



ACT
Government

Chief Minister, Treasury and
Economic Development

Freedom of Information Publication Coversheet

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

FOI Reference: CMTEDDFOI 2018-00237

Information to be published	Status
1. Access application	Published
2. Decision notice	Published
3. Documents and schedule	Published
4. Additional information identified	No
5. Fees	Waived
6. Processing time (in working days)	30
7. Decision made by Ombudsman	N/A
8. Additional information identified by Ombudsman	N/A
9. Decision made by ACAT	N/A
10. Additional information identified by ACAT	N/A

From: [REDACTED]
To: [CMTEDD FOI](#)
Subject: FOI Request: Adverse findings
Date: Friday, 7 September 2018 10:40:41 AM

Hello,

I'm writing to request information under the *Freedom of Information Act 2016*.

I am seeking:

- all documentation, including internal briefings, reports, correspondence and other documentation generated or discovered in the investigation and eventual termination of an employee in 2016-17 related to the misuse of timesheets.
- all documentation, including internal briefings, reports, correspondence and other documentation generated or discovered in the investigation and eventual transfer of an employee in 2017-18 related to the misuse of timesheets.
- all documentation, including internal briefings, reports, correspondence and other documentation generated or discovered in the investigation and eventual warning and admonishment of an employee in 2017-18 related to fraud.
- all documentation, including internal briefings, reports, correspondence and other documentation generated or discovered in the investigation and eventual pay reduction of an employee in 2017-18 related to unauthorised disclosure of confidential information.

I do not request duplicates of documents, including duplicate emails. I do not specifically request personally identifying material exempted under the Act, such as names, phone numbers and email addresses and am happy for this information to be redacted.

I would like advice if the information I have sought is due to be released under FOI to individuals or organisations prior to finalisation of my FOI application.

I also note the onus rests with the agency to prove why any information should not be released under the Act and I request the agency provide evidence in support of any assumptions or assertions used to justify non-disclosure.

I also advise I am seeking a total reduction in fees and charges associated with this request as release of the information will: contribute to community understanding on an important issue, inform debate and improve government accountability and transparency.

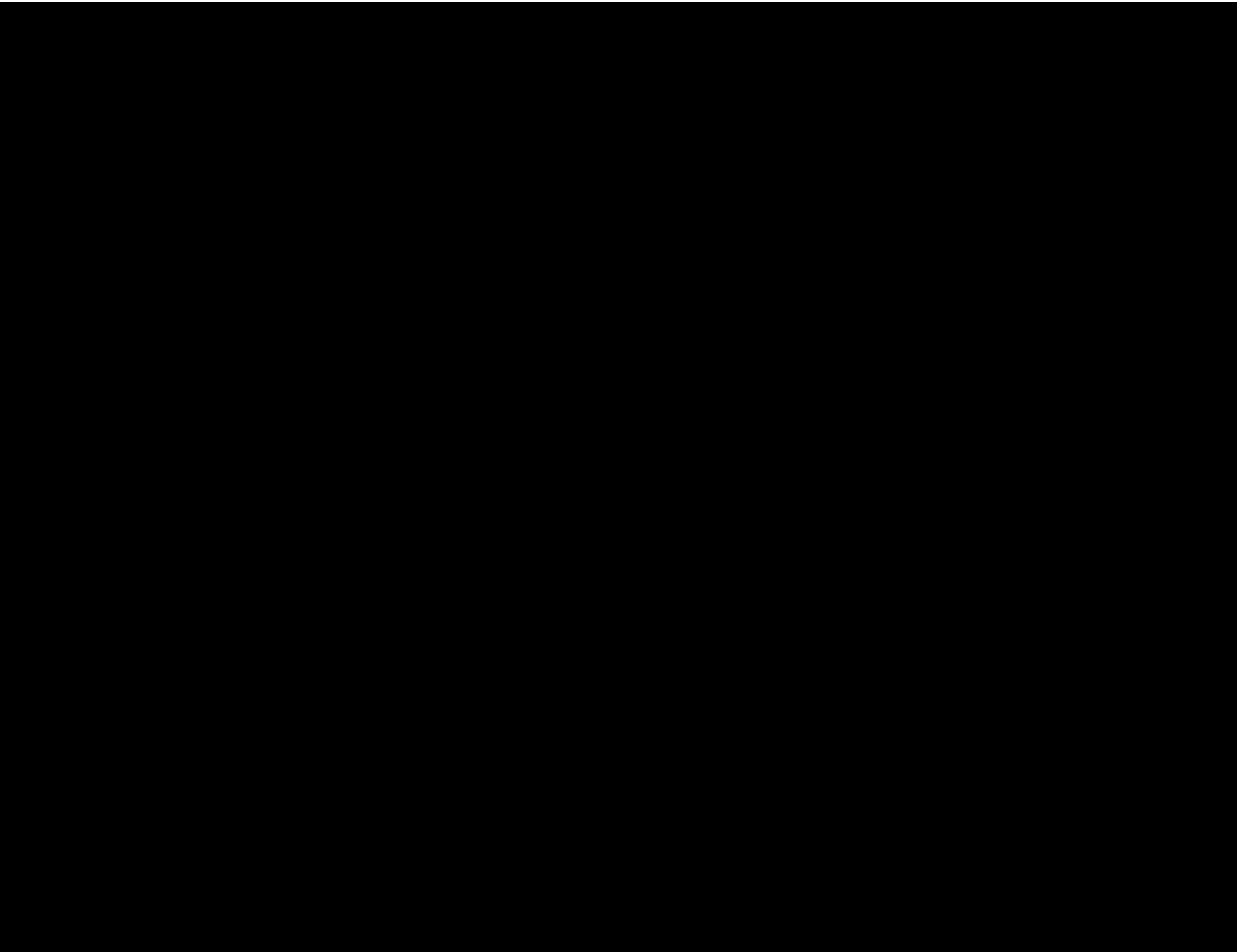
[REDACTED]

