Date	10 September 2024
To	**Senate Corporations and Financial Services Committee**
From	Ross Kearney, Chief Risk Officer
RE	**Inquiry into the financial services regulatory framework in relation to financial abuse**

Introduction

BankWAW is a small community owner bank that operates in Northeastern Victoria and in a small section of Southern NSW. There are approximately 25,000.00 customers serviced by 13 branches as well as a range of digital banking solutions - internet banking, mobile banking, phone banking, visa debit cards with tap and online functionality, real time payment, direct entry payment, mobile wallet pays and international funds transfers via Convera.

The average customer age is 50 years with a large customer cohort who rely on branch support for their banking arrangements. This cohort have a number who struggle to use digital banking solutions and have little understanding of how those solutions provide access to their bank accounts.

Financial abuse is a type of fraud that can be very hard to detect because of the way it is most likely to occur; that is a person close to the customer obtains or is given access to the customer's account and uses the customer's funds for their own benefit. A customer with a form of impairment is particularly vulnerable to financial abuse as they may be reliant upon the abuser for support and may not be able to identify that abuse is occurring or are even willing to ignore the abuse.

BankWAW has been supporting their customers for well over fifty years and has never deviated from providing services that are in the best interests of the customer. This a commitment that is embedded in Bank WAW's procedures and practices.

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?

Over many years BankWAW has developed and implemented a ranged of practices to protect customers from financial abuse. These practices are supported by the following procedural arrangements:

- Customer Owned Banking Code of Practice - commitment to addressing financial abuse.
- Operations Procedures that guide:
    - Managing accounts operated by Powers of Attorney and Authority to Operate.
    - Customer management in the branch where a third party is present and seeks to assist with the customers banking.
    - Profiling customer spending patterns, linked to know your customers processes and online monitoring by fraud detection systems.
- Online Financial Abuse training completed staff on an annual basis.

- Weekly in house training for all branch staff that has financial crime as a standing agenda topic,
- Customer onboarding procedures that establish a 'know your customer' baseline which is then maintained by a process known as 'ongoing customer due diligence'. Onboarding can be commenced online but cannot completed without branch attendance.
- 24/7 transaction monitoring systems for card and online transactions.
- The WAW Compliance Team monitors and generates customer verification reports that identify changes to in customer risk profiles and product usage.
- Community education programs
    - Delivered by staff directly to customer in branches.
    - Delivered at community forums at regional centres by WAW staff.
    - Newsletters to customers, information in social media and on the WAW website
- WAW maintaining comprehensive Fraud and Dispute Registers that track the management of fraud events by WAW.

WAW also supports the 10 recommendations made by Customer Owned Banking Association to this Inquiry and will seek to improve WAW processes in response to those recommendation.

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

WAW can generally identify when customers are suffering suspected financial if those customers have direct contact, either over the phone or in the branch.

The 'know your customer' processes and the training equip staff with the capacity to identify suspected financial abuse. When this identification is made, the issue is immediately escalated to more senior staff for their input as to how the issue should be managed. There are a set to protocols to be followed but each issue needs to be assessed so that the individual circumstances of the customer are addressed as far as possible.

Large value funds transfers are quickly identified via the 24/7 transaction monitoring systems. Contact is always made with the customer to check if the payment is authorised. The system will allow payments to be held or blocked to give WAW staff time to verify if the payment is authentic.

Suspected financial abuse is very hard to detect when the abuser adopts a 'fly below the radio' approach with the transaction patterns. This can involve payment of utility, grocery bills or some other payment that is consistent with the payment type that the account holder may make. In those circumstances WAW is significantly reliant on information receiving information from the customer or a third party about any changes being made to their payment arrangements.

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?

A discussion about the impact of payment arrangements that do not involve branch contact must involve the operation of the visa debit card. The card operates in a variety way that make financial abuse easy to perform and hard to detect. Even without the card PIN being stolen or provided the tap function will allow a maximum of $500.00 a day to be spent by another party in possession for the card.

The card with the PIN can be used for ATM and cash-out withdrawals. The card can also be used to make online purchases. The WAW monitoring system will detect some of these transactions but if the abuser is careful with payment type and size, it may be very hard to detect payment anomalies.

WAW does offer a service whereby the functionality of the cards is reduced in accordance customer requirements. This can involve for example the removal of the tap function or online purchasing. As customers often transition into a state of vulnerability WAW is not always on notice that extra vigilance is needed with the customer's account.

The system monitoring systems will detect large value transactions which may occur if a customer is the victim of a fraud. Online funds transfers do have second factor protections for new payees but the financial abuser that has gained access to bank details and devices may be able to circumvent the protections.

As noted above, WAW's systems can put friction into the payment processes by holding transactions until they are verified but this is not always a popular course. Customers now expect fast, efficient and comprehensive banking services but there is an inherent conflict with this expectation when banks adopt processes that will slow down payment services. The regulators are not clear about what their expectations regarding the services and protections provided by banks. The industry and regulators are working closely to develop a Scams Accord to implement processes to protect customers from fraudsters. At the same time the finance sector at the direction of the ACCC, is implementing a Consumer Data Rights system that will allow third parties access to a customer's banking information. This is a complex online environment. The dangers associated with the release of the customer banking information via this environment is not being discussed by the regulators nor are there discussions about processes that will provide customers with protections.

Conclusion

WAW is acutely aware of the harm and distress to customers who are the victims of financial abuse. These customers are quite often the least likely to be able to recover from the financial losses suffered which leaves them in a state despair.

As a community owned and regionally based bank, with all staff living in the local community, WAW has a very strong commitment to protecting customers. Notwithstanding this commitment the transaction channels provided in the modern banking environment make it impossible to detect all financial abuse. The key protections being deployed by WAW are transaction monitoring systems and a range of practices and procedures that focus on ensuing that the banking services provided are in the customer's best interest.