

## 5.1 OPTUS DATA BREACH

### LEAD/SUPPORT: JEREMY FENTON | CRAIG RIVIERE

The Australian Communications and Media Authority (ACMA) is investigating Singtel Optus Pty Limited (Optus) about its data breach, while working with other government agencies and telcos to protect customers and mitigate the risk of fraud.

### KEY ISSUES

- On 11 October 2022, the ACMA commenced an investigation into whether Optus contravened obligations enforced by the ACMA, due to its data breach on 21 September 2022.
- We are progressing this investigation as a priority however its nature requires a commensurate level of diligence and consideration. The ACMA cannot speculate about when findings may be made or published.
- The investigation has involved significant information gathering processes and analysis, noting the investigation is large, complex and novel, and Optus itself has taken some time to assess what happened.
- The ACMA news article released on 11 October 2022 is at **Attachment A**. The ACMA's opening statement of the 7 November 2022 Budget Estimates hearing about the events leading up to the investigation is at **Attachment B**.
- We are coordinating with other government agencies, including the Office of the Australian Information Commissioner, the Australian Competition and Consumer Commission and the Department of Home Affairs in relation to the investigation.
- We continue to monitor for spikes in Optus-related scams. We have not seen any direct indications that the data is being used by scammers. We observed an initial increase in opportunistic scams trying to use the data breach to trick people into providing their personal information. We issued alerts on 17 October 2022 and 25 January 2023.

### **ACMA investigation**

- The ACMA investigation is focused on Optus' compliance with regulatory obligations relating to the acquisition, authentication, retention, disposal and protection of personal information, and more general requirements to mitigate the risk of fraud set out in:
  - part 5-1A of Chapter 5 of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) relating to data retention
  - the Telecommunications (Service Provider— Identity Checks for Prepaid Mobile Carriage Services) Determination 2017, which imposes restrictions on the recording and keeping of certain information
  - the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022 (CID Determination) which, among other obligations, requires telcos to provide fraud mitigation protections to their customers
  - subsection 276(1) of Part 13 of the *Telecommunications Act 1997* (the Telecommunications Act)
  - section 313 of Part 14 of the Telecommunications Act
  - the Telecommunications Consumer Protection Code (TCP Code).

- We have used our information gathering powers under section 521 of the Telecommunications Act to obtain information and documents relevant to our investigation.
- At the 7 November 2022 Budget Senate Estimates a copy of the notice issued to Optus was requested and our response is at **Attachment C**. A request for copies of all correspondence and notices relating to the investigation to be provided to the Environment and Communications committee members was also made at the 14 February 2023 Budget Estimates. The ACMA response is at **Attachment D**.
- A notice given under section 521 of the Telecommunications Act allows the ACMA to collect information relevant to determining whether there is a possible breach of the law. Contents of statutory information gathering notices are not publicly disclosed prior to the conclusion of an investigation to avoid:
  - prejudicing the investigation and the ability for the entity to respond to the notice efficiently, and;
  - potentially prejudicing other investigations or enquiries, that may be occurring at that time, by disclosing methods for investigating and dealing with similar matters.
- There are a range of enforcement options available to the ACMA if our investigation finds that Optus has not complied with its regulatory obligations, potentially including formal warnings, remedial directions, infringement notices and civil court action to seek pecuniary penalties.

***Other telco data breaches/privacy breaches***

- On 9 December 2022, Telstra published on its website that some of its unlisted customers' details were incorrectly made available via Directory Assistance or the White pages.
  - On 14 December 2022, TPG Telecom notified the Australian Securities Exchange (ASX) and the ACMA that it had identified unauthorised access to its Hosted Exchange service, which hosts email accounts for up to 15,000 iiNet and Westnet business customers.
- [REDACTED]
- [REDACTED]

**BACKGROUND**

***Timeframes***

- The investigation into the Optus data breach is large and complex. So far, the ACMA has given three notices under the Telecommunications Act to obtain information. Further notices may need to be given.

***Information sourced from v.9 of WoG document, released 4 October 2022***

- On 22 September 2022, Optus released a media statement advising it had identified a data breach involving the exfiltration of potentially millions of its current and former customers' personally identifiable information from its network. Optus advised that:
  - payment details and account passwords had not been compromised
  - Optus services such as mobile, home internet and voice calls had not been affected
  - it commenced providing personal notifications to customers deemed to have 'heightened-risk'.