[REDACTED]

If I can assist with the processing of my request, including negotiation of scope, please do not hesitate to contact me by phone or email on the details below.

Best regards,

[REDACTED]



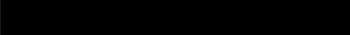


ACT
Government

Chief Minister, Treasury and
Economic Development

Our ref: CMTEDDFOI 2018-0237



via email: 

Dear 

FREEDOM OF INFORMATION REQUEST

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 7 September 2018, in which you sought access to:

1. *All documentation, including internal briefings, reports, correspondence and other documentation generated or discovered in the investigation and eventual termination of an employee in 2016-17 related to the misuse of timesheets.*
2. *All documentation, including internal briefings, reports, correspondence and other documentation generated or discovered in the investigation and eventual transfer of an employee in 2017-18 related to the misuse of timesheets.*
3. *All documentation, including internal briefings, reports, correspondence and other documentation generated or discovered in the investigation and eventual warning and admonishment of an employee in 2017-18 related to fraud.*
4. *All documentation, including internal briefings, reports, correspondence and other documentation generated or discovered in the investigation and eventual pay reduction of an employee in 2017-18 related to unauthorised disclosure of confidential information.*

On 7 September 2018 you were provided a link to an earlier decision that covered point 4 listed above therefore point 4 has not been considered in this decision.

On 18 October 2018 you refined the scope of your request to *"the documents created by the Professional Standards Unit in the course of the investigations that were subject to the Questions on Notice Paper 19"*.

On 19 October 2018 you also confirmed you do not require access to any of the attachments to the Professional Standards Unit reports.

Authority

I am an Information Officer appointed by the Director-General of CMTEDD 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 is required to provide a decision on your access application by 29 October 2018.

Third Party Consultation

In making this decision, I completed consultation with a relevant third parties in accordance with section 38 of the Act. The views of identified third parties were taken into account in making this decision.

Decision on access

Searches were completed for relevant documents and 3 cases were identified that fall within the scope of your request.

I have decided to grant partial access to those 3 cases. The redacted I consider to be information that would, on balance, be contrary to the public interest to disclose under the test set out in section 17 of the Act or is outside of the scope of your request. Due to specific workplace sensitivities some cases are redacted more heavily than others, however the principles in section 6(e) and section 9 of the Act have been applied.

I have included as Attachment A to this decision the schedule of relevant documents. This provides a description of each document that falls within the scope of your request and the access decision for each of those 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 decision is below.

Statement of Reasons

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

- the Act;
- the content of the documents that fall within the scope of your request;
- your views on the public interest in disclosing the government information;
- the views of the relevant third parties; and
- the *Human Rights Act 2004*.

Exemption claimed

My reasons for deciding not to grant access to the identified documents and components of these 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 these documents is within the 'public interest'.

Factors favouring disclosure (Schedule 2 section 2.1)

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

- (vi) *reveal or substantiate that an agency or public official has engaged in misconduct or negligent, improper or unlawful conduct or has acted maliciously or in bad faith;*

Factors favouring non-disclosure (Schedule 2 section 2.2)

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

- (ii) *prejudice the protection of an individual's right to privacy or any other right under the Human Rights Act 2004;*
- (xii) *prejudice an agency's ability to obtain confidential information;*
- (xv) *prejudice the management function of an agency or the conduct of industrial relations by an agency;*

Having considered the factors identified as relevant in this matter, I consider that release of information contained in these documents may reveal or substantiate that an agency or public official has engaged in misconduct or negligent, improper or unlawful conduct or has acted maliciously or in bad faith. The information contained in the investigation reports was compiled by the Professional Standards Unit (PSU) and takes into the alleged misconduct and the evidence that substantiates these claims. The release of this information allows the public to understand the types of misconduct that have occurred, the processes undertaken by the PSU to investigate each of the allegations and the outcomes of each allegation. The release of this information will demonstrate the work that is undertaken to ensure that members of the ACT Public Service uphold the requirements of the *Public Sector Management Act 1994* during their employment.

