serious harm as a result of the data breach? When will this occur?

If you do not intend to notify individuals because of an exception under s 26WN or s 26WP, please provide your reasons for relying on the relevant exception.

Further information can be found here:

- [Notifying individuals about an eligible data breach](#)
- [What to include in an eligible data breach statement](#)
- [Exceptions to notification obligations](#)

List any other data protection authorities, law enforcement bodies or regulatory bodies that you have reported this data breach to *

- Australian Cyber Security Centre (ACSC):
- Australian Taxation Office (ATO):
- Australian Prudential Regulation Authority (APRA):
- Australian Securities and Investments Commission (ASIC):
- Other: checked

Please specify *

No other data protection authorities have been notified of this breach as its not applicable.

You may wish to separately [report an incident](#) to the Australian Cyber Security Centre if it raises cyber security concerns.

Additional Information

Is there any other information you wish to provide at this stage, or any matters that you wish to draw to the

Webform WEB-NDB-24-00136

OAIC's attention?

You can provide additional information below, or attach supporting documents when you submit this form.

If you wish to provide further information or documents after you submit the form, you may email them to databreaches@oaic.gov.au.

You may attach other relevant information that supports your notification by using the "**upload file**" button below.

*Files you attach **must**:*

*be in *.pdf, *.docx, *.doc, *.txt, *.jpg, *.gif, or *.png format*

be no more than five files

in total be no larger than 20MB

Inconfidence Request

The OAIC will respect the confidence of commercially or operationally sensitive information provided voluntarily in support of a data breach notification, and will only disclose this information after consulting with you, and with your agreement or where required by law.

I request that the information provided in Part Two of this form is held by the OAIC in confidence:



Australian Government

Office of the Australian Information Commissioner

Our reference: DBN24/01010

Thank you for your statement notifying the Information Commissioner of a data breach.

If you have not done so already, please provide a copy of the notification that you have sent to affected individuals to databreaches@oaic.gov.au. This will assist our staff when assessing your notification.

If we require any further information, we will be in contact. If we receive a complaint from individuals affected by the incident, we will deal with that complaint on its merits.

Further resources

Entities covered by the *Privacy Act 1988* (Cth) 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. APP 6 also limits the circumstances in which an APP entity is permitted to disclose the personal information it holds. Please visit our website for more information on the [APPs](#).

The OAIC's [Guide to securing personal information](#) contains information about reasonable steps APP entities should consider taking to protect the personal information as required by APP 11 of the Privacy Act.

You may also find the OAIC's [Data breach preparation and response: a guide to managing data breaches in accordance with the Privacy Act 1988 \(Cth\)](#) useful in preparing for and responding to future data breaches.

If the breach you have reported is a cyber-security incident, you could also [report it to the Australian Cyber Security Centre](#) (ACSC). The ACSC can provide advice to organisations that have experienced a data breach, and reports to the ACSC help build the Australian Government's understanding of the cyber threat environment.

Yours sincerely

Office of the Australian Information Commissioner

5 August 2024

s.22(1)(a)(ii)

From:
Subject:

s. 47E(d) Home Affairs)
RE: Contact from the Department of Home Affairs

S. 47F(1)

On Tue, 13 Aug, 2024, 4:06 pm Immigration Connec s.22(1)(a)(ii) wrote:

OFFICIAL

Hello s. 47F(1)

My name is s.22(1)(a)(ii) and I am from the Department of Home Affairs.

s. 47F(1)

It is important that we speak with you as we also need to provide you with some important information.

Is there a preferred day and time that we may call you? Can you please also confirm the most appropriate mobile number to reach you.

If you wish to verify this information first, please call the Department on 131 881 as a note has been placed on your file documenting our attempts to contact you.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

I hope to hear from you soon.

Kind regards,

s.22(1)(a)(ii)

Assistant Manager | Student Program Delivery, SA
Temporary Visa Program Branch | Immigration Programs Division
Immigration and Settlement Services Group | Department of Home Affairs

P: s.22(1)(a)(ii) | E: s.22(1)(a)(ii)

OFFICIAL

Important Notice: The content of this email is intended only for use by the individual or entity to whom it is addressed. If you have received this email by mistake, please advise the sender and delete the message and attachments immediately. This email, including attachments, may contain confidential, sensitive, legally privileged and/or copyright information.

