OPTUS

A letter to our customers

To our customers,

Over the past month, we've taken a range of actions to try to prevent harm from coming to any customer as a result of the cyberattack. In the spirit of transparency, and to help you to better understand the unchartered and complex territory we navigated, we wanted to share these actions with you.

1. **We went public early with widespread warning** – we identified the incident, immediately shut down the cyberattack and alerted the public within a day of confirming what had happened. We informed the public to enable Australians to be alert for scams and password changes and any other anomalies that could signify attempted use of their data. We also knew it would put other businesses on alert so they could be on the lookout for attempted scams or incidents and could take any necessary steps to protect their employees and customers. In our initial media release, we also immediately let people know that we would be offering credit monitoring to those most affected as an extra precaution.

2. **We engaged with the government openly, transparently, and quickly, and respected the request of the Australian Federal Police to not speak in specifics about the attack** – we alerted both the Australian Cyber Security Centre and Australian Federal Police promptly so they could try to track down the responsible parties. Rapid collaboration with these two agencies made it more difficult for the criminals to use or profit from the data taken, and both the ACSC and AFP have acknowledged our timely and transparent engagement. We briefed key Federal Government Ministers and their offices on the incident, prior to our public announcement and on an ongoing basis. We respected the AFP's strict instructions to not speak publicly about any specific aspects of the attack, as we understand they rely on an information asymmetry in tracking down the responsible parties. We remain committed to working with the AFP to help them track down the criminals and retrieve our customers' data.

3. **We reconstructed the data set that was exposed** – this was no small feat. We had to reconstruct from raw log files the information that was exposed during the attack. This involved parsing, sorting, analysing and organising many terabytes of raw data. We had to do this meticulously, maintaining traceability and quality control so that we could recreate with a high level of confidence a reliable and complete picture of the relevant data. This painstaking analysis would then enable us to communicate with customers accurately.

4. **We contacted all affected customers** – while managing the data extrapolation process and seeking to be as accurate as possible, we reached out to all customers who we suspected could have had an ID document number exposed, even where that ID document had expired. This meant those customers could be extra vigilant for any suspicious activity.

5. **We then set about providing individual notification to customers about their specific data exposed, and what they needed to do as a result** – having completed the complex process of understanding what data had been exposed in the attack, we wanted to communicate to customers who had ID document numbers exposed with specific actionable advice. We worked with more than 20 different departmental and ID issuing authorities to determine what the right recommended actions were. The Optus team worked closely with those authorities, to get the right advice for customers. This process highlighted the way different ID documents are used and protected in various government organisations. While we remain extremely disappointed that this attack occurred, we hope that the coordinated response will help refine the approach to cyberattacks across business and government in the future. As a result of these actions, we have now sent communications to all customers who had an identity number exposed with clear and bespoke messaging. In the space of three weeks, we developed over 110 separate communication messages, sanctioned by the appropriate ID authority, and sent these to millions of customers.

6. **We apologised, took accountability, and kept our website up to date** – we have acknowledged this attack should not have happened and that we must do better to ensure our customers' ID documentation is safe. We have sought to engage publicly when and where we can even when we knew we didn't have all the answers yet, or when we were respecting the AFP's request not to make comments clarifying our cyber security defences. We also made sure our website was continually kept up to date. When we heard our messages were confusing to some people, we improved them, and we put up guides on our website to help customers understand them better. We listened, we learned, and we responded in real time. We apologised to our customers, and we kept our focus on taking actions to keep them safe. We also put on more staff in our call centres and tried to answer the questions and complaints from our customers as quickly as we could. This is still a work in progress, but rest assured we continue to take accountability.

7. **We complied with requests for information from governments** – we have responded to over 25 requests for information from government and regulatory bodies and continue to work with governments to cover the costs for replacing documents where customers have been advised to replace them.

8. **We have shared the lessons learned** – meeting with leading Australian businesses to alert them to the steps they may need to take in the event of a cyberattack.

Thanks to all these actions we are not aware of any harm coming to any customer from the misuse of their exposed data, but we have reminded all customers to remain vigilant. We are aware of 10,000 customer details being released on the web briefly, and those customers were notified so they could take action to replace identity documents and protect themselves. Thanks to the AFP's Operation Guardian, a person trying to take advantage of our customers with a scam was arrested, with no customer falling for the scam. We will continue to support the AFP and Operation Hurricane in the hope it will help the AFP track down the responsible party and retrieve our customers' data.

In addition, we have commissioned an independent external review - led by Deloitte - into the cyberattack and how criminals got through our defences this time, when we thwart over a million attacks a year and invest significantly in our cyber capabilities. We are committed to learning, doing better in the future, and sharing lessons so all companies and all Australians can benefit from our terrible experience.

We want to thank all our people, as well as employees across several Government agencies, departments and ministerial offices – all of whom have worked so tirelessly to help our customers.

As we move forward from this cyberattack, we make a commitment to you that we will strive to not just do better in the future - but strive for best.

Sincerely,
Your Optus Team