HOME AFFAIRS
QUESTION TIME BRIEF (QTB)

DATA SECURITY BREACHES

KEY TALKING POINTS:

- On 22 September 2022, Optus released a media statement advising they had identified a data breach involving the exfiltration of current and former customers' personally identifiable information.

- Optus advised that the data includes the names, dates of birth, phone numbers and email addresses of as many as 9.8 million customers. For a sub-set, it also includes their address, drivers licence and passport numbers.

- Optus has advised that:

  - Payment details and account passwords have not been compromised.

  - Optus services such as mobile, home internet and voice calls have not been affected.

- On 27 September 2022, 10,000 records were released on the 'Breached' online forum with a threat to continue to release data over the next four days until a $1m payment was paid. The criminal has since deleted their post and claims to no longer wish to sell the data. It is possible that other criminals took copies of the data.

- Optus advises that it has been notifying customers deemed to have 'heightened-risk'.

If asked: What is the government doing to protect Australians?

· Optus working closely with the Australian Signials Directorate's Australian Cyber Security Centre (ACSC), the Office of the Australian Information Commissioner (OAIC), the Australian Federal Police (AFP), financial institutions and other government regulators.

· The Department of Home Affairs has established a Commonwealth Credential Protection Register to help stop compromised identities from being used fraudulently.

  - The Register will prevent compromised identity credentials on the Register from being verified through the Document Verification Service. The Document Verification Service is used by government agencies and businesses, such as banks, to verify an individual's identity online.

- This will prevent credentials that are included on the Register being used fraudulently, such as taking out loans or setting up accounts. Rightful owners will also not be able to use them online. New credentials issued following the data breach will work as normal.

- In the interim, impacted individuals should consider using alternative credentials or speak to service providers that ask for identification for other options, such as visiting the service in person to present the credential.

- As at 13 October 2022, the Register includes around 100,000 Australian Passports. These passporst can still be used for international travel.

· The ACSC is supporting Optus with cyber security incident response and ongoing technical advice, and supporting other telecommunications providers that may be affected.

· The AFP is working with Optus to obtain the crucial information and evidence needed to conduct this complex, criminal investigation.

s. 37(1)(a)

· The AFP and state and territory police have also set up operation GUARDIAN to enable the protection of more than 10,000 customers whose identification creditentials have been unlawfully released online.

· The OAIC is working with Optus to ensure they are complying with the requirements of the Notifiable Data Breaches scheme and providing advice on how Australians can respond and protect themselves from further harm.

· The Attorney General's Department is reviewing the *Privacy Act 1988* to ensure that Australia's privacy laws are fit for purpose in the digital age and that they accord with community expectations in light of the rise of digital platforms and other technological changes.

· The Government provides funding to IDCare, Australia's national identity support service. IDCare offers support to affected members of the community across Australia who have concerns about their identity or related cyber security.

If asked: What is Optus or the Government doing about the sale of that data?

· The matter has been referred to the AFP. The AFP is aware of reports alleging that stolen Optus customer data and credentials are being sold through illicit forums.

HOME AFFAIRS
QUESTION TIME BRIEF (QTB)

DATA SECURITY BREACHES

s. 37(1)(a)

- The AFP and state and territory police have set up operation GUARDIAN to enable the protection of more than 10,000 customers whose identification creditentials have been unlawfully released online.

s. 37(1)(a), s. 37(2)(b)

- It is an offence to buy stolen credentials. Those who do face a penalty of up to 10 years' imprisonment.

If asked: Do we know who perpetrated this attack? Was it a state actor?

- Cyber crime investigations are complex and while the impact of a breach may be immediate, understanding what has occurred takes time.

- The initial priority is helping Optus remediate their networks and recover as quickly as possible, and notifying those immediately impacted.

- The Government will only make a public attribution when it is clear and in our national interest to do so.

If asked: What steps has the government taken under the critical infrastructure reforms?

- Optus is a designated critical infrastructure provider and has made a mandatory report under the *Security of Critical Infrastructure Act 2018*.

  The Department of Home Affairs regulates Optus under the *Telecommunications Act 1997* and the *Security of Critical Infrastructure Act 2018*.