Any review, retransmission, dissemination or other use of this information by persons or entities other than the intended recipient is prohibited. The Department of Home Affairs, the ABF and the National Emergency Management Agency respect your privacy and have obligations under the Privacy Act 1988.

Unsolicited commercial emails MUST NOT be sent to the originator of this email.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

s.22(1)(a)(ii)

Subject:

RE: New contact details

s. 47F(1)

Sent: Wednesday, 14 August 2024 3:17 PM

To: s. 47E(d)

s.22(1)(a)(ii)

Subject: RE: New contact details

s.22(1)(a)(ii)

OFFICIAL

Hi s.22(1)(a)(ii)

Thank you for your email.

Just confirming that I have spoken with the PA today. It appeared as though they didn't completely understand the letter and therefore had not responded or understood they were required to respond.

The PA now understands we will be contacting the s. 47F(1). I referred them to the s. 47F(1) services information provided in the letter.

The PA also confirmed the authorised recipient is s. 47F(1) recorded in ICSE), however they could not confirm the MARN.

Can you please confirm what our next steps should be from here? Can we now send a NJ letter to the DA?

Thank you for your assistance.

Kind regards,

s.22(1)(a)(ii)

Assistant Manager | Student Program Delivery, SA
Temporary Visa Program Branch | Immigration Programs Division

Home Affairs

s.22(1)(a)(ii)

OFFICIAL

From: s. 47E(d)

Sent: Tuesday, 13 August 2024 6:22 PM

To: s.22(1)(a)(ii)

s.22(1)(a)(ii)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Cc: s. 47E(d) s.22(1)(a)(ii)
Subject: New contact details - s. 47F(1) SEC=OFFICIAL]

OFFICIAL

Hi s.22(1)(a)(ii)

s. 47F(1) has responded to the Connect email (attached) and provided a new mobile number and time to call them on Wednesday.

With Regards

s.22(1)(a)(ii)

A/g Assistant Manager s. 47E(d)
Family Visas Branch | Immigration Programs Division
Immigration Group
Department of Home Affairs
E: s.22(1)(a)(ii)



The Department of Home Affairs and the Australian Border Force acknowledge the Traditional Custodians throughout Australia and their continuing connection to land, sea and the community. We pay respect to all Aboriginal and Torres Strait Islander peoples, their cultures and to their Elders past and present.

OFFICIAL

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*



22 August 2024

s. 47F(1)

By email: s. 47F(1)

Dear s. 47F(1)

I write to inform you that the Department has been made aware, through an internal audit of your ImmiAccount that there may have been unauthorised access to your personal information.

The Department takes its obligations under the *Privacy Act 1988* (Privacy Act) seriously. The audit was escalated to our Privacy Section to review and investigate.

The investigation has found that your personal information has been accessed by two migration agents which departmental records indicate are unauthorised. The personal information accessed included your name, date of birth, residential address, phone number, email and government issued identifiers.

The Department has placed a block on your ImmiAccount to prevent unauthorised access. We recommend you change your password to your ImmiAccount. If you require assistance with your ImmiAccount, you can contact the Global Feedback Unit on 131 881 within Australia between 9am and 5pm Monday to Friday (excluding Australian National Public holidays). Alternatively, you can email feedback@homeaffairs.gov.au

If you require help with translating and interpretation you can contact The Translating and Interpreting Service within Australia (TIS) 131 450

For crisis and ongoing support please contact:

s. 47E(d)

- 13 11 14 – Lifeline crisis support and suicide prevention.

We consider this breach meets the requirements for notification to the Office of the Australian Information Commissioner (OAIC) under the Notifiable Data Breach Scheme. This notification to OAIC of this incident did not include your name or contact information.

If you are dissatisfied with the way the Department has managed your privacy complaint you can lodge a complaint directly with the OAIC

- on their website <https://www.oaic.gov.au/privacy/privacy-complaints/>
- email, send it to enquiries@oaic.gov.au
- mail, send it to GPO Box 5218, Sydney NSW 2001
- fax, send it to 02 9284 9666

Released by Department of Home Affairs
under the Freedom of Information Act 1982

If you have further concerns about the incident or should you wish to discuss this matter, please do not hesitate to contact me on the details below.

Yours sincerely

Privacy Section

Department of Home Affairs

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*