Legislative Assembly for the
Australian Capital Territory
Standing Committee on Environment,
Planning, Transport and City Services

Submission Cover Sheet

Inquiry into the procurement and delivery of MyWay+

Submission number: 056.1

Submitter: Patrick Reid - Supplementary

Date authorised for publication: 3 April 2025

From: Patrick Reid
To: LA Committee - Environment
Subject: User data for Andrew Donnellan
Date: Thursday, 27 March 2025 12:49:36 PM
Attachments: [redacted]

Hey,

I hope you have been having a great day. I was watching the hearing and noted that a Government representative repeatedly claimed that data access was limited. You will find attached a copy of Andrew Donnellan's data (which he has permitted me to share with the committee).

Whilst I deleted all of the records that I collected, I had send Andrew's record to him so he could confidently state the scope of the vulnerability. This was stored in our message history. I would like to stress that I do not currently have the records of any other person. They have been deleted.

Attached is a file called *ajd_fare-media.json*. This is encoded in JavaScript Object Notation, a common format for sharing data between systems.

You can open this file in a text viewer (Windows notepad, macOS Text Edit), a web browser (FireFox, Google Chrome), or a code-specific editor (Visual Studio Code). I find that FireFox provides the clearest viewer.

This file contains a section called "response". This is an array of the fare-media Andrew had registered at this time. The first item in the list (sometimes numbered 0, because computers count from 0), is the testing card Andrew was issued. It has a card number of [redacted]. This section also includes the MyWay+ card's cvv and the mobile number associated with the card.

The second entry (numbered 1) is an EMV card, which is Andrew's bank card. The media number includes part of his bank card number. Specifically, the first 6 digits correspond to the first 6 digits on his bank card. The last 4 digits correspond to the last 4 digits on his bank card. The middle 6 digits ([redacted]) are seemingly random with no discernible data. It also includes the expiry date of the card. This card has since been canceled.

Andrew's account number is [redacted], which means to get this data, my script had to fetch all records between 0 and [redacted]. From memory, this was relatively few, because the first testing user started at 500. Not every account number corresponds to a valid set of user data. As I stated when in front of the committee, I fetched the records between 0 and just under 10,000. From memory, this corresponded to somewhere between 1.5k and 1.7k user records.

Given that the government seems to be unaware I collected these records, I believe there are roughly three options:

- There is a flaw in the way they collect logs. For example, they only collect

logs on the protected endpoints, which would mean that the vulnerability would have bypassed them
- They failed to interpret the data. My guess for a system of this size, is that they have many gigabytes worth of logs. It is impossible to search through every event individually.
- They know that I collected this data, and are lying to save face (I think this is very unlikely)

If you have any further questions, feel free to get in touch

Regards,
Patrick Reid