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?**

Our current framework for dealing with vulnerable members consists of a combination of transaction monitoring activity, detailed processes, training for frontline team members and leaders, clearly defined escalation points, external training for leaders, and an online form used for recording and reporting purposes.

Our processes are:

- We have specific processes outlined for both 'suspected' financial abuse and 'identified' financial abuse. A brief summary is provided below:

Suspected financial abuse:

- Identify possible warning signs/red flags
- Discuss the possible red flags with the member. For example, confirm if the member is aware of the specific transactions or make sure they have possession of any cards on their account that may have been used for suspect transactions. Example questions are provided for our people within the documented process.
- Where financial abuse is identified, our team will enact processes per 'identified financial abuse'.

Identified financial abuse:

- If this discussion identifies financial abuse, the team member that is supporting the member should take steps immediately. These can include restricting account access, changing access authorities, and cancelling cards linked to the account/s.
- Where further investigation or financial support is required, the initial point of referral/escalation is the staff members regional manager.
- In more severe or critical cases, further referral/escalation as required.
- Where any escalation is deemed appropriate, an internal webform is completed and a warm transfer is completed to minimise the need for the member to repeat their circumstances.
- When financial abuse is confirmed, referral is made to the (external) services listed on our website appropriate to the members situation.

Training for frontline team members and leaders:

- Training for vulnerable members covering these procedures was run in May 2024 and is now part of our BAU training for all member facing staff.
- Escalation points are clearly articulated for staff that consider the different types of vulnerability (transaction and savings accounts, lending, account restrictions, impairment and cognitive concerns, complex interactions).

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

Defence Bank have no recorded instances of financial abuse within our membership and therefore within defence communities this year.

We have had two recorded examples of suspected financial abuse in the past 12 months. In both instances these cases have been appropriately escalated and investigated - however conclusions

were reached that these did not constitute financial abuse. One of these instances was identified by transaction monitoring and the other by a frontline staff member.

Defence Bank has had one member claim financial abuse as part of a separation. This was addressed by the Collections Team Leader. As the financial abuse was not related to any Defence Bank accounts, the member was appropriately referred to external support services and an offer was made to support with any Defence Bank services.

The Department of Defence include financial abuse as a form of abuse in **Defence Strategy for Preventing and Responding to Family and Domestic Violence 2023–2028** which outlines key initiatives to address family and domestic violence within the **Australian Defence Force (ADF)** and are supportive of measures adopted to identify this within the Defence community and address it.

1) **An observation from our teams** – the prevalence of financial abuse by current members of the ADF may be less due to the relative comparable independence of many of our members and their partners/spouses due to the nature of their work. A central theme of financial abuse is control and access – and given the nature of defence employment – with regular military exercises, training and deployments, many members and spouses have a great need to operate with financial independence and autonomy. Due to the locations of most Defence Bank branches, we will primarily deal with the individual serving in the ADF. This can potentially result in a one-sided view of financial activity, making financial abuse less apparent and more difficult to identify.

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?

Defence Bank monitors transactions for multiple purposes including financial abuse and vulnerability. For example, Defence Bank has a rule that will identify multiple cash withdrawals over a brief period of time which can indicate when somebody has access to a Visa card. These "rules" are not unique to financial abuse but can often uncover red flags or suspicious behaviours. The fraud and AML team that do the monitoring are trained in what to look for and how to escalate/investigate appropriately where suspicions of financial abuse are present.

Defence Bank have had instances of suspected financial abuse based on this reporting which has triggered an investigation. After thorough investigations, no financial abuse has been uncovered.

Whilst the prevalence of online usage removes 'face to face' interactions with members and therefore a greater level of sophistication required to identify vulnerability, our current processes around online security was reviewed with no gaps in our online processes or services in relation to vulnerability identified. Where transaction monitoring alerts us to suspected vulnerability, this will trigger phone contact to the member to investigate by our trained team.