- Optus advised that the data may include the names, dates of birth, phone numbers and email addresses of as many as 9.8 million customers. For a sub-set, that it also includes their address, driver licence and passport number.
- On 27 September 2022, an actor on the 'Breached' online forum released a 10,000 sample data set and threatened to continue to release data over the next 4 days until a \$1 million payment was paid. The actor then deleted their post and claimed to no longer wish to sell the data. It is possible that other actors took copies of the data.
- On Thursday 29 September 2022, Optus confirmed the exfiltration of 14,900 current Medicare card numbers and 22,000 expired Medicare card numbers. Optus advised it would shortly contact all affected customers.
- On Monday 3 October, Optus provided an update in which it confirmed:
  - approximately 1.2 million customers had at least one number from a current and valid form of identification, and personal information, compromised. Optus communicated with these customers and recommended that they take action to change their identification documents
  - approximately 900,000 customers had numbers relating to expired IDs compromised, in addition to personal information. Optus continued to work with governments and agencies regarding what further steps, if any, those customers should take
  - approximately 7.7 million customers had data containing details such as email addresses, dates of birth or phone numbers compromised.

## **ATTACHMENTS**

<b>Attachment A</b>	ACMA media release about investigation into Optus Data Breach
<b>Attachment B</b>	ACMA opening statement – Budget Senate Estimates – 7 November 2022
<b>Attachment C</b>	Questions on Notice and response from Budget Senate Estimates – 7 November 2022
<b>Attachment D</b>	Questions on Notice and response from Budget Senate Estimates – 14 February 2023

**Clearing Officer**  
Jeremy Fenton  
General Manager  
Content Division  
Ph (03) 9963 6909  
[REDACTED]

**Contact Officer**  
Craig Riviere  
EM Telecommunications  
Safeguards and Numbers Branch  
[REDACTED]

Date 3/10/2023

**News article 11 October 2022: ACMA Investigation into Optus Data Breach**

The Australian Communications and Media Authority (ACMA) has advised Singtel Optus Pty Limited (Optus) that it has commenced a formal investigation in response to the September 2022 Optus data breach.

The ACMA will investigate the data breach in regard to Optus' obligations as a telecommunications service provider. These include obligations relating to the acquisition, authentication, retention, disposal and protection of personal information, and requirements to provide fraud mitigation protections.

The ACMA's investigation will take some time and will be made public once completed. The ACMA will not be commenting further as the investigation progresses.

The ACMA is working in conjunction with the Office of the Australian Information Commissioner and the Department of Home Affairs to ensure effective information-sharing across the respective jurisdictional investigations.

**Quote from ACMA Chair, Nerida O'Loughlin**

"When customers entrust their personal information to their telecommunications provider, they rightly expect that information will be properly safeguarded. Failure to do this has significant consequences for all involved.

All telcos have obligations regarding how they acquire, retain, protect and dispose of the personal information of their customers. A key focus for the ACMA will be Optus' compliance with these obligations.

We look forward to full cooperation from Optus in this investigation."

**Budget Estimates – ACMA opening statement (7 November 2022)**

The ACMA was notified by Optus of the data breach on 22 September shortly before the company released its public statement. In the first few days following the breach, we worked with agencies across government, including our portfolio department, to inform advice to government both about the risks of scams and identity theft to affected Optus customers and what mechanisms could be used to facilitate Optus sharing relevant information with banks and financial institutions.

After this initial focus, we moved to consider whether the nature of the breach raised any questions about Optus' potential compliance with the telco specific obligations we are responsible for enforcing. This consideration was based on information in the public domain and that which had been provided to government by that time.

On 11 October, we opened an investigation under the Telecommunications Act and have since issued an information gathering notice to various Optus entities. This is designed to elicit detailed information about the nature of the incident. Key issues we will need to consider are:

- Whether Optus was collecting and keeping any personal data that it was prohibited from doing.
- Whether Optus was not disposing of any data it was required by law to dispose of in the required timeframes.
- Whether Optus was keeping any personal data in the manner the law requires where there are obligations to keep it in a particular way, including under encryption.

We are looking at Optus' compliance under various laws, including the Telecommunications Act, the Telecommunications (Interception and Access) Act, identity checks for pre-paid mobile services and customer identity authentication rules and some requirements of industry's consumer protection code.

It is early days in our investigation and we have not formed a view as to whether Optus has breached any of its obligations. This will be a large and complex investigation, and one on which we are working collaboratively with colleagues at the Office of the Australian Information Commissioner and the Department of Home Affairs. It is not possible at this early stage to be definitive about when the investigation will conclude but I would expect it will take some months. We will make our investigation public once finalised.

**Environment and Communications  
QUESTION ON NOTICE  
Budget Estimates 2022 - 2023  
Infrastructure, Transport, Regional Development, Communications and the Arts**

**Departmental Question Number:** SQ22-000545

**Division/Agency Name:** Australian Communications and Media Authority

**Hansard Reference:** Spoken, Page No. 77 (7 November 2022)

**Topic:** ACMA - Information notices issued to Optus

**Senator Sarah Henderson asked:**

Ms O'Loughlin: We do have concerns. As I mentioned, there are a wide variety of rules that we're having a look at. We need to get a significant amount of detailed information from Optus first to be able to come to some of the issues that I outlined in our opening statement. For example, were they collecting and keeping any data that they were not required to keep? Were they not disposing of any data that they were required to dispose of? Were they keeping any personal data that wasn't kept in the way that the law envisages—for example, under encryption? They are the types of things that we will be investigating. For example, there are some that require the keeping of a name, address and mobile number—which you imagine that a mobile provider would keep. Were they keeping that securely? For our prepaid identification determination, they must record or be able to say that they have seen passport or driver's licence information. But they are required by law to dispose of that in a timely manner. What we are trying to gather is enough information for us to look at each of those areas. Have they kept stuff that they should have kept, whether they've kept it encrypted or whether they've actually kept stuff that shouldn't have been kept. That's what we're working our way through in this investigation.

