ACT Government
Chief Minister, Treasury and Economic Development

Freedom of Information Disclosure Log Publication Coversheet

The following information is provided pursuant to section 28 of the *Freedom of Information Act 2016*.

Application Details	
Ref. No.	CMTEDDFOI 2023-412
Date of Application	1 December 2023
Date of Decision	22 January 2024
Processing time (in working days)	30
Fees	N/A
Decision on Access	Full Release
Information Requested (summary)	What procedures and processes are in place in the instance where a license number or card number has been compromised and could potentially be used in fraud?

Publication Details		
Original application	☑ Published	☐ N/A
Decision notice	☑ Published	☐ N/A
Documents and schedule	☑ Published	☐ N/A
Decision made by Ombudsman	N/A	
Additional information identified by Ombudsman	N/A	
Decision made by ACAT	N/A	
Additional information identified by ACAT	N/A	

From: [redacted]
To: CMTEDD FOI
Subject: Re: Freedom of Information request-CMTEDDFOI 2023-412
Date: Monday, 11 December 2023 4:00:50 PM

Thanks for your time on the phone on Friday.

Thank you for the notes below, my updates included:

What procedures and processes are in place in the instance where a licence number or card number has been compromised and could potentially be used in fraud? And what policy, procedures and associated rationale is applied to events like these, noting the requirements under Territory Privacy Principle 11.1 that an organisation must take reasonable steps to protect information from misuse, interference and loss from unauthorised access, modification or disclosure?

Thanks [redacted]

On Fri, Dec 8, 2023 at 11:07 AM CMTEDD FOI <CMTEDDFOI@act.gov.au> wrote:

OFFICIAL

Good morning [redacted]

Thankyou for your time on the telephone this morning. As per our discussion regarding a rescope of your request, please see below the proposed new scope:

“ What procedures and processes are in place in the instance a licence number or card maybe used in fraud? And What Policy and associated rationale is applied to events like these? “

Could you please reply to this email with your confirmation, if you are happy to proceed with this new scope for your information request.

Please do not hesitate to contact me, should you need to discuss further.

Kind regards

Freedom of Information Coordinator | Information Access Team

Phone: 02 6207 7754 | Email: CMTEDDFOI@act.gov.au

Corporate | Chief Minister, Treasury and Economic Development Directorate | ACT Government

Level 1, 220 London Circuit, Canberra ACT 2601 | GPO Box 158 Canberra ACT 2601 | act.gov.au

---

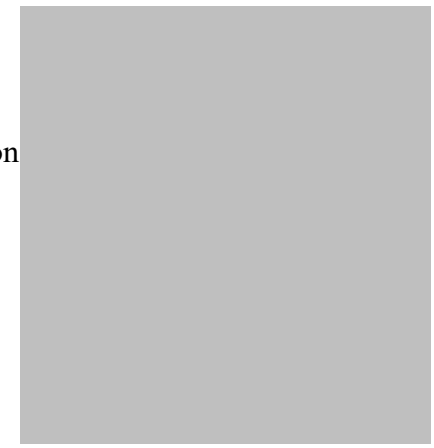
From: no-reply@act.gov.au <no-reply@act.gov.au>
Sent: Friday, December 1, 2023 5:06 PM
To: CMTEDD FOI <CMTEDDFOI@act.gov.au>
Subject: Freedom of Information request-CMTEDDFOI 2023-412

Please find online enquiry details below. Please ensure this enquiry is responded to within fourteen working days.

Your details

All fields are optional, however an email address OR full postal address must be provided for us to process your request. An email address and telephone contact number will assist us to contact you quickly if we need to discuss your request.

Title:
First Name:
Last Name:
Business/Organisation
Address:
Suburb:
Postcode:
State/Territory:
Phone/mobile:
Email address:



Request for information

(Please provide as much detail as possible, for example subject matter and relevant dates, and also provide details of documents that you are not interested in.)

- procedure / process / etc to issue someone with a new driver's licence number (not a new card number, but a driver's licence number) - resources needed to issue someone with a new

Under the Freedom of Information Act 2016 I want to access the following document/s (*required field):	driver's licence number (not a new card number, but a driver's licence number) - reasoning / policy / emails / internal notes / etc as to why those people whose driver's licence numbers were only compromised in the 2022 Optus cyber security breach were not permitted to be given a new driver's licence number, whereas those people who had both their driver's licence and card numbers compromised were issued with a new driver's licence number (as well as a new card number)
I do not want to access the following documents in relation to my request::	

Thank you.
Freedom of Information Coordinator

ACT Government
Chief Minister, Treasury and Economic Development

Our ref: CMTEDDFOI 2023-412

[redacted]

FREEDOM OF INFORMATION REQUEST – NOTICE OF DECISION

I refer to your application under section 30 of the *Freedom of Information Act 2016* (the Act), received by the Chief Minister, Treasury and Economic Development Directorate (CMTEDD) on 1 December 2023.Specifically, you sought:

"procedure / process / etc to issue someone with a new driver's licence number (not a new card number, but a driver's licence number) - resources needed to issue someone with a new driver's licence number (not a new card number, but a driver's licence number) - reasoning / policy / emails / internal notes / etc as to why those people whose driver's licence numbers were only compromised in the 2022 Optus cyber security breach were not permitted to be given a new driver's licence number, whereas those people who had both their driver's licence and card numbers compromised were issued with a new driver's licence number (as well as a new card number)"

On **8 December 2023** a Freedom of Information Coordinator contacted you regarding a rescope.

