

4 September 2024

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


47 Burelli Street
Wollongong NSW
2500
PO Box 2077
Wollongong NSW
2500
133 462
imb.com.au

By email only: corporations.joint@aph.gov.au; seniorclerk.committees.sen@aph.gov.au

To the Committee,

**Parliamentary Joint Committee on Corporations and Financial Services (the Committee)
Inquiry into the financial services regulatory framework in relation to financial abuse (the Inquiry)**

We refer to the Committee's request for a response to three questions, received by IMB Ltd trading as IMB Bank (**IMB**) via email on 18 June 2024 (**Request**) and IMB's response dated 3 July 2024.

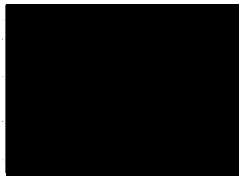
IMB is a mutual bank with its head office located in Wollongong, NSW. IMB has been in continuous operation for 144 years and was originally formed in 1880 as Illawarra Mutual Building Society. IMB is a mutual organisation, owned by its members. IMB strives to provide banking that makes its members and communities better off. This commitment extends to supporting the financial safety and security of IMB's members and taking a firm stand against financial abuse.

IMB currently has approximately 219,000 customers (known as its members) and operates a total of 52 retail bank branches across Australia, 51 of which are in NSW and the ACT and one in Victoria. IMB employs approximately 622 employees, representing approximately 520 FTE.

IMB refers the Committee to **Attachment A**, being IMB's response to the Request provided by IMB to the Committee on 3 July 2024, with certain data points removed for publication purposes.

Please contact Lauren Wise, General Manager, Corporate Services / Company Secretary on [REDACTED] or [REDACTED] if the Committee requires further information.

Yours sincerely



Robert Ryan
Chief Executive

ATTACHMENT A

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

In this attachment:

- “Account Holder” means the member who owns the account in question;
- “ATO” means an individual appointed by an Account Holder as an ‘Authority to Operate’ on their account;
- “Attorney” means an attorney appointed under a Power of Attorney document by a relevant Account Holder;
- “Customer Service Staff” means IMB’s customer facing staff, such as bank tellers, bank managers and call centre operators, and collections and hardship personnel, as relevant;
- “IMB” means IMB Ltd trading as IMB Bank; and
- “Member” means an IMB member/customer.

Question	Response
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?	<p>IMB is committed to supporting its Members’ financial safety by providing information to Members regarding safe banking practises, the warning signs of financial abuse and how IMB may be able to help. Customer Service Staff have traditionally played a crucial role in identifying indicators of financial abuse and taking action in a timely and sensitive manner, to reduce the likelihood of financial abuse from occurring. IMB ensures that its Customer Service Staff receive regular and focussed training regarding financial abuse and the tools available to them, to support IMB’s Members.</p> <p>IMB maintains a financial abuse prevention framework (Framework) which includes:</p> <ul style="list-style-type: none"> • a focussed financial abuse training module, which is completed by Customer Service Staff and others annually; • procedures and fact sheets for IMB’s Customer Service Staff, which include detail regarding the warning signs of financial abuse and how to detect them, and what steps should be taken to respond and reduce the risk of financial abuse occurring (for example, not actioning transactions and escalating concerns to management or IMB’s Legal and Compliance department for advice); • a process by which all powers of attorney and financial management orders are subject to a centralised compliance review by Legal & Compliance before IMB will act upon instructions purported to be given under the authority of such documents;

- a financial abuse webpage and brochure for Members which is available in IMB's branches;
- Procedures and a potential financial abuse matter register maintained by IMB's Legal and Compliance department, to record concerns of financial abuse which are escalated to it;
- terms and conditions within IMB's PDS, relating to suspected financial abuse and steps available to IMB should it detect suspected matters of financial abuse;
- in person domestic and family violence training, which is completed by Collections and Hardship staff;
- large payment procedures and daily transaction limit increase processes which require a higher level of scrutiny over certain transaction before they are processed;
- transaction monitoring and security controls, utilised to manage the overall risk of financial crime;
- procedural safeguards for guarantors and a Legal & Compliance review process for powers of attorney documents proposed to be used in lending transactions; and
- support measures to support IMB employees who may be affected by family and domestic violence, often involving financial abuse.

As listed above, IMB took proactive steps to update the terms and conditions contained in our PDS, to explicitly address suspected financial abuse and ensure IMB is better equipped to intervene in situations where a Member may be experiencing financial abuse. Part 3.3.3 of IMB's PDS, enables IMB to take action, such as suspending the authority of an Attorney or an ATO on an account, including any facilities, in circumstances where IMB has *"...reasonable grounds to believe there is a fraud or financial abuse risk associated with the continued use of [the] Account"*.