Senator HENDERSON: So these information notices have been issued to Optus?

Ms O'Loughlin: They have indeed.

Senator HENDERSON: Are you able to provide the committee with a copy of those notices?

Ms O'Loughlin: I will take that on notice only because we are covered by some quite tight information sharing provisions. I will certainly take that on notice and do our best to provide that to the committee.

Senator HENDERSON: Unless you want to raise a claim.

Ms O'Loughlin: No.

Senator HENDERSON: I am asking for a copy of that information.

Ms O'Loughlin: I might need to advise Optus that you have asked that question.

Senator HENDERSON: Thank you very much.

Ms O'Loughlin: But we will do that to the best of our ability.

Senator HENDERSON: Thank you...

**Answer:**

On 11 October, the ACMA opened an investigation under the Telecommunications Act and has since issued an information gathering notice to various Optus entities. In general terms, this notice is designed to elicit detailed information about the nature of the incident such that we can determine:

- Whether Optus was collecting and keeping any personal data that it was prohibited from doing.
- Whether Optus was not disposing of any data it was required by law to dispose of in the required timeframes.
- Whether Optus was keeping any personal data in the manner the law requires where there are obligations to keep it in a particular way, including under encryption.

It is possible that the ACMA may need to seek additional information from Optus under statutory notice as its investigation progresses.

The ACMA is concerned that the disclosure of detailed statutory information gathering notices might reasonably be expected to prejudice the current investigation into a possible breach of the law.

The ACMA will publicly release the findings of its investigation once completed. This will include a broad description of the relevant data received from Optus that informed the ACMA's decisions.

**Environment and Communications  
QUESTION ON NOTICE  
Budget Estimates 2022 - 2023  
Infrastructure, Transport, Regional Development, Communications and the Arts**

**Departmental Question Number:** SQ23-003200

**Division/Agency Name:** Australian Communications and Media Authority

**Hansard Reference:** Spoken, Page No. 66 (14 February 2023)

**Topic:** ACMA - Optus Cyber Investigation

**Senator Sarah Henderson asked:**

Senator HENDERSON: ... Chair, I just want to quickly ask ACMA about the Optus cyber investigation. Ms O'Loughlin, could you provide an update into ACMA's investigation into the Optus cyber breach, please?

Ms O'Loughlin: As you know, we commenced our investigation in October. We are currently working collaboratively with other government agencies, including the Office of the Australian Information Commissioner, the ACCC and the Department of Home Affairs, who are undertaking various investigative processes. Our focus has really been on compliance of Optus around things like data retention, recording and keeping certain information, mitigation protections for customers and the security of network. We are progressing that investigation. We have used our information-gathering powers to receive quite a significant amount of information from Optus to date. Recently, we went back to Optus with another series of information-gathering notices to provide us with more information. We will be reviewing that information and the initial information over the coming weeks. I think that's probably all I've got to report back to you on that at the moment.

Senator HENDERSON: Ms O'Loughlin, would you be able to provide to the committee, on notice, all correspondence, including those notices, in relation to your investigation? All correspondence, submissions, emails?

Ms O'Loughlin: I will need to take that notice.

Senator HENDERSON: Thank you.

Ms O'Loughlin: We did respond to a question on notice from you on this, and we do have some concerns around disclosing the detailed statutory information-gathering notices, as our view is that it might be reasonably expected to prejudice the current investigation. So I will take it on notice.

**Answer:**

On 11 October, the Australian Communications and Media Authority (ACMA) opened an investigation under the Telecommunications Act and has since issued two information gathering notices to various Optus entities. In general terms, these notices are designed to elicit detailed information about the nature of the incident such that we can determine:

- Whether Optus was collecting and keeping any personal data that it was prohibited from doing.



**ATTACHMENT D**

- Whether Optus was not disposing of any data it was required by law to dispose of in the required timeframes.
- Whether Optus was keeping any personal data in the manner the law requires where there are obligations to keep it in a particular way, including under encryption.

It is possible that the ACMA may need to seek further additional information from Optus as its investigation progresses.

The ACMA is concerned that the disclosure of detailed statutory information gathering notices, Optus' response to these and any other correspondence between the ACMA and Optus might reasonably be expected to prejudice the current investigation into a possible breach of the law.

The ACMA will publicly release the findings of its investigation once completed. This will include a broad description of the relevant data received from Optus that informed the ACMA's decisions.