However, when considering this finding against the factor favouring non-disclosure, I am satisfied that the protection of an individual's right to privacy, especially in the course of assisting in a misconduct investigation is a significant factor as the parties involved have provided their personal information for the purposes of meeting obligations under relevant legislation or in their duties as an ACT Government employee which, in my opinion, outweighs the benefit which may be derived from releasing the personal information of the individual's involved in this matter.

Personal information is defined by the *Information Privacy Act 2014* as “information or an opinion about an identified individual, or an individual who is reasonably identifiable (i) whether the information or opinion is true or not; and (ii) whether the information or opinion is recorded in a material form or not.” I am satisfied that information which allows for an individual to be identified is personal information. Having reviewed the documents within the scope of the request, I note that details such as staff members’ names, employment levels, personal accounts of events, the dates, times and locations they occurred and their comments and opinions about other staff members, if released could allow for the individuals involved to be identified. I consider that disclosing such information would cause significant intrusion into privacy of these individuals which would impact their rights under the *Human Rights Act 2004*. Given the sensitive nature of the information, I have given significant weight to this factor.

In making this decision, I have also considered the right to privacy for ACT Government Officials named in the investigation and related correspondence. I am satisfied that the names, signatures, and contact information of government employees at the Senior Executive Level should be released as these staff members were acting in their official capacity and the personal information being released is done so in relation to these individuals exercising their delegations in a work related capacity. I do not consider the release of this information is unreasonable or could prejudice their right to privacy. ACT Government employees below this level have been removed where it has been requested this is done.

The release of identified documents also contain information which could prejudice the Directorate’s ability to obtain confidential information. Staff members should be able to freely raise sensitive concerns and seek advice from the Human Resources (HR) teams, particularly in the situation involving improper conduct. Witnesses to events should be able to give advice to the HR teams without any concerns. It is expected by all parties involved that this kind of information is treated in a confidential manner and should only be disclosed on a need-to-know basis. I consider that there is a strong public interest in the HR teams being able to consult with staff members and obtain frank and honest advice to allow them to fully address these matters. The release of information is likely to make staff reluctant to raise similar concerns or give advice in the future. Consequently, the release of this information could prejudice the ability of the HR business areas to receive sensitive concerns and address the issues effectively. For these reasons, I have attributed quite significant weight to both factors.

Having applied the test outlined in section 17 of the Act and deciding that release of personal information contained in the documents is not in the public interest to release, I have chosen to redact this specific information in accordance with section 50(2). Noting the pro-disclosure intent of the Act, I am satisfied that redacting only the information that I believe is not in the public interest to release will ensure the intent of the Act is met and will provide you with access to the majority of the information held by CMTEDD within the scope of your request.

Charges

Pursuant to *Freedom of Information (Fees) Determination 2017 (No 2)* processing charges would normally be applicable for this request because the total number folio's to be released to you is above the charging threshold of 50 pages however, in this instance, I have chosen to waive fees associated with your access application in accordance with section 107(2)(b) of the Act.

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, my decision and documents released to you in response to your access application will be published in the CMTEDD disclosure log after 25 October 2018. Your personal contact details will not be published.

You may view CMTEDD disclosure log at:

<https://www.cmtedd.act.gov.au/functions/foi/disclosure-log>.

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 published in CMTEDD disclosure log, or a longer period allowed by the Ombudsman.

If you wish to request a review of my decision 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
Level 4, 1 Moore St
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 me by telephone on 6207 7754 or email CMTEDDFOI@act.gov.au

Yours sincerely,

A handwritten signature in black ink, appearing to read 'Daniel Riley', with a stylized, cursive script.