Financial abuse can also be considered alongside other risks that are managed, such as those associated with credit risk and fraud and scams, when developing transaction monitoring and controls that are applicable to the preventing and detecting those kinds of financial crime. IMB notes the following initiatives / enhancements which are underway or being considered in this regard:

- IMB has a transaction monitoring program established for broader fraud and financial crime prevention. Through this program IMB can identify payments that are not within a Member's normal pattern of behaviour or are not being performed using the Members' usual device. IMB then has investigation methods and intervention tools to either reverse, restrict a payment or to investigate the legitimacy of that payment further; and
- IMB is in the process of implementing new rulesets within its financial crime monitoring systems that focus on payment descriptions with abusive, coercive, or threatening language.

	<p>As noted above IMB also has a range of support measures in place to support our employees who may be affected by family and domestic violence, as follows:</p> <ul style="list-style-type: none"> • Family and Domestic Violence Leave Policy which provides employees with a range of financial and non-financial support measures; • Employee Assistance Program with 24 x 7 access to a range of immediate and confidential support services; • ten days per year of paid leave for all IMB employees dealing with family and domestic violence; • additional support deemed appropriate to the circumstances, including financial and non-financial measures such as further unpaid leave, flexible work arrangements, accommodation and relocation support, and technology support to manage external communications; and • leadership development and training to enable our leaders to support their teams with first responder care. <p>IMB's Framework is consistently reviewed and improved as and when IMB identifies further opportunities to support its Members or better enable our staff to manage cases of suspected financial abuse. A recent example was IMB's implementation of a 'quick exit' button on a relevant IMB webpage, to be utilised by victims as needed. IMB is also engaged in discussions with its mutual peers as to how we can continue to enhance the tools available to staff to combat financial abuse.</p>
<p>2 What is the extent of suspected financial abuse identified by any such measures in place?</p>	<p>IMB has previously provided detail to the Committee regarding:</p> <ul style="list-style-type: none"> • the number of suspected financial abuse matters escalated by Customer Service Staff to IMB's Legal and Compliance department for advice in the previous 12 month period; • the number of hardship matters which included known financial abuse risks in the previous 10 month period. <p>Periodically IMB's Fraud Operations team receives reports of "unauthorised" card or online banking transactions which were performed using correct passwords, PINs and secure authentication codes and which after investigation appear to be performed by parties well-known to the relevant Account Holder. In some of these cases, there is the potential that some form of financial abuse has occurred.</p> <p>IMB has also previously provided the Committee with detail regarding the number of complaints that were received by IMB in the previous 12 month period, relating to steps taken by it in response to suspected financial abuse matters. These included complaints in relation to IMB:</p> <ul style="list-style-type: none"> • placing restrictions on the relevant account due to unusual activity or suspected financial abuse; • declining a Power of Attorney document; • declining to process a transaction due to suspected financial abuse; and • declining to honour a cheque made payable to and signed by the Attorney.

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 increasing shift of financial products to online platforms has included the following impacts on the prevalence of, and ability of IMB to identify, respond to and report suspected financial abuse matters:

- the ability of Members to access a wide range of products and services online, often without the need for any assistance from a bank staff member ('customer self-serve'), makes it much easier for perpetrators of financial abuse to access and control a victim's accounts, for example via unauthorised transactions and the use of victim login details to monitor accounts. The 24 x 7 nature of digital banking and the speed of real-time payments makes it more challenging for IMB to intervene prior to an act of financial abuse occurring in relation to certain transactions;
- IMB has historically been most successful in identifying and managing financial abuse through face-to-face interactions with our Members. In this changed environment, systems and technology have and will continue to become more critical in detecting and preventing financial abuse. This requires ongoing investment and continuous improvement in our banking and payments systems and training of our teams responsible for transaction monitoring. Teams need to be alert to the way in which financial abuse risks can be detected in a digital banking context, at a time where there is an increasing volume of broader fraud and scam risk activity that also requires management through these systems;
- more varied (and more difficult to manage) forms of financial abuse, including written abuse from perpetrators to victims in form of electronic payments descriptions; and
- consideration of potential financial abuse can involve longer timeframes to investigate and resolve. It can be challenging to strike a balance between preventing further financial abuse when a suspicion has been formed (for example by restricting account access or transactions while an investigation is pursued) and putting into place undesirable obstacles for already vulnerable Members.