On **11 December 2023** you agreed to a new scope:

"What procedures and processes are in place in the instance where a licence number or card number has been compromised and could potentially be used in fraud? And what policy, procedures and associated rationale is applied to events like these, noting the requirements under Territory Privacy Principle 11.1 that an organisation must take reasonable steps to protect information from misuse, interference and loss from unauthorised access, modification or disclosure?"

Authority

I am an Information Officer appointed by the CMTEDD Director-General under section 18 of the Act to deal with access applications made under Part 5 of the Act.

Timeframes

In accordance with section 40 of the Act, CMTEDD was required to provide a decision on your access application by **24 January 2024.**

Decision on access

Searches were completed for relevant documents and two documents were identified that fall within the scope of your request.

I have included as **Attachment A** to this decision the schedule of relevant documents. This provides a description of the documents that fall within the scope of your request and the access decision for those documents. I have decided to grant access in full to these documents.
My access decisions are detailed further in the following statement of reasons and the documents released to you are provided as **Attachment B** to this letter.

In accordance with section 54(2) of the Act a statement of reasons outlining my decisions is below.

Statement of Reasons

In reaching my access decisions, I have taken the following into account:

- the Act
- the content of the documents that fall within the scope of your request
- the *Human Rights Act 2004*.

Exemption claimed

My reasons for deciding to grant access to the identified documents are as follows:

Public Interest

The Act has a presumption in favour of disclosure. As a decision maker I am required to decide where, on balance, public interests lies. As part of this process I must consider factors favouring disclosure and non-disclosure.

In *Hogan v Hinch* (2011) 243 CLR 506, [31] French CJ stated that when 'used in a statute, the term [public interest] derives its content from "the subject matter and the scope and purpose" of the enactment in which it appears'. Section 17(1) of the Act sets out the test, to be applied to determine whether disclosure of information would be contrary to the public interest. These factors are found in subsection 17(2) and Schedule 2 of the Act.

Taking into consideration the information contained in the documents found to be within the scope of your request, I have identified that the following public interest factors are relevant to determine if release of the information contained within the documents is within the 'public interest'.

Factors **favouring disclosure** in the public interest:

(a) disclosure of the information could reasonably be expected to do any of the following:

> *(ii) contribute to positive and informed debate on important issues or matters of public interest.*
>
> *(iii) inform the community of the government's operations, including the policies, guidelines and codes of conduct followed by the government in its dealings with members of the community.*

I have placed substantial weight on the above factors favouring disclosure. The release of this information can reasonably be expected to provide information that will inform the community and increase their understanding of government operations.

I did not identify any factor favouring nonrelease and have decided to release this information to you in full.

Charges

Processing charges are not applicable for this request because the number of pages released to you is below the charging threshold of 50.

Online publishing – Disclosure Log

Under section 28 of the Act, CMTEDD maintains an online record of access applications called a disclosure log.

Your original access application and my decision will be published on the CMTEDD disclosure log. Your personal contact details will not be published.

Ombudsman Review

My decision on your access request is a reviewable decision as identified in Schedule 3 of the Act. You have the right to seek Ombudsman review of this outcome under section 73 of the Act within 20 working days from the day that my decision is provided to you, or a longer period allowed by the Ombudsman.

We recommend using this form *Applying for an Ombudsman Review* to ensure you provide all of the required information. Alternatively, you may write to the Ombudsman at:

The ACT Ombudsman
GPO Box 442
CANBERRA ACT 2601

Via email: actfoi@ombudsman.gov.au

ACT Civil and Administrative Tribunal (ACAT) Review

Under section 84 of the Act, if a decision is made under section 82(1) on an Ombudsman review, you may apply to the ACAT for review of the Ombudsman decision. Further information may be obtained from the ACAT at:

ACT Civil and Administrative Tribunal
GPO Box 370
Canberra City ACT 2601
Telephone: (02) 6207 1740
http://www.acat.act.gov.au/

Should you have any queries in relation to your request please contact the Information Access Team by telephone on 6207 7754 or email CMTEDDFOI@act.gov.au.

