House of Representatives Standing Committee on Economics Review of Australia's Four Major Banks

WPC04QW - Risk management

A. Please provide your most recent Prudential Standard CPS 220 Risk Management (CPS 220) report (even if redacted).

B. Which consultant undertook the majority of the work?

C. Please provide a high-level summary of the most recent assessment of key financial and non-financial risks, for example, as a traffic light indicating the importance/likelihood of risk and organisational preparedness.

Response

A. Our most recent CPS 220 report did not identify any new financial or non-financial risks, rather it assessed our risk management framework and its effectiveness in managing our key risks. These risks are outlined below.

B. Oliver Wyman

C. Westpac has 11 risk classes, these include:
   - Capital Adequacy
   - Funding and Liquidity
   - Credit
   - Market
   - Strategic
   - Risk Culture
   - Operational
   - Compliance and Conduct
   - Financial Crime
   - Cyber
   - Reputation and Sustainability

Each risk class is divided into risk appetite metrics that we use to track whether we are operating within appetite or not for each risk class. Each metric is assessed against our risk management framework and classified Green, Amber, or Red.

- Green: The relevant risk appetite metric is operating within risk appetite. Risk generated from the activity is appropriately managed and all relevant policies are adhered to.
- Amber: The relevant risk appetite metric is operating within risk appetite but requires action. Heightened monitoring required and the development of plan to reduce risk.
- Red: The relevant risk appetite metric is operating out of appetite and requires action. A plan is to be developed to reduce risk to be in appetite.

As at 31 August 2023, each of the risk classes outlined above were operating within our risk appetite.

WPC07QW - Fraudulent activities

A. How many scammers have been found to hold host accounts with your bank and its subsidiaries in the past 12 months?

B. When an account sends money to a new payee, does your bank check if that payee has ever received money from any other accounts? If not, why not?

Response

We have revised our response to this question from last year to ensure a like-for-like comparison with the banks that made their response public. Our response to this question and the more recent question posed by the Committee on scam accounts is below.

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

Response

Most illegitimate bank accounts start as genuine bank accounts making them difficult to detect. This includes legitimate business bank accounts with a registered ABN. Table 1 outlines the three main types of illegitimate use of bank accounts related to scams.

Table 1: Types of illegitimate bank accounts use to transfer scammed monies

Stolen IDs	Customer identification is fraudulently obtained enabling access to a bank account – for example, personal information is obtained following a cyber breach.
Sold IDs / bank accounts	Customer sells their ID and or their Australian bank account – for example, when a student visa period ends, and the person leaves Australia. A simple search of the words “Sell my ID” on the Meta platform shows the prevalence of this activity.
Those complicit in the scam	Customers may—either wittingly or unwittingly—help facilitate the movement of scammed funds through their account. For example, a romance scam victim who is tricked into facilitating money transfers.

Westpac has robust measures in place to detect illegitimate use of bank accounts, including through inbound transaction surveillance, interbank cooperation and onboarding controls such as facial biometrics. As a result of these measures, Westpac has seen a 31 per cent reduction in total inbound and attempted outbound movement of scammed funds*.

An overview of total estimated illegitimate use of bank accounts that have been “referred to exit” is outlined in Table 2 below. It’s important to note that not all illegitimate use of bank accounts will necessarily be referred for exit – for example, where a criminal has used a stolen ID, exiting the customer profile could negatively affect the genuine individual. Exiting decisions are also carried out in line with the bank’s broader regulatory requirements, such as those outlined under the Banking Code of Practice.

Table 2: Westpac total estimated illegitimate use of bank accounts related to scams

12-month period	Total exits recommended
FY24^	2,220
FY23^^	962

The increase in FY24 recommended exits can be attributed to:

- An uplift in illegitimate bank account detection capabilities, which means we are proactively detecting more. While this figure has grown, gross scammed funds and customer scam losses have both decreased by 31 per cent and 29 per cent respectively due to improved bank detection and prevention measures.

- Scammers are redirecting efforts to use Australian bank accounts to move funds since the introduction of blocks to certain digital currency exchanges. Prior to these blocks, cryptocurrency was the main exit point of choice for scams.

* % reduction in gross inbound payments and attempted outbound payments from 2023 to 2024
^ October 2023 – September 2024
^^ October 2022 – September 2023

WPC08QW - Fraudulent activities

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.

Response

A. In relation to scam control, since April 2023, Westpac has:
   - Increased the size of our scam control team.
   - Led the Australian market in blocking high risk crypto-currency exchanges, which has led to a correction in that industry and their scam controls.
   - Upgraded our fraud / scam system.
   - Joined the NASC in its fusion cells and the Optus lead call blocking initiative.
   - Expanded our inbound scam detection capabilities.
   - In March 2023, we launched Westpac Verify. However, since then we have committed to further enhancing the feature to bring forward the scam risk rating to when customers enter a new payee into their online or mobile banking for the first time, so they can determine if they want to proceed with a payment. We expect this to be in place in 2024.
   - Announced In App Dynamic Scam Questions and uplifts to Westpac Verify (both to be released in early 2024), which are significant market-leading scam mitigation initiatives.

B. Westpac not only monitors transactions, but intervenes, counsels, educates, and recalls funds for our customers. Westpac continues to prevent more scams than not, which can only be achieved through our 24/7, real time monitoring activities and in-depth customer conversations.

C. We note and support the Government's intention to apply a mandatory scams code to the banking, digital platforms, and telecommunication sectors.

Westpac has an internal scams framework in place that covers the circumstances in which a reimbursement may be payable.