People First Bank

Committee Secretary
Parliamentary Joint Committee on Corporations and Financial Services
PO Box 6100
Parliament House
Canberra ACT 2600
Sent via corporations.joint@aph.gov.au

2 July 2024

Inquiry into the financial services regulatory framework in relation to financial abuse
Response to the Committee's request for information on 18 June 2024

About People First Bank

People First Bank is a leading Australian customer-owned banking organisation, formed through the merger of Heritage Bank and People's Choice Credit Union in in March 2023. This has created a new national mutual bank with approximately $24.5 billion in assets and 2,000 employees supporting more than 740,000 members.

Our origins date back to 1875, making us one of Australia's longest-running financial institutions. We maintain a strong connection to regional communities with dual head offices in Toowoomba and Adelaide.

While we continue to operate under the Heritage Bank and People's Choice brands for an interim period, we have begun rolling out our new People First Bank brand this year.

As a member of the Customer Owned Banking Organisation, we support COBA's submission to this Inquiry.

The following responses reflect practices across our organisation.

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 customer-owned banking organisation, People First Bank is committed to serving the interests of its members.

In today's banking environment, we have recognised an increasing need to protect our customers against the threat of financial abuse. As a result, we have in place a comprehensive customer vulnerability model to identify, manage and report cases of financial abuse.

This includes:

- A centralised Customer Care & Wellbeing portal, accessible by all employees, which contains all information and procedures to help identify and respond to potential cases of financial abuse.

- Compulsory training for all customer-facing employees including call centre teams on how to identify vulnerability (including instances of financial abuse) through our service standard framework of 'transacting with reasonable care and skill'. This involves making reasonable enquiries on every occasion, especially when instructed by a third party.
- Limitations built into our systems and processes when a Power of Attorney is involved which require additional steps and checks that help minimise the potential for abuse.
- Additional monitoring through other regulatory requirements such as AML/CTF and fraud alerts. This can potentially alert us to a precursor to abuse through initial changes in banking behaviour on the account.
- Escalation processes to ensure that complex cases of suspected financial abuse are escalated to our dedicated team of Customer Care specialists, who have specific expertise in managing cases of financial abuse.
- Record-keeping processes to note, for example, what support a customer needs in response to the vulnerability being experienced, what has been put in place to reduce harm and what is important to not cause harm.
- Collaboration with external organisations who specialise in financial abuse, such as TASC (a Queensland-based legal and social justice service).

Our reporting measures include:

- Internal quantitative and qualitative reporting on complex cases that are escalated to our Customer Care & Wellbeing team. This is overseen by the Chief Member Officer and published in her weekly report.
- External reporting, where appropriate. This includes the referral of certain matters to the police, referral to governing bodies (e.g. Adult Safeguarding units) and/or mandatory reporting to state-based authorities in those states where mandatory reporting is in place. It is important to recognise that banks face numerous challenges when escalating individual cases to external authorities. This includes consideration of whether reporting will aggravate the circumstances or cause further harm to customers who are experiencing vulnerability.

People First Bank subscribes to the Customer Owned Banking Code of Practice (COBCOP) and we hold ourselves accountable to these standards.

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

In the 2023-24 financial year, 299 suspected cases of financial abuse were escalated to our Customer Care & Wellbeing team. Attempting to quantify the extent of financial abuse by number of cases or dollar amount is difficult and, in isolation, can have limited impact on addressing the issue. Therefore, we have examined the cases of financial abuse that our measures have identified, to ascertain the most common circumstance in which it occurs.

The most common circumstances that can lead to financial abuse are as follows:

- Situations where there is an Authorised Signatory to an account, including where a parent or guardian can act on a child's account.

- Situations where someone has been given General or Enduring Power of Attorney to act on a customer's account.
- To a lesser extent, situations where there is a court-appointed administrator. There are often measures put in place by the appropriate court to manage these relationships.
- Third-party influence (coercive control) by a friend or family member, often where coercion occurs due to a customer's impaired capacity or exploitation of their kind nature.
- Third-party influence by a total stranger – financial abuse linked to romance/relationship scams where customers are coerced into transactions.

These circumstances create the environment in which financial abuse is more likely to occur, with common issues including the following:

- A sense of entitlement from third parties who have control over a customer's account. This includes circumstances where a son or daughter has control over a parent's accounts; or alternatively a third party acting on behalf of a child who may receive a large settlement. This kind of abuse is justified by the rationale that "it is really mine anyway" so "I can do as I like".
- Inheritance impatience – a third party taking funds before a customer passes away to circumvent probate timeframes or costs.
- When a third party is assigned a Power of Attorney, they often receive legal advice about their entitlements which fails to take into account their fiduciary responsibility and banks' fiduciary responsibility to act in their customers' best interests.
- Legally-appointed decision-makers using customers' diminished capacity to misuse their consent to instruct.
- Legally-appointed decision-makers blocking banks from contacting customers to confirm transactions, when no evidence exists of any lack or impaired capacity. This includes decision-makers hiding the fact that the customer may have passed away to access funds prior to probate.
- Customers aware that they are experiencing duress or coercive control but hiding the control and abuse from the bank. This is often seen in matters of family and domestic violence, or due to the blur between romance/relationship scams. This makes it difficult to identify that financial abuse is happening.
- Weaponising banking services platforms such as fast payments to send threatening and controlling messages.
- Lack of financial literacy, which may be due to cultural background, illness, disability, lack of language skills or other factors.
- On joint accounts, one party may use allegations of family or domestic violence to discourage the bank from checking with the other party about whether transactions are legitimate.
- We are increasingly seeing instances of financial abuse where there is aggressive behaviour from legally-appointed decision-makers. We can apply precautionary measures to an account to try to prevent the financial abuse. However, this often means our customer-facing staff having to interact regularly with the individual who has displayed aggressive and/or inappropriate behaviour. This can be extremely challenging long term and affect employee wellbeing.

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?

While banks have traditionally relied heavily on personal interactions with customers and authorised parties to identify cases of financial abuse, as an industry we need to invest more in technology and tools to support the shift to online platforms.

Examples in place at People First Bank include:

- Transaction monitoring for fraud, scams and AML/CTF, with processes to apply precautionary measures and escalate to the Customer Care & Wellbeing team for review and management.
- Participants in the New Payments Platform, including People First Bank, use an alert system where financial institutions can identify when the platform has been weaponised to send threatening or controlling messages to customers.

Some existing activities around scam and fraud prevention align with this. In principle, our behavioural analysis of financial abuse cases could be applied in a similar way as scam and fraud metrics to help identify and prevent financial abuse. However, with limited resources compared to the major banks, this is one of many areas competing for investment.

Banks often rely on manual processes to manage complex cases of financial abuse. This may include talking to customers directly, removing online/card access to reduce the risk of unauthorised transactions, or requiring an authorised party to provide documentation showing that funds are being used for a customer's benefit.

Automated processes designed to identify potential cases of financial abuse in an online environment may activate precautionary measures such as freezing an account or limiting access as the primary way to prevent the abuse. These measures should be used as a last resort only, as they may unintentionally create adverse effects for people experiencing vulnerability by stopping them accessing their funds to use for legitimate reasons.