Australian Military Bank

03 July 2024

Committee Secretary
Parliamentary Joint Committee on Corporations and Financial Services
PO Box 6100
Parliament House
Canberra ACT 2600

Inquiry into the financial services regulatory framework in relation to financial abuse

Dear Committee Secretary,

Further to your email correspondence on 18 June 2024, please find attached our response to your questions regarding the upcoming “Inquiry into the financial services regulatory framework in relation to financial abuse”.

Should you have any questions in relation to our submission, please do not hesitate to contact me.

Kind regards,

Darlene Mattiske-Wood
Chief Executive Officer

Australian Military Bank

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?**

Australian Military Bank's (**AMB**) approach is governed by our Vulnerable Customer Policy and the Vulnerable Customer Framework, supplemented by targeted staff training through the e-learning training module "Protecting Vulnerable Customers". Additionally, our systems and procedures are designed to ensure thorough and prompt action in cases of suspected financial abuse.

AMB has implemented robust policies, comprehensive training, and detailed processes to identify, respond to, and report suspected financial abuse of customers. These measures help to ensure that vulnerable customers are protected and supported effectively, maintaining the integrity and trustworthiness of our services.

Policies and Frameworks

Vulnerable Customer Policy

The Vulnerable Customer Policy establishes the Bank's guidelines and policies concerning customer vulnerability. It aims to protect and support customers who may be at risk due to various vulnerabilities.

Vulnerable Customer Framework

The Vulnerable Customer Framework details the Bank's comprehensive approach to customer vulnerability, including:

- Identification: Procedures to identify customers experiencing vulnerability.
- Empowerment: Strategies to empower staff to adapt their services to meet the needs of vulnerable customers.
- Consideration: Integration of vulnerability considerations at all levels of the organisation.

Staff can access and refer to these documents on our internal intranet.

Staff Training

Annual Training Requirements

Staff are required to complete the "Protecting Vulnerable Customers" training. This mandatory annual training module educates staff on recognising and responding to financial vulnerability. It covers:

- Identification of various forms of vulnerability.
- Techniques to assist vulnerable customers and ensure they understand financial products.
- Recognition of improper manipulation and steps to take in such cases.
- Reduced decision-making capacity.
- Special needs.
- Vulnerability to other parties.
- Relationship breakdowns and domestic violence.
- Elder financial abuse.

Effective Questioning and Escalation

Staff are trained to use effective questioning to detect potential financial abuse. If suspected, the case is escalated to the Bank's specialist member advocate team, and a UAR (Unusual Activity Report) is raised in our reporting system (**Triline**).

Observational and Interaction Protocols

Transaction Monitoring

Staff are trained to observe suspicious transactions, transfers, payments, or withdrawals, and to recognise physical and behavioural cues that may indicate financial abuse.

Authorisation Verification

Staff review the Banking system to verify authorisation to act on behalf of the customer, treating authorised individuals as account owners when interacting with them.

Seeking Guidance

If uncertain, staff are encouraged to seek a second opinion from a colleague or supervisor before proceeding with any action.

Collaboration and Additional Measures

Coordination with Financial Crime and Fraud (**FCF**) Team

Staff work closely with the FCF team to address and mitigate risks of financial abuse.

In-Branch Protocols

In cases where the member and potential abuser are present in the branch, staff are trained to separate them and speak privately with the account holder.

Periodic Updates

Periodic updates ensure frontline staff are updated on procedures and necessary actions.

Account Freezing

Staff can freeze accounts suspected of being misused to provide time for further investigation and support for the customer.

Financial Literacy and Coaching

Promoting financial literacy helps members recognise and address discrepancies in their banking activities. We have a launched educational material on our website earlier this year. While not formalise yet, our frontline staff engage with and coach members on safe banking practices.

Third-Party Support

For additional support, staff can refer cases to the Elder Abuse Hotline (1800 353 374) or recommend family members call 1800Respect (1800 737 732). We also provide links to a number of third party support services on our website.

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

The measures and safeguards implemented by our business, combined with the unique support structures and secure environments provided by institutions like the Australian Defence Force (**ADF**), have resulted in a very low incidence of suspected financial abuse. The existing policies, training programs, and reporting protocols effectively support the identification and response to any potential issues, ensuring that vulnerable customers are protected.

Overall, while financial abuse is a critical concern, the data suggests that our proactive measures and vigilant reporting processes are successful in maintaining a secure and supportive environment for our customers.

Observations and Trends

- Rarely Reported: Instances of suspected financial abuse are rarely reported to us.
- Reporting Protocols: When issues are identified, they are promptly reported by team members to the member advocate team and recorded in Triline. Using Triline, we can monitor trends over time.
- Secure Environment: Physical access to ADF bases is highly secure, requiring families to be escorted onto bases so we do not always interact with both parties.
- Power of Attorney (POA): A large number of ADF members have POAs due to the nature of their roles and the possibility of extended deployments. We have not had any mistreatment of POAs reported.

Australian Military Bank

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?

The shift to online financial products introduces new challenges in identifying and responding to financial abuse. However, our implementation of Consumer Data Right (**CDR**) Rules, advanced fraud monitoring tools, and robust internal processes provide a strong foundation for managing these risks. Continuous improvement in financial literacy education and enhanced detection systems will further support our efforts to protect vulnerable customers in the evolving digital landscape.

CDR Rules and Data Sharing Provisions
The CDR Rules include provisions allowing data holders, such as AMB, to refrain from complying with certain rules when it is necessary to prevent physical, psychological, or financial harm or abuse to customers.

- CDR Rule Implementation: Within our Finacle system, staff can activate a flag to prevent data sharing through CDR if there is a risk of harm or abuse. This proactive measure helps protect vulnerable customers from potential misuse of their data.

Monitoring and Fraud Detection
Fraud Monitoring Tools: These include real-time monitoring and behaviour tracking, which can identify suspicious activities and anomalies in member accounts, aiding in the detection of financial abuse.

Challenges in Online Platforms
The shift to online financial platforms presents several challenges in identifying and responding to financial abuse due to the personal and potentially subversive nature of the abuse.

- Personal Devices: Financial abuse can occur through personal devices, often password-protected, making it difficult for the bank to detect. Examples include excessive requests for funds, threatening texts, small denomination transfers, monitoring spending history through shared banking access, and changing passwords to deny access.
- Embarrassment and Isolation: Victims may feel embarrassed and reluctant to report abuse, creating a cycle of silence and continued abuse. The hidden nature of online abuse makes it harder for bank staff to identify without explicit reports from the victims.

Internal Processes and Capabilities
Despite these challenges, our FCF team has a focused and thorough process to identify issues within accounts.

- Collaboration with Frontline Staff: When appropriate, the FCF team shares findings with frontline staff to help manage the customer's situation effectively.
- Financial Literacy: Emphasis on financial literacy and self-protection on online platforms, including guidance on avoiding scams and the importance of security measures such as not sharing passwords or PINs.

Reporting and Trend Analysis
Our reporting capabilities are robust, supported by systems and processes designed to track and analyse incidents of financial abuse.

- Suspicious Matter Reports (SMRs): We have strong capabilities in handling SMRs and the associated processes.
- Triline Reporting: Utilised for reporting UAR, Triline helps in organisational trend analysis, providing collective reports to understand and address emerging issues.