25 March 2021

The Hon. Tara Moriarty MLC
Chair
Portfolio Committee No. 1 Premier and Finance
Inquiry into Cybersecurity
c/- Portfolio Committee Secretariat

via email: portfoliocommittee1@parliament.nsw.gov.au

Dear Ms Moriarty

I appeared as a witness on 3 February 2021 at the inquiry into Cyber Security, and I am writing to correct answers that I provided regarding the status of customer notifications relating to the 2020 Service NSW cyber security incident.

Subsequent to the hearing, I have received further clarification regarding the status of these customer notifications, including the percentage of identified individuals affected by the incident for which a safe notification has been attempted and successfully received. For clarification and transparency, the status regarding notifications as at 22 March 2021 is as follows:

- Identified individuals impacted by the breach: approximately 103,000 (revised down from approximately 104,000 following the removal of a small number of duplicate records)
- Individuals for which sufficient information exists, including a name and valid address to attempt a safe notification via Australia Post person-to-person registered mail or via email to Service NSW employees who elected to receive the notification via email: approximately 67,000
- Individuals who have successfully received a safe notification via Australia Post person-to-person registered mail or via email: approximately 42,000
- Individuals for which the registered mail notification has been returned: approximately 18,500
- Individuals for which the registered mail notification is still in transit or awaiting collection with Australia Post: approximately 6,500

Service NSW has begun a final round of notifications for approximately 18,500 customers who haven't signed for their registered mail about the cyber attack on 47 staff email inboxes in 2020.

There are approximately 36,000 individuals (of the approximately 103,000 identified) where insufficient information is available to attempt a safe notification via Australia Post person-to-person registered mail. The risk to these individuals is considered lower based on the limited amount of data about the individuals that was able to be extracted from the email accounts that were compromised in the cyber incident. Importantly, there is no NSW Drivers Licence or Tax File Number (TFN) information impact for these individuals. For this remaining group of customers:

- Service NSW is investigating alternate methods that may enable a safe notification to be effected for as many as possible.

- Service NSW has taken action on their behalf to reduce the risk through working with other government agencies including NSW Births, Deaths and Marriages, Services Australia and DFAT to have stronger security measures applied to the identity credentials compromised in the cyber incident.

Notifying as many customers as possible is a priority for Service NSW. We decided our notification methods carefully to minimise the risk of notifying the wrong person and to avoid copycat scams. We are consulting with experts including IDCARE on these options, as we have done throughout our response to the cyber incident.

I have also written in similar terms to the Acting Chair of the Portfolio Committee No.6 - Transport and Customer Service in relation to evidence I provided to Budget Estimates on 8 March 2021. Service NSW will also reflect this information in our responses to Questions on Notice taken during the hearing on 8 March, and in our responses to Supplementary Questions on Notice. Service NSW has also published an update on notification progress including the above information on our website at service.nsw.gov.au/privacy.

Please accept my apologies for this error. I would be grateful if my corrected response could be distributed to the Committee.

Kind regards

Damon Rees
Chief Executive Officer
Service NSW