Yours sincerely,

EH

Emma Hotham
Information Officer
Chief Minister, Treasury and Economic Development Directorate

22 January 2024

ACT Government
Chief Minister, Treasury and Economic Development

FREEDOM OF INFORMATION REQUEST SCHEDULE

WHAT ARE THE PARAMETERS OF THE REQUEST	Reference NO.
"What procedures and processes are in place in the instance where a licence number or card number has been compromised and could potentially be used in fraud? And what policy, procedures and associated rationale is applied to events like these, noting the requirements under Territory Privacy Principle 11.1 that an organisation must take reasonable steps to protect information from misuse, interference and loss from unauthorised access, modification or disclosure?"	**CMTEDDFOI 2023-412**

Ref No	Page number	Description	Date	Status	Reason for Exemption	Online Release Status
1	**1-2**	**Staff instruction -1046 Optus Data Breach**	**7 October 2022**	**Full Release**		**Yes**
2	**3**	**Area response to scope of FOI request CMTEDDFOI 2023-412**	**Undated**	**Full Release**		**Yes**

Total No of Docs
2

ACT Government
Chief Minister, Treasury and Economic Development

Staff Instruction Number 1046

Staff Instruction Type	**New procedure**

Subject	**Optus data breach, September 2022.**

Purpose	To inform staff of the process to replace a driver licence or proof of identity card due to the Optus breach.

Target Audience	**Requires Action**	**Information Only**
Access Canberra Contact Centre	☐	☑
Access Canberra Service Centre	☑	☐
All Transport Licensing Staff	☐	☑
Transport Solutions Staff	☐	☑
Jervis Bay Territory Staff	☐	☑

Background	An Optus data breach occurred on 22 September 2022, resulting in some compromised driver licence and proof of identity card numbers.

Please see the scenarios below regarding obtaining a replacement data card for clients affected by the Optus data breach.

ACT Driver Licence

The client provides evidence of the Optus breach to the CSO, detailing that both the licence number and card number were compromised and recommending they get a replacement licence card (in the form of an email/letter).

1. The client attends a Service Centre about the Optus breach and requests a replacement driver licence.
2. The CSO replaces the card with the reason 'Stolen', and the client pays the fee.
3. The client must have a new photo taken.
4. The client provides evidence of the Optus breach to the CSO, detailing that both the licence number and card number were compromised and recommending they get a replacement licence card (in the form of an email/letter).
5. The CSO lodges the request in the Immediate Print data card register and identifies that the request is due to the Optus Breach for the print to be prioritised and posted via registered mail.

Contact: **Business Support and Training**
6207 7020
Rego.act.HELP@act.gov.au
Date Issued: **07/10/2022**

The client did <u>not</u> have both the licence number and card number compromised.

1. The client attends a Service Centre about the Optus breach and requests a replacement driver licence.
2. The CSO replaces the licence card with the reason 'Stolen', and the client pays the fee.
3. The client must have a new photo taken.
4. The client doesn't provide evidence of the Optus breach, resulting in the replacement card being printed and posted per the usual process.

<u>ACT Proof of Identity (POI) Card</u>

The client was advised that their POI details have been compromised.

1. The client attends a Service Centre about the Optus breach and requests a replacement POI Card.
2. The CSO replaces the POI with the reason 'Stolen' and the client pays the fee.
3. The client must have a new photo taken.
4. The POI Card is printed and posted per the usual process.

Impact Statement	1. When replacing a driver licence or POI due to the Optus data breach, CSOs are to select the reason 'Stolen', and the client is to pay the fee. 2. Clients who provide evidence their driver licence number and card number were compromised are entitled to have the card priority printed and sent through registered post. All other requests are printed and posted through the normal process.

Attachments /Links	Replacement licence policy Replacement POI procedure Staff Instruction Index

Effective	**07/10/2022**

The issue of a driver licence is performed under Road Transport legislation with the corresponding function of enabling a person to prove their right to drive as well as detailing the types of vehicles and/or other relevant conditions central to that activity. A driver licence contains personal information (as specified by the Road Transport legislation) and Access Canberra has numerous controls in place to ensure the information is held appropriately with regard to Road Transport and Privacy Legislation.

Access Canberra acknowledges that a holder of a driver licence often use it for a secondary purpose, such as to support identification. To that end, the physical artefact contains a number of security features to prevent its fraudulent replication. Furthermore, as an additional protection to prevent its misuse, an ACT driver licence is one of the documents that is able to verified through Commonwealths Document Verification Service (DVS).

The DVS is the secure online platform (overseen by the Attorney General's Department) that provides for the electronic verification of various Government issued documents commonly furnished in support of proving identity. With respect to an ACT driver licence, where both a card number and driver licence number has been compromised, the reissue/printing of a driver licence alters the card number and combination of data points relied on by the DVS for its verification. Put simply, the protection from misuse achieved through the DVS is enabled through the changed card number without the need to alter the driver licence number.

With respect to queries raised concerning 'Territory Privacy Principle (TPP) 11 - Security of Personal Information, particularly the need to take reasonable steps to protect information from misuse, interference or loss and from unauthorised access modification or disclosure . I am able to assure you that within the scope of TPP 11 Access Canberra has robust controls in protect the personal information held from misuse, interference or loss as well from unauthorised access modification or disclosure. The recent incidents that have resulted in the compromise of personal information contained on a driver licence has not occurred due to a failure of Access Canberra's policies or procedures. Regardless, the measures expressed above aid to prevention the misuse of the information by others.