Daniel Riley
Information Officer
Information Access Team
Chief Minister, Treasury and Economic Development Directorate

22 October 2018



ACT
Government

Chief Minister, Treasury and
Economic Development

FREEDOM OF INFORMATION REQUEST SCHEDULE

NAME		Reference NO.
[REDACTED]		CMTEDDFOI2018-0237

Ref No	Page number	Description	Date	Status	Reason for Exemption	Online Release Status
Matter 1	1-44	Matter 1	2016-2017	Withheld	N/A	N/A
Matter 2	45-52	Matter 2	2017-2018	Withheld	N/A	N/A
Matter 3	53-64	Matter 3	2017-2018	Partial Release	Sch 2 s2.2 (a)(ii)	Yes
Total No of Docs						
3						



ACT
Government

Chief Minister, Treasury and
Economic Development

Investigation Report

Sch 2.2(a)(ii)

CMTEDD

Case Reference: 2017/44

Prepared by:

Sch 2.2(a)(ii)

Senior Investigator
Professional Standards Unit

18 October 2017



ACT
Government

Chief Minister, Treasury and
Economic Development

Sch 2.2(a)(ii)

Sch 2.2(a)(ii)

Dear **Sch 2.2(a)(ii)**

Investigation Report regarding allegations of possible misconduct by **Sch 2.2(a)(ii)**

Background

Sch 2.2(a)(ii) conducted a preliminary investigation into a complaint received by **Sch 2.2(a)(ii)** a member of the public, and subsequently recommended an investigation into allegations of misconduct resulting from the complaint (Attachment 1).

On 7 July 2017 **Sch 2.2(a)(ii)** was notified in writing by **Sch 2.2(a)(ii)** of the investigation (Attachment 2). The preliminary allegations identified and notified to **Sch 2.2(a)(ii)** were:

1. That **Sch 2.2(a)(ii)** may have knowingly used credit card details provided by a member of the public for her own personal use.
2. That **Sch 2.2(a)(ii)** did not correctly handle sensitive information by a member of the public.

Investigative process

On 12 July 2017, the matter was referred to the Professional Standards Unit for investigation (Attachment 3).

This investigation was conducted in accordance with the provisions of the *ACTPS Administrative and Related Classifications Enterprise Agreement 2013-2017* under which **Sch 2.2(a)(ii)** is employed.

Relevant witnesses were identified and interviewed which included the complainant, **Sch 2.2(a)(ii)** supervisor, and a member from another team involved in the matter. Virgin Australia Fraud Team, provided information regarding relevant policies and procedures via telephone. Information was obtained from Commonwealth Bank via telephone and at a meeting.

On 2 August 2017, the Delegate gave approval to retrieve **Sch 2.2(a)(ii)** email records within relevant search parameters. Emails from **Sch 2.2(a)(ii)** ACTPS email account were obtained from ICT Security and reviewed.

Information in relation to this matter was provided by:

Person	Position	Relevance to Investigation	Information source	Attachment
Sch 2.2(a)(ii)	External	Complainant	Unsigned Statement dated 28.8.207	4
Sch 2.2(a)(ii)	Project Manager	Witness	Statement dated 16.8.2017	5
Sch 2.2(a)(ii)	Senior Manager	Manager of Sch 2.2(a)(ii)	Statement dated 14.8.2017	6
Commonwealth Bank service representatives	Various	Advice on credit card process	File note dated 6.9.2017	7
Sch 2.2(a)(ii), Virgin Australia	Fraud Leader	Advice on fraudulent transaction and company policy.	Record of conversation dated 9.10.2017	8

Other Documents/Evidence

Description	Attachment
Explanation of events – email to Sch 2.2(a)(ii) dated 4 July 2017 and attached emails	9
Email records – Sch 2.2(a)(ii)	10
Virgin Australia flight documents	11

Initial enquires indicated a lack of policy, procedure or common practise to determine the correct process for handling sensitive information such as credit card details in this situation. Primarily, this was a result of it being uncommon for credit card information to be obtained by the Sch 2.2(a)(ii). Subsequently, on 31 August 2017, the delegate approved changes to the preliminary allegations.

On 4 September 2017, Sch 2.2(a)(ii) was provided in writing (Attachment 12) the following final allegation, particularised with the relevant information obtained, and was offered an opportunity to respond:

1. On Thursday 29 June 2017 you used credit card details provided by a member of the public for your own personal use.

Further particulars:

On 27 June 2017 you received credit card details from Sch 2.2(a)(ii) for the purposes of forwarding to the Sch 2.2(a)(ii) to process a payment.

On Thursday 29 June 2017 you booked flights with Virgin Australia for yourself and Sch 2.2(a)(ii) using the credit card details provided to you by Sch 2.2(a)(ii)

Examination of your ICT records shows that you received the booking confirmation and E-tickets from Virgin Australia to your ACTPS email account.

On Sunday 2 July 2017 Sch 2.2(a)(ii) noticed an unauthorised payment to Virgin Australia of around \$300 on her credit card statement and contacted them. She accessed the booking information

and noted flights booked in the name of **Sch 2.2(a)(ii)** and a person whom she believes to be your partner.

Sch 2.2(a)(ii) was interviewed on 7 September 2017 and was provided with a transcript of the recording. **Sch 2.2(a)(ii)** provided investigators with a verified copy of the transcript on 12 October 2017 (Attachment 13).