If asked: Was this a ransomware attack?

- There are no indications this was a ransomware attack.

If asked: What is the government doing to keep our data safe?

- The Government is taking an all vectors approach to cyber and data security.

- The Government's new Cyber Strategy will build whole of nation resilience against these types of attacks and ensure our networks and devices are protected against malicious actors.

HOME AFFAIRS
QUESTION TIME BRIEF (QTB)

DATA SECURITY BREACHES

- The Department of Home Affairs is developing Australia's first National Data Security Action Plan, which will map the nations' data security settings and provide measures to strengthen consistency and resilience against data security threats.

s. 37(1)(a), s. 37(2)(b)

- The Attorney General's Department is reviewing the *Privacy Act 1988* to ensure that Australia's privacy laws are fit for purpose in the digital age and that they accord with community expectations in light of the rise of digital platforms and other technological changes.

· The Australian Government works with industry to take action and address the possible consequences and harm relating to a serious data breach.

· Under the Notifiable Data Breaches scheme, entities regulated by the Privacy Act must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.

The Government provides funding to IDCARE, a not-for-profit organisation providing identity support services. IDCARE offers personalised support to individuals who are concerned about their personal information.

If asked: Is the government concerned about the recent data breaches including

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

· These data breaches are further reminders of the need for strong cyber security.

· Australians need to be confident their information is protected. Affected entities will continue to access appropropiate advice and support from the ACSC and Home Affairs.

BACKGROUND AND CHRONOLOGY

· 21 September 2022 – Optus identified potential compromise and reported a data breach to the ACSC.

HOME AFFAIRS

QUESTION TIME BRIEF (QTB)

DATA SECURITY BREACHES

- 22 September 2022 – Optus released a media statement on their website, advising of the cyber incident and the associated actions taken to investigate and remediate.

- 22 September 2022 – Office of the Australian Information Commissioner (OAIC) released a statement advising of the Optus data breach and provided advice about how Australians can respond to a data breach notification and protect themselves from further impacts of a data breach.

s. 37(1)(a)

- 27 September 2022 – 10,000 records were released with a threat to continue to release data over the next four days until a $1m payment is paid.

- 28 September 2022 – The Foreign Affairs Minister has contacted Optus to cover the cost for replacement passports.

- 28 September 2022 – The Prime Minister, confirmed that Optus has agreed to cover the cost for replacement passports.

- 04 October 2022 – Optus has provided the Australian Government with the detailed information of customers who had Medicare cards, or other government credentials, exposed.

- 11 October 2022 – The OAIC and ACMA commenced an investigation into the personal information handling practices of Singtel Optus Pty Ltd in regard to the data breach.

HOME AFFAIRS

QUESTION TIME BRIEF (QTB)

DATA SECURITY BREACHES

MEDIA

Date	Outlet	Reporting
15 October 2022	**ABC News**	MyDeal.com.au, a subsidiary of the Woolworths Group, has announced that data was exposed when its customer relationship management system was accessed by a "compromised user credential". Woolworths MyDeal becomes latest target of cyber attack. What information was leaked and what can you do if you're affected?
14 October 2022	**Nine News**	The AFP are scrambling to ensure the safety of some of its secret agents and operations exposed in a massive cyberhack of Colombian government files. AFP concerned for safety of anti-drug agents exposed by data hack
13 October 2022	**ABC News**	Medibank Private says it has been hit by a cyber attack. The company said 'unusual activity' had been detected on its network, but there was not evidence that sensitive data had been accessed. Health insurer Medibank Private hit by cyber attack
13 October 2022	**itNews**	Home Affairs boss Michael Pezzullo has suggested the Optus breach, while driving much discussion about cyber security policy, isn't necessarily a good model for policy debates. Home Affairs: Optus breach is not a model for policy debate
11 October 2022	**Sydney Morning Herald**	The Office of the Australian Information Commissioner and the Australian Communications and Media Authority announced co-ordinated investigations to investigate whether Optus needed to keep extensive data on millions of its customers and understand how it was stored. OAIC launches investigation into telco
11 October 2022	**Australian Financial Review**	Experts who advise big companies on their data strategies say they are seeing a post-Optus surge in inquiries from executives who don't even understand existing rules, while tech chiefs at both Commonwealth Bank and ASX said companies had to review and ensure they were using data for valid reasons. Optus breach: Corporate Australia expects tough privacy laws, rushes to check data hoards
11 October 2022	**ABC News**	Optus customers who signed up using international identification say they feel abandoned by the company, and are unsure whether they need to replace documents or who will cover the cost. International students, visa holders feel 'abandoned' by company
7 October 2022	**Daily Telegraph**	An Australian law firm has formally started legal action against telco giant Optus to seek compensation for the millions of customers who had their personal information stolen in last month's cyber attack. Aussie law firm Maurice Blackburn files action against telco
6 October 2022	**ABC News**	Operation Guardian the Australian Federal Police (AFP) investigation set up after 10,200 customer records were published online following the Optus cyber attack has arrested and charged a 19-year-old Sydney man.

