

**From:**  
**Sent:**  
**To:**  
**Subject:**

**Follow Up Flag:**  
**Flag Status:**

**Categories:**



To the Committee Secretary

Thank you for the opportunity to respond to the *Inquiry into the financial services regulatory framework in relation to financial abuse*. On behalf of Bank of us I advise our response to the Committee as follows:

1. What specific policies, systems, processes, or other safeguards does your business have in place to identify, respond to and report suspected financial abuse occurring to your customers?

*As a subscriber to the Customer Owned Banking Code of Practice (COBCOP), we have adopted the COBCOP vulnerability provisions which specifically reference domestic violence, elder abuse and financial abuse. Bank of us has a number of processes and systems / safeguards in place to identify, respond to and report suspected financial abuse. This includes training in respect to Vulnerable Customers undertaken by all front-line employees at commencement of employment and annually thereafter.*

*Documented procedures include:*

- *A set of processes which includes information for our employees in respect to Vulnerable Customers & Elder Financial Abuse including:*
  - *Overview of Vulnerable Customers & Elder Financial Abuse*
  - *Warning Signs of Elder Financial Abuse*
  - *Assistance for Vulnerable Customers*
  - *Preventing Elder Financial Abuse*
  - *Reporting Financial Abuse*
  - *Understanding AFCA's Standards (for complaints involving Financial Elder Abuse)*
- *Red Flags*
- *Duty of Care with Large or Unusual Withdrawals & Transfers*
- *An activity within our Open Banking (Consumer Data Right) process to follow if a vulnerable person is concerned about data sharing, with the ability to load a vulnerable flag.*
- *Name Change Process (considers vulnerable people)*
- *Hardship Assistance (including how we manage customer complaints)*

*Our 24/7 transaction monitoring rule set includes rules specific to vulnerable customers e.g. aged-based alerts (e.g. over 50) for certain transactions.*

*We have very low external transfer limits on our Internet Banking Platform for first time payees, and customers have to pass strict verification processes over the phone to increase those limits. If they fail those requirements, they need to present in a person at a Branch to reset their phone identification and increase / change limits.*

*For customers visiting our branches, we have created a 'Scam awareness' bookmark. We've found this to be a useful tool in starting the conversation and gives the customer something tactile to take with them as a reminder.*

*We regularly communicate with our customers to educate them on ways of safer banking e.g. scam awareness, etc. via social media and our website. We also issue an annual Security Guidelines document to all customers as part of our 6 monthly statement run at the end of December each year.*

Our website has information available to assist customers with protecting their personal information and a dedicated Safe Banking page [Safe Banking | Bank of us](#) and our Internet Banking Landing page [Internet Banking \(bankofus.com.au\)](#) also has a warning about scams, prior to logging in.

2. What is the extent of suspected financial abuse identified by any such measures in place?

*Bank of us has had no recent (last 3 years) confirmed reports or instances of elder financial abuse. We have had a couple of instances where red flags have caused concern, and the customer has been privately questioned and offered advice and assistance but, in those instances, they have denied any financial abuse has occurred. In one instance, where a younger and aggressive unrelated male was accompanying an elderly female into our Branch when she was making regular cash withdrawals, a concern for welfare was raised with Tasmania Police, but we understand the customer refused to cooperate with them. That customer ceased banking with us shortly thereafter.*

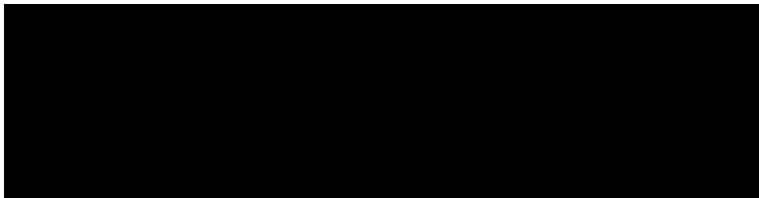
*We do occasionally see older people fall victim to investment, romance, remote access and phishing, vishing, smishing etc. scams but they are not unreasonably represented in the entire cohort of customers who fall victim to scams and card related fraud.*

3. What is the impact of the shift of financial products to online platforms on the prevalence of, and ability of your business to identify, respond to and report, suspected financial abuse?

*As detailed above, Bank of us has systems and processes in place to identify and respond to suspected instances of financial abuse and fraud, but we note it is becoming increasingly difficult to balance the rights of an individual to conduct their own business freely online without question and the underlying risk to the Bank if they do fall victim to financial abuse and red flags are missed. A potential consequence of increased regulation or liability shift etc. may see Banks review their risk appetite and reduce or restrict access and services available to customers online. This may negatively impact on vulnerable customers being able to access normal banking services remotely, including from the comfort of their own home.*

Kind regards,

Natasha Whish-Wilson



bankofus.com.au

1300 306 716



87 Brisbane Street, Launceston, 7250



This email may contain legally privileged and confidential information. If you are not the intended recipient, you must not disclose, transmit, copy, distribute or use the information contained in it. If you have received this email in error, please tell us immediately by return email and delete the document. B&E Ltd. does not represent or warrant that this communication or any attached file(s) is free from computer viruses or other faults or defects. B&E Ltd will not be liable to you or any other person for any loss or damage (including direct, consequential or economic loss or damage) however caused and whether by negligence or otherwise which may result directly or indirectly from the receipt or use of this communication or any files attached. It is the responsibility of any person using this communication or opening any files attached to this communication to scan those files for computer viruses. Bank of us is a trading name of B&E Ltd ABN 32 087 652 088 AFSL & Australian Credit Licence 236870

**From:** [Corporations.Joint@aph.gov.au](mailto:Corporations.Joint@aph.gov.au)