

HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON ECONOMICS

REVIEW OF AUSTRALIA'S FOUR MAJOR BANKS 2023

Commonwealth Bank of Australia (CBA)

CBA06QW:

Employment practices

c. Please provide a time series over the past 10 years:

i. total staff outsourced overseas.

ii. by function (e.g. call centres, back office data analysis, cyber security).

Answer:

The following table outlines the number of employees working at CBA India, a wholly owned subsidiary, for the 2021-22 and 2022-23 financial years.

Note this information was disclosed in our 2023 Annual Report.

	30 June 2022	30 Jun 2023
CBA India total headcount	2,854	4,721

HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON ECONOMICS

REVIEW OF AUSTRALIA'S FOUR MAJOR BANKS 2023

Commonwealth Bank of Australia (CBA)

CBA08QW: In April 2023 the Australian Competition and Consumer Commission (ACCC) called on businesses 'to be vigilant and implement effective monitoring and intervention processes to prevent scammers using their services and stop them when they do'.

- a. What has the bank done since April 2023 in response to the ACCC's calls?
- b. Do you think it is appropriate for AFCA to continue to say* banks do not have a duty to monitor transactions when the ACCC has called for action from key sectors like banks? *As outlined in an AFCA letter, dated 3 July 2023, related to a customer complaint about scam activity.

Answer: a. CBA invested around \$750 million in FY23 to help protect and defend our customers from cyber security threats, financial crime, and fraud and scams. In addition to significantly increasing operational capacity to protect and support scam victims, we have announced initiatives to better protect customers, including recent new announcements outlined below.

NameCheck

We introduced the account name technology, NameCheck in March. We intend to make this technology available to trusted organisations. From 31 March to 5 June 2023, NameCheck helped over 11,000 CBA customers by preventing \$11 million in mistaken payments.

CallerCheck

CallerCheck enables customers to confirm that CBA is genuinely contacting them. Customers are able to check in their banking app or online if a phone call underway is a genuine CBA call. Around 300,000 customers every month are using CallerCheck to confirm that the call they are receiving is genuinely from CBA.

Crypto limits

Cryptocurrency transfers are a preferred option for scammers. Once scam proceeds have been transferred to crypto, it is very difficult for banks to recover funds. Announced in June, we now decline or hold for 24 hours¹ certain payments to cryptocurrency exchanges. We have also introduced \$10,000 limits in a calendar month where we can identify the customer payments are to exchanges for cryptocurrency purchases.

Industry collaboration

CBA has worked with the Australian Banking Association to develop six industry initiatives to strengthen the industry against scams and identify opportunities to partner with digital platforms and telecommunications industry to strengthen industry against scams.

Partnerships with telcos

CBA also supports strong collaboration across industry sectors to tackle scams nationally. For illustration, we have partnered with Telstra to share information to help prevent scams by ingesting data from Telstra directly into our Fraud Decisioning Platform.

b. As mentioned in other responses to questions on notice, CBA invests heavily to help protect and defend our customers from cyber security threats, financial crime, and fraud and scams. We work with all ecosystem participants including the ACCC and AFCA to prevent, detect and respond to scams and continue to advocate for increased participation in initiatives such as the AFCX which would help to reduce the risks of scams across the ecosystem.

As the AFCA letter relates to a customer issue at a competitor bank, we do not have sufficient understanding of the circumstances surrounding the complaint to be able to comment.

HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON ECONOMICS

REVIEW OF AUSTRALIA'S FOUR MAJOR BANKS 2024

Commonwealth Bank of Australia (CBA)

QON30: Please provide for-publication data on the estimated number of mule accounts with your bank for the two most recent 12-month periods.

Answer: CBA provides mule account data noting important context.

Firstly, technologies used to detect mule accounts are not uniform across the industry, with varied sophistication and accuracy. CBA continues to invest in new technologies and enhance existing detection technologies for mule accounts.

Secondly, the definition of a mule account is likely to vary across financial institutions given the lack of a standardised taxonomy and consistent reporting methods in relation to fraud and scams. A standardised approach to defining mule accounts is essential for producing reliant and comparable industry data.

Data standards are particularly relevant when a diverse range of activities could be categorised as muling – a minority of which are customers intentionally committing criminal conduct, while the majority are unwitting mules who are themselves scam victims. These victim customers are deceived by the scammer into receiving and transferring funds (e.g. a romance scam or an employment scam). Victim customers are not exited from the bank, but rather given education and warnings about how to avoid being deceived by scammers in future.

Banks are currently working with Treasury and the National Anti-Scam Centre on scams typologies to ensure greater consistency and to better support reporting required by the Government's proposed Scams Prevention Framework Bill. This work will establish a consistent baseline for future reporting on scams.

In the last two financial years, CBA exited the following number of customers who we believed were complicit in the fraud or scam or alternatively were, in our opinion, aware that they were receiving the proceeds of a scam or fraud:

- In FY23, 3,309 customers were exited
- In FY24, 2,993 customers were exited.