HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON ECONOMICS

REVIEW OF THE FOUR MAJOR BANKS AND OTHER FINANCIAL INSTITUTIONS

Westpac

WBC89QW: **Consumer Data Right**
(a) How many customers have requested that their data be shared with accredited data recipients through the Consumer Data Right regime?
(b) How long, on average, does it take for the bank to transfer data to accredited data recipients after it has been requested by customers?
(c) What strategies or processes has the bank implemented to overcome the following challenges with Consumer Data Right:
(i) The critical challenge of low consumer trust in the Consumer Data Right system;
(ii) Managing consent; in particular, balancing the need for consumers to understand what they are consenting to without being deterred by excessively complex procedures; and
(iii) The risk of data breaches.

Answer:

(a) Approximately 700 (across Frollo and Regional Australia Bank) as at April 2021.

(b) Within seconds once the customer has authorised data sharing.

(c)

(i)   Our implementation of the Consumer Data Right, including in relation to managing consent, aligns with the CX standards as set by the Data Standards Body which have been formulated on the basis of optimal consumer processes. We have a consistent user experience and language which we believe is an important factor to gaining consumer acceptance. We also provide consumer-friendly information about Open Banking on our website about safety, security and the consumers' control over their data. Our public facing CDR policy provides information to consumers about how CDR data is managed as well as how they can make an inquiry or a complaint. This is designed to manage CDR data in an open and transparent way, and is important for earning and maintaining consumer acceptance.

(ii)   As per above response. Additionally, we also provide training and FAQs to our front-line staff to handle customer queries.

(iii) Westpac's open banking solution has been built in accordance with the CDR Rules and technical standards which include stringent and detailed security and privacy requirements that seek to minimise the risk of data breaches. These include requirements relating to authentication of data recipients and consumers, and data security requirements such as masking of sensitive fields.

Additionally, our solution is also integrated into Westpac's existing enterprise control environment which has extensive controls in place designed to mitigate the risk of data breaches including:
- Security experts embedded within our CDR project team who review and certify the security aspects of our solution;
- A framework to identify applicable enterprise controls for IT systems;
- Scheduled audit and reviews of our control design and operational effectiveness;
- 24/7 Security Operations Centre; and
- Application and infrastructure monitoring.