Allegation 1:

On Thursday 29 June 2017 **Sch 2.2(a)(ii)** used credit card details provided by a member of the public for your own personal use.

Summary of Evidence

The following facts are drawn from information contained in signed statements and documents, obtained from relevant parties.

Background

Sch 2.2(a)(ii)

Sch 2.2(a)(ii)

Sch 2.2(a)(ii)

Sch 2.2(a)(ii)

Sch 2.2(a)(ii)

option when paying online. **Sch 2.2(a)(ii)** called her and requested her credit card details, which **Sch 2.2(a)(ii)** informed her would be passed on to the **Sch 2.2(a)(ii)** to pay the difference between the selected **Sch 2.2(a)(ii)** **Sch 2.2(a)(ii)** said "I think it was a day or two before the **Sch 2.2(a)(ii)** so maybe 28 or 29 June 2017, when she called me."

Sch 2.2(a)(ii) stated that she provided **Sch 2.2(a)(ii)** her personal credit card details over the phone. The credit card she used for this purpose was in her own name and was a Commonwealth Bank MasterCard.

Sch 2.2(a)(ii) provided the following information:

*On the Sunday following the **Sch 2.2(a)(ii)** I was making payments relating to **Sch 2.2(a)(ii)** and checked my bank statements to see what had already been paid. At this time I noticed an unauthorised payment to Virgin Australia of around \$300.*

I called Virgin Australia to query the charge and they asked me if I knew someone called Sch 2.2(a)(ii), they didn't give me the last name. They wouldn't tell me much, but I realised I had the booking reference so was able to log into the booking. When looking at the booking details, I saw that the flight was booked for Sch 2.2(a)(ii) and her boyfriend (whose name I was able to confirm by looking on facebook).

I do not recall seeing payment details or what name was entered on the credit card details.

Sch 2.2(a)(ii) notified Sch 2.2(a)(ii) Project Manager Sch 2.2(a)(ii) of the unauthorised use of her card and also provided a formal statement to the police.

On 28 August 2017 Sch 2.2(a)(ii) was provided with a copy of her witness statement however, was unavailable to sign it prior to this report being finalised.

Sch 2.2(a)(ii)

Sch 2.2(a)(ii)

On 3 July 2017 he received a text message from Sch 2.2(a)(ii) containing words to the effect of "call me urgently please". He returned her call that day. He recalled:

She reported to me that there had been fraudulent activity on her credit card. She said that she had been charged for flights by Virgin Australia. She told me that Virgin would not give her the details of the booking but she somehow used the payment details to find the booking information herself. She discovered that the booking was made under the name of Sch 2.2(a)(ii) Sch 2.2(a)(ii) and was for flights in September 2017. Flights were also booked for a second passenger named Sch 2.2(a)(ii) who I know to be Sch 2.2(a)(ii) partner.

From recollection, Sch 2.2(a)(ii) had noticed a charge on her credit card and contacted Virgin to query it. She notified Virgin that it was an unauthorised payment.

Sch 2.2(a)(ii) immediately raised the issue with Sch 2.2(a)(ii) and then Sch 2.2(a)(ii) to seek advice on the appropriate course of action.

Following this, Sch 2.2(a)(ii) sent a formal email to Sch 2.2(a)(ii) supervisor notifying her of the matter.

Sch 2.2(a)(ii) declared a personal relationship with Sch 2.2(a)(ii) stating that she had previously worked with his partner and that they are now friends. He said that he found "her to be trustworthy and do not believe that this would have been an intentional action."

In relation to Sch 2.2(a)(ii) taking credit card details from Sch 2.2(a)(ii) stated:

Sch 2.2(a)(ii) has a heavy emphasis on doing what is best for the customer. In my opinion, Sch 2.2(a)(ii) would have taken the card details to provide an expedited solution to the problem with Sch 2.2(a)(ii). I believe she would have been trying to solve a problem that the customer had.

Sch 2.2(a)(ii)

Sch 2.2(a)(ii)

Sch 2.2(a)(ii) completed a preliminary assessment into the matter. Both the report resulting from her assessment and the witness statement provided dated 12 August 2017 were used as her evidence.

In the preliminary assessment report, Sch 2.2(a)(ii) noted the events that took place after being notified by Sch 2.2(a)(ii) of the complaint by Sch 2.2(a)(ii) regarding unauthorised use of her credit card by Sch 2.2(a)(ii).

On 4 July 2017 at 10.30, Sch 2.2(a)(ii) and I spoke with Sch 2.2(a)(ii). I read her the email I'd received from Sch 2.2(a)(ii) with the allegations detailed. As I read the email, Sch 2.2(a)(ii) raised her hands to her face and gasped. She said "I've used the wrong credit card, did I use her card details? Oh my god"

Sch 2.2(a)(ii) explained that she usually copies her credit card details from an old email she has in her sent items (and finds it through a word search in outlook). She stated that she must have just searched and copied the wrong numbers.