DATA SECURITY BREACHES

		The AFP announce the first arrest linked to the Optus data breach.
6 October 2022	**ABC News**	The federal government has released planned changes to telecommunications laws following the Optus data breach, which affected nearly 10 million customers and former customers. Government strengthens powers for telcos to share affected data following Optus hack
3 October 2022	**Daily Telegraph**	Optus has informed current and former customers whether their driver licence and card numbers were exposed in the cyberattack — but has again come under fire over its poor communication and ongoing confusion. Problem with Victorian driver licence number text notification
29 Sep 2022	**ABC News**	Professor Asha Rao, Associate Dean of Mathematical Sciences at RMIT University, says Australia needs new laws to prohibit companies from engaging in unnecessary data harvesting. Too much data collection means we're more at risk of having personal details stolen, expert say
28 September 2022	**The Guardian**	Australians residing in New South Wales, Victoria, Queensland and South Australia who were affected by the data breach, will be able to change their driver's licence numbers and receive new cards. Optus is expected to bear the multimillion-dollar cost of this changeover. Optus data breach: Australians will be able to change their driver's licence with telco to pay.
27 September 2022	**Twitter**	Chris O'Keefe, Political Reporter for 9News claims that victims are now receiving text messages from hackers demanding $2000AUD be paid into a CBA bank account, with threats their data will be sold for "fraudulent activity within 2 days." Chris O'Keefe: Victims are now receiving text messages from hackers.
27 September 2022	**ABC News**	An online account that claims to be behind the Optus data breach says it has deleted its only copy of customers' information and it no longer cares about a ransom. Online account claiming to be behind data leak apologises, drops ransom threat.
27 September 2022	**The Sydney Morning Herald**	Fresh laws to constrain the use of facial recognition technology used by retailers, police and schools - are a step closer to reality after the Optus breach. New laws to tackle hackers head-on.
27 September 2022	**The West Australian**	Anthony Albanese says companies will be forced to notify banks faster when they experience cyber attacks, after describing the hacking of the country's second-biggest telecoms firm as a "a huge wake-up call" for the corporate sector. Albanese puts banks on notice as AFP joins Optus hack probe.
27 September 2022	**Australian Financial Review**	The focus of the disastrous Optus data breach has shifted from the company's campus in Sydney's Macquarie Park to the Canberra office of Home Affairs and Cyber Security Minister Clare O'Neil. Optus breach needs federal response.

HOME AFFAIRS
QUESTION TIME BRIEF (QTB)