Sch 2.2(a)(ii) said she'd been contacted by Virgin the day before to advise they wouldn't be authorising her flight payment, because it wasn't her credit card. Sch 2.2(a)(ii) said she hadn't been able to explain the credit card issue and had assumed it was a mistake made by Virgin, because she had confirmed with her bank afterwards that the money hadn't been charged to her credit card.

Sch 2.2(a)(ii) further explained that she double checked her emails after being contacted by Virgin, to ensure she had deleted Sch 2.2(a)(ii)'s credit card details, to eliminate that as a possibility and said she could no longer find the email and assumed she had deleted it before booking her flights.

In her witness statement, Sch 2.2(a)(ii) also said:

Sch 2.2(a)(ii) had discussed with me (most likely on 23 June) her plans to attend a wedding in Perth and that she would require leave for this. She had discussed openly in the workplace that she was booking flights for this purpose. She also openly discussed with other team members when she was contacted by Virgin to inform her that there was a problem processing the credit card payment and how she was trying to figure out what had happened. She did not attempt to hide these details from anyone. Her behaviour did not seem suspicious.

Commonwealth Bank Customer Service Representatives

The Commonwealth Bank of Australia was contacted to confirm whether it was possible that Sch 2.2(a)(ii) could have made a successful online payment with Sch 2.2(a)(ii)'s credit card if she had entered her own name as the Cardholder Name, rather than the name listed on the card.

Conflicting advice from Commonwealth Bank was received.

On 6 September 2017 a Customer Service Representative from the Commonwealth Bank general information line stated that a payment could be electronically processed if an incorrect cardholder name was entered. She said that it would be possible if all other details were the same.

Following this, a staff member from the Commonwealth Bank Security Team provided information that it would be possible to order something online in another person's name, for example a flight booked for a third party. But she categorically stated that if a cardholder name is required in the credit card details section it must match exactly what is on the card for the payment to be processed.

On 7 September 2017 the Manager, Commonwealth Bank, Sch 2.2(a)(ii) stated that he believed he was not as knowledgeable on the process as the Security Team, however, he provided information that he knew from personal experience that an online credit card payment could be processed if an incorrect name was entered in the cardholder name field.

ICT Security email records

ICT Security provided an electronic file containing email records relevant to the investigation.

From these records, it is evident that on 27 June 2017 Sch 2.2(a)(ii) sent an email to Sch 2.2(a)(ii) Sch 2.2(a)(ii), containing credit card details provided to her by Sch 2.2(a)(ii) and requesting that Sch 2.2(a)(ii) use the details to process a payment of Sch 2.2(a)(ii). The credit card details contained within this email were related to a MasterCard ending in numbers Sch 2.2(a)(ii). This email was found by ICT Security within Sch 2.2(a)(ii) deleted items folder but it was indeterminable when it had been moved to this folder.

Also from the email records provided by ICT Security it could be seen that on 29 June 2017 Sch 2.2(a)(ii) received an email from Virgin Australia to her ACTPS email account entitled "Virgin Australia Itinerary". This email contained, as attachments, electronic receipts and a flight itinerary.

The flight documents showed that flights had been booked for Thursday 21 September 2017 with two passengers listed, being Sch 2.2(a)(ii). Two separate tax invoices were issued, both detailing a separate payment of \$169, listing payment by Credit Card - MasterCard XXXX XXXX XXXX Sch 2.2(a)(ii) frequent flyer number was also recorded.

Sch 2.2(a)(ii) forwarded the email from Virgin Australia to a Gmail account containing her own name.

Sch 2.2(a)(ii)

Sch 2.2(a)(ii)

On 4 July 2017, Sch 2.2(a)(ii) was informed of the complaint from Sch 2.2(a)(ii) regarding the unauthorised use of her credit card in a meeting with Sch 2.2(a)(ii) [The details of this meeting are contained within the preliminary assessment report.]

On the same day, Sch 2.2(a)(ii) submitted an email to Sch 2.2(a)(ii) which contained her explanation of the event and also copies of the two previously discussed emails containing credit card details. The first email is correspondence between herself and her gym administrator and contains credit card details which she requests be used for gym fee payment. The second is the email sent to the Sch 2.2(a)(ii) Sch 2.2(a)(ii) containing Sch 2.2(a)(ii) credit card details. On examination, it can be seen that both emails are formatted in a very similar manner. The emails contain very different content, however

when looking directly at the formatting of the credit card details in the emails side by side, there are no obvious differences between the two emails.

On Thursday 7 September 2017, **Sch 2.2(a)(ii)** responded to the allegation against her at interview.