DATA SECURITY BREACHES

27 September 2022	**Australian Financial Review**	Companies may face multimilliondollar fines for failing to protect customer data from hackers, as Home Affairs Minister Clare O'Neil rebuked Optus over its data breach that has affected almost 10 million Australians. Labor scolds Optus, flags stricter laws.
26 September 2022	**The Canberra Times**	Slater and Gordon is investigating a potential class action against Optus on behalf of current and former customers who have been affected. Optus: Class action under consideration for customers.
26 September 2022	**7 News**	Optus has announced it would offer 12 months of free credit monitoring from a credit reporting agency Equifax for their "most affected" current and former customers. Telco to offer credit monitoring program amid fears hack could lead to identity theft.
26 September 2022	**ABC News**	Home Affairs Minister said today that the massive breach of Optus customer data should not have happened, and urged the company to offer free services to monitor customer accounts for fraud. Home affairs minister points finger at Optus, saying hack should not have happened.
25 September 2022	**The Age**	News of the Optus cybersecurity attack is shocking. The millions of customers potentially impacted by the breach is mind-boggling. But the real startling question is how a breach of this magnitude is still occurring in 2022. No, Optus doesn't need to keep your sensitive information for so long.
25 September 2022	**Mercury**	A person claiming to be the evil genius responsible for the Optus data breach is demanding $1.5 million in ransom money from the telco giant. Optus data breach: Hacker demands $1.5 million ransom, customer info leaked on dark web.
25 September 2022	**7NEWS**	Optus customers whose passport or driver's licence numbers were stolen in a massive data breach are being contacted, amid warnings that scammers will try to profit from the cyber attack. Optus issues fresh warning as $1.5m ransom threat is investigated: 'Do not click'.
25 September 2022	**ABC News**	The Home Affairs Minister is soon expected to announce several new security measures following the massive Optus data breach that saw hackers steal the personal details of up to 9.8 million Australians. Federal government to unveil new security measures following massive Optus data breach.
24 September 2022	**9news**	Optus said today the attack could trigger illegitimate offers to sell customer details online as a user on a data breach forum has claimed two files containing sensitive customer information will be sold if a $1.53 million ransom is not paid within a week. Optus cyber attack investigation amid alleged ransom threat.

HOME AFFAIRS
QUESTION TIME BRIEF (QTB)

DATA SECURITY BREACHES

24 September 2022	**SBS News**	Optus has admitted it is likely that criminals will make claims capitalising financially on the leak, after the company announced it was a victim of a major cyberattack, but says it won't comment on the veracity of the claims its customer data is being sold online. Federal police monitoring reports of stolen Optus data being sold on the dark web.
24 September 2022	**Guardian**	Attorney general Mark Dreyfus has been briefed by the privacy commissioner about hack and is seeking 'urgent' meeting with telco AFP investigates $1m ransom demand posted online for allegedly hacked Optus data.
23 September 2022	**ABC News**	Anonymous senior Optus figurehead offers confidential insights into the early findings of the investigation. Breach likely down to human error. 'Human error' emerges as factor in Optus hack affecting millions of Australians.
23 September 2022	**The Guardian**	Peter Dutton criticises Government's handling of Optus breach and emphasises the need for Ministers to provide information and assurances to the public. Australia news live: Dutton reiterates support for national anti-corruption commission; stranded whale rescue operation continues.
23 September 2022	**Newcastle Herald**	Senator Sarah Henderson has urged Labor to deliver tougher online privacy and data protection laws and to adopt the Coalition's Online Privacy Bill. Laws questioned after Optus cyber attack.
23 September 2022	**ABC Radio National**	Shadow Minister for Cyber Security, Senator James Patterson will be requesting a briefing from the government, and has questions about what steps the government took at when under the critical infrastructure reforms. Optus data breach could be Australia's largest - ABC Radio National- Optus data breach could be Australia's largest.

Lead Division
Cyber Digital and Technology Policy Division,
Department of Home Affairs
Contact: First Assistant Secretary Brendan Dowling
Division: Cyber Digital and Technology Policy
Date first prepared: 23 September 2022
Originating Source: MO

Mobile: s. 22(1)(a)(ii)
Action Officer: s. 22(1)(a)(ii)
Date last Updated: 9/11/2022 - 10:11 AM

Cyber Security Resilience Division, Australian Signals Directorate
Contact: First Assistant Secretary Jessica Hunter
Division: Cyber Security Resilience
Date first prepared: 23 September 2022
Originating Source: 24/7 Operations

Phone: s. 22(1)(a)(ii)
Action Officer: s. 22(1)(a)(ii)
Date last Updated: 9/11/2022 - 10:11 AM