Sch 2.2(a)(ii) confirmed that she had received credit card details from **Sch 2.2(a)(ii)** to allow her to pass the details to the **Sch 2.2(a)(ii)** team to arrange payment of the difference between the **Sch 2.2(a)(ii)** **Sch 2.2(a)(ii)**. She took the credit card details over the phone and stated "in hindsight I should have just forwarded [the call] through to them, but I had never been ... talked through the process to take any payments because it's not really a requirement of the team."

She stated that she recorded the credit card details directly into an email which she sent to the **Sch 2.2(a)(ii)** **Sch 2.2(a)(ii)** and then deleted the email from her sent folder.

Sch 2.2(a)(ii) confirmed that on Thursday 29 June 2017 she booked flights with Virgin Australia for herself and her partner. She recalled that she looked online at Virgin's "Happy hour" sale which occurs on Thursdays and found flights to Perth at a discounted rate. **Sch 2.2(a)(ii)** stated that she had left her wallet at home that day and remembered that she had previously sent an email to her gym with her own credit card details contained within it. She searched her sent emails folder and found it. She further stated:

I then doubted myself on when - what date the wedding was. I wanted to make sure it was the right week. So I went back into and did an "All emails" search, or "All Outlook" search to find all - pretty all, correspondence with one of my friends because I had asked her a couple of times when it was.

[I] found the date, confirmed [the date], and then just re-searched "MasterCard".

*So when I did the re-search I was in "All Outlook" emails, so it searched through my deleted items too, which I just didn't even realise that was still in there, that that **Sch 2.2(a)(ii)** email was in there.*

Sch 2.2(a)(ii) explained that **Sch 2.2(a)(ii)** email, being the more recent, would have been the first email to present in the search list.

Sch 2.2(a)(ii) believed that she may have used her Gmail address when purchasing the flights but wasn't certain.

She said that the following Monday after purchasing the flights [3 July 2017] she received a phone call from Virgin Australia asking if she had used her own credit card for the transaction. She had replied yes and provided her card number to them to confirm but was informed by Virgin that the numbers did not match. She stated "I was quite confused and baffled. I asked him if it could be a problem on his end, he said 'no'."

Sch 2.2(a)(ii) asked Virgin Australia if she could pay for the existing booking with her card and was told she could not. She subsequently lost her existing booking.

She stated that she had a conversation with her colleagues about it and "had a bit of a whinge".

She also contacted her mother via email to ask if she had inadvertently used her credit card for the transaction, as she stated that she knows her mother's credit card details off by heart.

During the interview Sch 2.2(a)(ii) provided personal bank statements to show that she had adequate funds available to her to pay for the original flights at the time of booking (Attachment 14). She also provided documents to show that on 15 August 2017 she rebooked flights for the same date and destination (Attachment 15).

Virgin Australia Representative

Between July and September 2017 Virgin Australia were contacted for information regarding this matter. A representative from Virgin Australia subsequently provided the requested information on 9 October 2017 after seeking legal advice.

Sch 2.2(a)(ii) Credit and Fraud Team Leader, provided information via the telephone and confirmed the details of the discussion by email. Sch 2.2(a)(ii) stated that they received a call from the credit card holder Sch 2.2(a)(ii) to advise them that she was unaware of the Virgin Australia booking that she had been charged for.

Sch 2.2(a)(ii) stated that the normal process was to contact the passenger who had made the booking but that most often the passenger details provided on a fraudulent transaction are falsified and the listed passenger is not contactable. In this case, the passenger, Sch 2.2(a)(ii), had entered accurate personal details.

Sch 2.2(a)(ii) stated:

If an online booking was paid for using a MasterCard and an incorrect name was entered in the Cardholder Name section but the numbers were correct for that card, the payment will still be processed.

Sch 2.2(a)(ii) was clear that, in this case, the name entered in the cardholder field was the same name as in the passenger field, being Sch 2.2(a)(ii)

Sch 2.2(a)(ii) also advised that following notification of an unauthorised payment, the passenger will not be permitted to pay for, or travel on that booking.

Analysis

From the evidence of Sch 2.2(a)(ii) she provided Sch 2.2(a)(ii) with her credit card details to pay for a price difference of a required Sch 2.2(a)(ii) later discovered an unauthorised transaction against her personal Mastercard from Virgin Australia.

Sch 2.2(a)(ii) does not dispute that she used the credit card details belonging to Sch 2.2(a)(ii) to purchase personal flights online with Virgin Australia for \$338 without authorisation. However, Sch 2.2(a)(ii) claims this was accidental and she was not aware at the time that she had used the wrong credit card details.

It is noted that, in each situation where Sch 2.2(a)(ii) recalled the events and her explanation, the details she provided were consistent each time.

Sch 2.2(a)(ii) claimed that she first located an email containing her personal credit card details, then searched "all outlook items" to find an email confirming the required travel dates. She then searched again for her credit card details, however this time she searched using the "all outlook items" search

bar rather than the "sent items" search bar and in doing so, inadvertently accessed the email containing **Sch 2.2(a)(ii)** credit card details which was in the deleted items folder.

In considering the similarities between the email containing credit card details in her name and the email containing the credit card details in the name of **Sch 2.2(a)(ii)** it is considered possible, due to how the credit card details were formatted, that the two could be inadvertently interchanged if the person accessing them was paying little attention to the detail.

Sch 2.2(a)(ii) explanation of how the email containing **Sch 2.2(a)(ii)** credit card details was accessed at the time of booking her personal flights appears to be a logical sequence of events.

Most notably in confirming **Sch 2.2(a)(ii)** claims that her use of **Sch 2.2(a)(ii)** credit card was accidental, is the evidence to show that she entered her own name, rather than **Sch 2.2(a)(ii)** in the cardholder name section of the credit card payment. While it is evidently possible that a payment could be processed with the incorrect name against the card number details, it seems most likely that, had **Sch 2.2(a)(ii)** intentionally used **Sch 2.2(a)(ii)** card in an attempt to have the flights charged to that account, she would have entered **Sch 2.2(a)(ii)** name as the cardholder name. It is also noted that **Sch 2.2(a)(ii)** entered accurate personal details on the transaction, including her own frequent flyer number, as seen on the original flight itinerary and tax invoice. Virgin Australia stated this was unusual for a fraud case.

In further support of her claim that she was unaware that she had fraudulently used **Sch 2.2(a)(ii)** credit card, it would seem unlikely that a person would speak so openly about the matter within her workplace, as stated by **Sch 2.2(a)(ii)** who said **Sch 2.2(a)(ii)** told her colleagues that her payment was considered unauthorised following notification from Virgin Australia.

Sch 2.2(a)(ii) stated that she asked Virgin Australia if she could pay for her existing booking with her own credit card when they notified her of the unauthorised transaction and that they had replied that she could not. **Sch 2.2(a)(ii)** from Virgin Australia confirmed that this would have been against their policy and standard procedure. It is noted from her willingness to pay for the flights and confirmation by bank statements that she had funds available to do so, implies that there was no genuine financial situation preventing **Sch 2.2(a)(ii)** from legitimately purchasing the flights at the time she used **Sch 2.2(a)(ii)** credit card details.

From the evidence gathered it is therefore reasonable to conclude that **Sch 2.2(a)(ii)** accidentally, rather than intentionally, accessed **Sch 2.2(a)(ii)** credit card details and used these details for the payment to Virgin Australia for personal flights.

Although reported in the Preliminary Assessment that **Sch 2.2(a)(ii)** was reasonable and understanding about the matter she did go on to file a police report and when interviewed discussed how she was required to cancel her credit card.

It is noted that **Sch 2.2(a)(ii)** actions, albeit considered accidental, caused significant inconvenience to a member of the public and further, has the serious potential to impact on the communities perception of the Directorate and the ACT Public Service's integrity and reputation.

Conclusion

On the basis of the information provided, there is sufficient evidence to conclude, on the balance of probabilities that on Thursday 29 June 2017 **Sch 2.2(a)(ii)** used credit card details provided by a member of the public for her own personal use.

This finding is based on an analysis by the investigator of the relevant evidence obtained. It is not a determination that misconduct has or has not occurred, which is a decision for you, as the delegate, to make.

In determining whether this behaviour constitutes misconduct (as defined in clause H6.5 of the ACTPS Administrative and Related Classification Agreement 2013-2017), you may wish to consider whether **Sch 2.2(a)(ii)** failed in her obligations under Section 9 of the *Public Sector Management Act 1994*, in particular:

- 2) A public servant must not—
 - (a) behave in a way that
 - (ii) undermines the integrity and reputation of the service;

Additionally, you may consider whether **Sch 2.2(a)(ii)** conduct has brought, or is likely to bring, CMTEDD Directorate or the ACT Public Service into disrepute.

Recommendations

It is recommended that, as the delegate, you:

- a) review this report, along with the accompanying evidence, to determine on the balance of probabilities whether misconduct has occurred;
- b) if misconduct is found, determine an appropriate sanction in accordance with the ACTPS Administrative and Related Classification Agreement 2013-2017; and
- c) notify **Sch 2.2(a)(ii)** of the outcome.

Sch 2.2(a)(ii)

Senior Investigator
Professional Standards Unit

18 October 2017

Sch 2.2(a)(ii)

Investigations Manager
Professional Standards Unit

19 October 2017

Attachments to report:

