Vulnerability

Inquiry into how Code subscribers approach vulnerability and deal with issues concerning domestic and family violence and elder abuse.

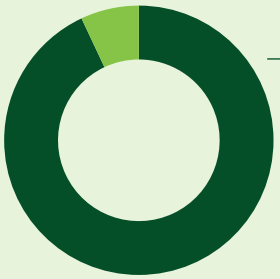
June 2022

CUSTOMER OWNED BANKING
CODE COMPLIANCE COMMITTEE

Contents

1 IN 5 SUBSCRIBERS HAVE A DEDICATED TEAM OR STAFF MEMBER TO MANAGE VULNERABILITY

95% SUBSCRIBERS PROVIDE, OR ARE PLANNING TO PROVIDE VULNERABILITY TRAINING PROGRAMS



93% subscribers rely on appropriately trained frontline staff to detect vulnerability in a customer

60% subscribers said customers self-report as vulnerable

60% SUBSCRIBERS HAVE A POLICY THAT ADDRESSES VULNERABILITY FOR CUSTOMERS WHO ARE VICTIMS OF DOMESTIC/FAMILY VIOLENCE

16% SUBSCRIBERS SAID THAT THESE POLICIES WERE SOLEY DEDICATED TO THE MANAGEMENT OF VULNERABLE CUSTOMERS

1 IN 4 SUBSCRIBERS REPORT VULNERABILITY MATTERS TO THEIR BOARD/EXECUTIVE COMMITTEE

LESS THAN HALF USE DATA ANALYTICS TO IDENTIFY VULNERABLE CUSTOMERS

FEWER THAN ONE-THIRD OF SUBSCRIBERS HAVE PARTNERED WITH A COMMUNITY ORGANISATION THAT SPECIALISES IN HELPING VULNERABLE PEOPLE

Executive summary

The treatment of customers experiencing vulnerability by financial services institutions and other service providers has been a growing focus of regulators and consumer advocacy groups in the last few years. This has now been reinforced by the publication of a new international standard on consumer vulnerability, ISO 22458.

In updating the Customer Owned Banking Code of Practice (the Code), the Customer Owned Banking Association (COBA) has included specific obligations for the treatment of different types of vulnerability that may be experienced by customers. The new Code comes into effect on 31 October 2022 and will replace the 2018 Code, which does not specifically refer to vulnerability.

Recognising that many Code subscribers have been working for some time to improve the way they identify and respond to customers experiencing vulnerability, the Customer Owned Banking Code Compliance Committee (the Committee) conducted this Own Motion Inquiry to understand how subscribers define vulnerability and deal with issues concerning domestic/family violence and elder abuse. We also wanted to find out how mature subscribers' vulnerability frameworks are as they prepare to meet their compliance obligations under the 2022 Code and identify areas where further work may be required.

This report describes the findings of the Inquiry. It provides case studies from different subscribers on how they manage customers experiencing different types of vulnerability, and a list of further reading resources for Code-subscribing institutions to consider.

Overview of findings[1]

Many subscribers have established vulnerability frameworks, but further work will be needed to comply with the new Code

Many subscribers report they have well-established frameworks for addressing vulnerability, even though the 2018 Code does not explicitly mention vulnerability. At their most sophisticated, these frameworks include rigorous policies, processes and training programs based on a clear definition of vulnerability, and effective use of internal resources where different business units (from customer service to financial crime, credit control, and risk and compliance) share intelligence to help identify and manage customers experiencing or potentially experiencing vulnerability.

Nevertheless, as the provisions relating to vulnerability in the 2022 Code are significantly more detailed and comprehensive than the 2018 Code, even subscribers with more substantial vulnerability frameworks likely have more work to do to ensure they comply with the new Code. The Committee encourages all institutions to evaluate their existing approach to managing vulnerability against each of the new Code's vulnerability obligations.

[1] The Own Motion Inquiry was conducted as part of the 2021 Annual Compliance Statement. All findings in this report should therefore be read in the context of subscribers' compliance with the 2018 Code.

Many subscribers report they prioritise customers who are experiencing elder abuse

Code subscribers told us protecting elderly customers experiencing vulnerability from financial abuse and/or domestic/family violence is a key priority. Many gave examples of having managed actual and suspected cases of elder abuse in customers when explaining how they define, identify, and respond to various types of vulnerability. Additionally, almost two-thirds of subscribers reported having a policy to address customers experiencing elder abuse, and almost all say they have a policy relating to Powers of Attorney.

Most subscribers provided very little explanation for how they identify and respond to customers experiencing domestic/family violence

While 60% of subscribers reported they have a policy relating to customers experiencing vulnerability who are victims of domestic/family violence, only 16% of subscribers said this was a standalone policy relating solely to the management of customers experiencing domestic/family violence (and/or elder abuse). Subscribers provided very little detail about the nature of these policies and few real-life examples to demonstrate how they are put into practice.

Similarly, few subscribers referenced addressing domestic/family violence when discussing their approach to training staff to identify and respond to customers in this situation, although there were a handful of good examples. Given the 2022 Code states subscribers' training "will include awareness of vulnerable circumstances because of domestic violence and elder abuse", the Committee expects this to be an area of focus for all subscribers as they transition to the new Code.

Very few subscribers have policies and processes covering each of the vulnerable circumstances outlined in the 2022 Code

At the time of responding to the inquiry, fewer than half of all subscribers confirmed they have vulnerability policies or processes relating to mental health, physical disability, serious illness, First Nations Peoples, customers who are unfamiliar with banking products and financial services, or working with financial counsellors, community representatives and/or other specialists.

These vulnerability examples are specifically referenced in the 2022 Code and subscribers need to be able to demonstrate they can identify and respond to customers experiencing these types of vulnerability – as well as others not explicitly listed – to be compliant with the new Code when it comes into effect at the end of October 2022.

Subscribers rely heavily on frontline staff to identify vulnerability, but most provide their staff with specialised training

Almost all subscribers reported they rely on interactions between staff and customers to identify when a customer is experiencing vulnerability. Ninety-three per cent said they rely on appropriately trained frontline staff to detect a customer experiencing vulnerability by observing and talking to them, while 60% said customers sometimes self-report as vulnerable. Less than half use data analytics (transaction monitoring, loan applications, suspicious matter reports, etc.) to identify customers experiencing vulnerability.

Given the reliance on frontline staff to recognise and assist customers experiencing vulnerability, the Committee was pleased to note that 95% of subscribers reported they provide, or are planning to provide, comprehensive training programs that cover a range of customer types experiencing vulnerability.

Subscribers say they have robust policies and processes for managing Powers of Attorney

All but two Code subscribers reported having documented policies and processes in place to protect customers experiencing vulnerability with a Power of Attorney (POA) from financial abuse. Many described comprehensive staff training programs for accepting, verifying and managing POAs.

One in four subscribers report vulnerability matters to their Board/executive committee but the focus is usually on the financial impacts

Smaller and mid-sized institutions are more likely to inform their Board about matters regarding customers experiencing vulnerability. Larger institutions tend to report to their executive committee, which may inform the Board if required. Often, matters relating to vulnerability are included as part of reporting on other issues, such as customer complaints, dispute resolution, credit reporting or financial crime/fraud reporting. The focus for many subscribers in reporting vulnerability matters to the Board/executive committee is largely on the potential financial impact on the business, as opposed to seeking or suggesting ways to help and improve outcomes for customers experiencing vulnerability. The use of internal reporting systems for tracking, monitoring, and reporting vulnerability is rare. Subscribers' Boards should play a strategic and proactive governance role in relation to customers in vulnerable situations

One in five subscribers has a dedicated team or staff member to manage vulnerability

Just 19% of subscribers reported having a specifically appointed team or individual whose role is largely to oversee how customers experiencing vulnerability are managed within their organisation. For the 65% of subscribers that do not have a dedicated vulnerability team/staff member, most said responsibility for managing vulnerable customers falls to frontline teams, with support from other business areas where required. Smaller institutions reported they lack the available resources or sufficient customers to appoint a dedicated vulnerability team/staff member.

Fewer than one-third of subscribers have partnered with a community organisation specialising in helping vulnerable people

While many institutions refer their customers to not-for-profit financial counselling services, government agencies, charities and other organisations that assist vulnerable people in the community, few have established partnerships with these organisations as a way to seek expert support and advice on vulnerability matters. Subscribers who partner with community organisations gave interesting examples of how they and their customers have benefited from the arrangement.

Introduction

Vulnerability in the spotlight

Consumer vulnerability is firmly in the spotlight of regulators, law makers, consumer advocates, the media, and the wider community. Various Royal Commissions into financial services, aged care, the disability sector, and family violence unearthed many examples of poor outcomes for some of society's most vulnerable members and highlighted the need for service providers and commercial businesses to address vulnerability at all stages of the customer journey.

More recently, the prevalence of extreme natural disasters, the COVID-19 pandemic and our ageing population have led to increasing numbers of people experiencing vulnerability and demonstrating that vulnerability can happen to anyone, at any time. Indeed, in their December 2020 report *Spotlight on customer vulnerability*,[2] COBA and EY Australia found that over half the Australian population is experiencing vulnerability risk factors, with COVID-19 having a particularly severe impact on those already considered to be vulnerable.

This presents a significant challenge to customer owned banking institutions; whose purpose is to improve the financial wellbeing of their individual members and communities. A new version of the Code, which takes effect in October 2022, introduces more stringent obligations around how institutions will respond to customers experiencing a range of different vulnerable circumstances.

About the Inquiry

As part of the 2021 Annual Compliance Statement, all Code subscribers were asked to complete a questionnaire[3] relating to how they identify and respond to customers experiencing vulnerability, including instances of elder abuse and domestic/family violence. Each subscriber was then interviewed via video conference as part of the ACS Verification Program to seek additional information and clarify responses to the vulnerability questionnaire. The Committee aimed to find out:

- how Code subscribers define vulnerability
- how Code subscribers manage issues concerning domestic/family violence and elder abuse
- what policies, processes and training programs Code subscribers have in place as part of their vulnerability frameworks
- whether Code subscribers are ready to meet their compliance obligations under the new 2022 Code.

[2] https://www.customerownedbanking.asn.au/news-and-resources/reports/spotlight-on-customer-vulnerability
[3] See Appendix 1.

Code subscriber classifications as per $ amount in assets:

- Category AA - Over $5b
- Category A – Between $2b and $5b
- Category B – Between $1b and $2b
- Category C – Between $500m and $1b
- Category D – Between $200m and $500m
- Category E – Under $200m

The Code obligations

2018 Customer Owned Banking Code of Practice

Although the 2018 Code does not specifically mention customers experiencing vulnerability, Key Promise 2 contains the following provisions:

Key Promise 2: We will focus on our customers

We will place a high priority on service, competitiveness and customer focus. We will provide friendly and reliable service to our customers. Our customer service standards will be appropriately tailored where we are aware that you have special needs (for example, because of your age or a disability, because you are an indigenous person, because English is not your first language, or because you are unfamiliar with financial products and services).

2022 Customer Owned Banking Code of Practice

The 2022 Code, which comes into effect on 31 October 2022, includes specific obligations relating to the identification and treatment of customers experiencing vulnerability.

Part B: Inclusive Banking Services, sections 17 to 27

Inclusive banking services

We are committed to providing inclusive and accessible banking services

17. We will take reasonable steps to make our banking services accessible for individual customers in the areas in which we operate, including customers who speak English as a second language, older customers, people with a disability, and First Nations Peoples.
18. We will offer to communicate with you through an interpreter service where reasonably practical if you do not speak fluent English, and we think that you would clearly benefit from this assistance.
19. We will offer to communicate with you through the National Relay Service if you have hearing difficulties, and we think that you would clearly benefit from this assistance.
20. If you tell us about your personal or financial circumstance, we will work with you to identify a way for you to access and undertake your banking.

When providing banking services to low income earners or Commonwealth concession card holders

21. When you apply for a new banking product, if you tell us that you are on a low income or we are aware that you hold a Commonwealth concession card, we will give you information about banking products we offer that may be more favourable.
22. We may offer a low or no fee transaction account that does not have an overdraft facility and that is only available to customers who hold a Commonwealth concession card and who meet other eligibility requirements. If so, we will publicly disclose annually, for example in our annual report, how many of our customers have accounts of this type.
23. If we offer an account of this type, we will train our staff to help them recognise customers or potential customers who may qualify for this account.
24. If:

    a. we establish an account of this type for you, and
    b. we process a transaction that causes your account to be overdrawn, and charge you an overdrawn fee or any interest on the overdrawn amount

    we will rebate this fee or interest to you within 30 days. We will state this rebate commitment clearly in the account Terms and Conditions.

25. The rebate commitment in paragraph 24 does not apply to an account that was opened for you prior to this Code coming into effect.

When providing banking services to people experiencing vulnerability

26. We will adapt our customer service standards where reasonably practicable and take extra care where we are aware that you are experiencing vulnerable circumstances. This might be because of:

    a. age-related impairment
    b. cognitive impairment
    c. disability
    d. elder abuse
    e. domestic violence
    f. financial abuse
    g. mental illness
    h. a serious health issue
    i. factors relating to your cultural background or because English is not your first language
    j. your unfamiliarity with banking products and services, or
    k. other personal or financial circumstance causing significant detriment.

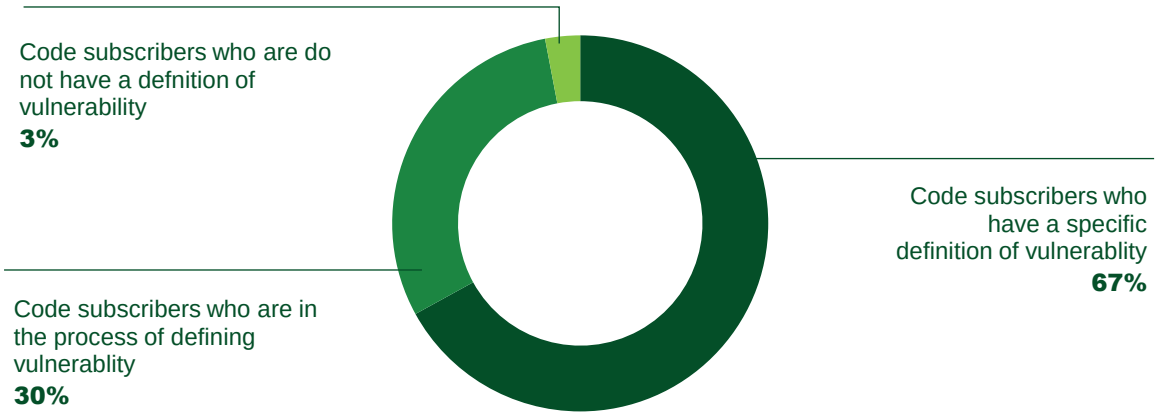
27. We will train our staff how to identify customers experiencing vulnerability, and how to adapt our customer service standards for them in a sensitive and helpful way. Our training will include awareness of vulnerable circumstances as a result of domestic violence and elder abuse.

Defining vulnerability

The first step to developing a framework that recognises and responds to the needs of customers experiencing vulnerability is to understand what is meant by the term 'vulnerability'. Without a clear definition of vulnerability and its associated risk factors, it becomes more difficult to identify and help a customer who may be experiencing it.

While not directly defining vulnerability, the 2022 Code is certainly more explicit than the 2018 Code. It provides examples of why a customer might be considered vulnerable, including age-related impairment, elder abuse, domestic violence, ill physical or mental health, or an unfamiliarity with banking products and services. The examples provided in the new Code should be front of mind for subscribers as they consider what vulnerability looks like and prepare to meet the new Code's requirements, although they need to watch out for other risk factors too.

How subscribers define vulnerability



In response to the ACS vulnerability questionnaire, 67% of Code subscribers said they have a specific definition for vulnerability. Another 30% reported they are in the process of defining vulnerability or are planning to do so. Only two subscribers (3%) said they do not currently have a definition.

For the 97% of institutions that have a definition for vulnerability or are developing one, their overall vulnerability frameworks (including their policies and processes for servicing customers experiencing vulnerability) are underpinned by a general understanding from staff across the organisation of what vulnerability looks like.

Most subscribers' definition of vulnerability was broad and encompassed people in a range of different situations. For many subscribers, the list of identifiers for customers experiencing vulnerability was wide-ranging and included people who are:

- older Australians
- living with a disability, impairment or illness, including mental illness
- experiencing family violence
- experiencing elder abuse
- from culturally and linguistically diverse backgrounds
- Indigenous Australians

- living in isolated locations
- experiencing challenging personal circumstances, such as bereavement, job loss or divorce
- from LGBTIQA communities
- impacted by natural disasters.

"A vulnerable person can be anyone who is unable to protect themselves against significant harm or exploitation."

— Category B subscriber

Institutions in the larger size categories were more likely to have documented definitions of vulnerability than smaller institutions. For example, three Category AA subscribers reported that they publish and distribute their definition of vulnerability throughout the organisation to help staff identify customers experiencing vulnerability.

"Vulnerability can be permanent, temporary or periodic, and may be linked to a particular significant life change (for example, a serious illness or job loss), or multilayered (for example, a person with low financial literacy)."

— Category AA subscriber

For one of these subscribers, this occurs in the form of a Customer Vulnerability Standard. In addition to defining vulnerability, this document reminds staff that anyone can experience vulnerability and not all customers will be impacted in the same way. For the other two subscribers, their definition of vulnerability is in guidance on how to identify and help vulnerable customers, which includes examples of circumstances that may lead to a person experiencing vulnerability.

Smaller institutions, on the other hand, tend to define vulnerability in broader terms. One Category B subscriber reported it defines vulnerability as "a person or people whose ability to understand and effectively communicate appears diminished and there is evidence to indicate that they may be unable to protect themselves from harm or exploitation, or report abuse, or to effectively provide suitable self-care without assistance".

Adopting what it describes as a "broad, common-sense" approach, one Category E subscriber defines vulnerability as "any member needing extra care in any way with their banking. This can be the elderly, the young, non-English speaking or anyone that simply doesn't understand their banking and looks to us for guidance and assistance".

A Category C institution defines vulnerability as a situation where someone may be exposed to financial loss or harm. It has introduced a Vulnerable Persons Program – a formalised process to help staff understand and identify customers experiencing different types of vulnerability, from financial abuse and family violence to misuse of Powers of Attorney and joint accounts.

"As a credit union based in remote Aboriginal communities, vulnerability is a major focus. People coming into the branch are coming from a remote community or for a hospital visit. Taking extra care is part of what we do, as all our customers are potentially vulnerable."

— Category E subscriber

Many subscribers commented that any customer could find themselves at risk of vulnerability due to unforeseen circumstances. Some also noted that vulnerability can sometimes be temporary, depending on the customer's individual situation. One Category D subscriber observed that those who perpetrate abuse against vulnerable people are often vulnerable themselves, and that defining vulnerability is therefore not always straightforward.

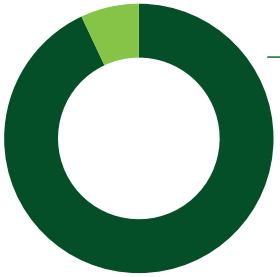
Two Code subscribers noted that having a prescriptive definition of vulnerability could lead to unintended consequences if applied too rigidly. One Category A subscriber observed that the definition of vulnerability needs to be broad enough to identify all vulnerable customers, but not so broad that it assumes all customers in a particular risk category are vulnerable.

A Category B Code subscriber raised a concern that customers who are deemed to be vulnerable by their financial institution may feel stigmatised or discriminated against. The subscriber also noted that while vulnerability is relatively easy to define, classifying a customer as vulnerable can be far more challenging, particularly when a customer has not previously been considered vulnerable but becomes so due to unforeseen circumstances.

"We define vulnerability to include both situations whereby a customer's particular characteristics and circumstances may render them permanently or temporarily in need of additional care in respect to the management of their affairs. This also captures individuals who may generally be capable of managing their affairs but in certain circumstances may need assistance or additional support."

— Category A subscriber

Identifying vulnerability



93% subscribers rely on appropriately trained frontline staff to detect vulnerability in a customer

60% subscribers said customers self-report as vulnerable

The 2022 Code includes provisions for identifying vulnerable customers – namely, that subscribers must provide their staff with training in how to identify customers experiencing vulnerability. Whilst training aspects of these provisions are covered in a separate chapter of this report, the Committee was interested in understanding what methods subscribers currently use to identify vulnerability in their customers.

According to the questionnaire responses, the most common method is by interacting directly with customers: 93% of subscribers reported their staff are trained to identify vulnerability by listening to what individual customers tell them and/or observing how they behave; and 60% of subscribers reported in some cases customers will directly advise they are experiencing vulnerability.

Less common is the use of data analytics to identify when customers may be in vulnerable circumstances. Around 49% of subscribers reported that they use customer-specific data, such as information about irregular activity on accounts or dishonoured direct debits, while only 7% of subscribers said they use in-house data, such as demographics.

Training staff to identify vulnerable customers

All but four subscribers reported they train their staff to detect signs of customers experiencing vulnerability while interacting with individuals. This includes learning to recognise certain ‘red flags’ during face-to-face or phone conversations with customers and observing their behaviour for anything out of the ordinary.

According to subscribers, some of the scenarios their staff are trained to look out for when interacting with customers are:

- confusion about or lack of awareness of account balances and transfers
- requests for unusual account transfers or withdrawals, particularly if the customer is accompanied by another person
- showing fear, uncertainty or not being allowed to speak for themselves when accompanied by another person
- mail no longer being sent to their home address
- behaving or speaking in a manner that differs from the usual
- advising they are paying bills for a friend or relative
- having income or Centrelink payments paid into a partner or relative’s account
- changing or adding authorised signatories to their accounts
- being unaware of newly issued ATM, debit or credit cards for their accounts

- showing sudden concern about protecting their personal privacy or the security of their accounts
- being reluctant to involve a co-borrower when seeking a hardship variation or other assistance
- conducting banking in a way that is inconsistent with their ability – for example, withdrawing money from an ATM despite being housebound or in hospital
- registering for internet banking when all prior banking has been carried out in the branch.

"By observing their behaviour or discussion, we can identify a member who is clearly struggling to understand their banking needs or to complete their banking transactions and needs our assistance, as well as members who may expose themselves to fraud or be taken advantage of."

— Category E subscriber

Several subscribers provided examples of what their staff are trained to do if they suspect a customer may be experiencing vulnerability because of fraud, elder abuse, domestic violence or coercion from a friend or family member.

At one Category E institution, if an elderly customer comes into the branch to withdraw money and they are accompanied by another person, branch staff are trained to make sure the customer can clearly articulate why they are making the withdrawal and what the funds will be used for before the transaction can occur.

A Category D institution described a similar process, using the example of an elderly customer who was brought into the branch by her son to transfer a large sum of money into the son's account. Before enabling the transfer, branch staff interviewed the customer alone in an office to make sure she understood what she was requesting and that she was not being pressured by her son to make the transfer.

Another Category E subscriber reported that its staff are trained to take a comprehensive 'Know Your Customer' (KYC) approach to each of its customers. This helps them identify if someone is withdrawn, stressed, upset, or demonstrating other behaviour that may indicate they are experiencing vulnerable circumstances, such as family violence or elder abuse.

One Category A subscriber reported that as part of its vulnerability training, staff learn how to broach the subject of a potentially vulnerable customer's personal situation in a sensitive and respectful manner. Once a staff member has confirmed the customer is experiencing vulnerability, a note is recorded on the customer's file (with their consent) so that other members of staff are aware of the customer's situation and can act appropriately in future dealings.

"With COVID, we telephoned all borrowers who worked within industries affected by any lockdowns/restrictions, to let them know what hardship assistance was available. We wanted to do this before members had to ask for help."

— Category D subscriber

In a similar vein, a Category AA subscriber reported that it conducts workshops for staff on how to deal with challenging interactions, which includes identifying and responding to vulnerable customers. New employees attend training sessions as part of their induction and are allocated a 'buddy' to help them handle challenging situations such as identifying customers experiencing vulnerability and responding to customer aggression.

This is supported by a procedure that incorporates 'red flags' to help staff recognise when a customer is experiencing vulnerability, and a policy of authenticating each customer's identity before making changes to personal information or providing a requested service.

Customers self-identifying as vulnerable

A customer may advise their financial institution they are experiencing vulnerability before the institution becomes aware of it through other means.

In some cases, this advice may be explicit – i.e., the customer tells branch or call-centre staff they are in a vulnerable situation due to family violence, ill health, or fraud. In other cases, the advice may be implicit – i.e., the customer requests financial hardship assistance or discloses the existence of a family violence intervention order, indicating they are experiencing or at risk of experiencing vulnerability.

While almost two-thirds of Code subscribing institutions reported this is one of their methods for identifying customers experiencing vulnerability, many acknowledged it rarely happens, further underscoring the importance of training staff to identify vulnerability.

On the occasions when it does happen, subscribers emphasised the need to show care and respect for the customer. One Category B institution described a process whereby customers in this situation are invited somewhere more private, such as an office, to discuss their situation and hear about what assistance is available to them.

Other institutions described the procedures that kick in once a customer has self-identified as vulnerable. One Category E subscriber said it immediately implements measures to protect customers who advise they are experiencing family violence by offering to restrict access to or freeze accounts.

At one Category AA institution, staff access resources via the intranet that provide guidance on how to protect the safety, privacy and finances of a customer who advises that they are experiencing family violence.

Some subscribers reported they refer all customers experiencing vulnerability to their Compliance and Legal team for review. In the case of one Category AA subscriber, customers experiencing vulnerability are also referred to risk advisers and to the financial crimes team if the customer has been a fraud or scam victim. A Category D subscriber noted if the customer experiencing vulnerability is also a borrower, it will notify the credit control team.

One Category C subscriber noted, for consistency, it tries to ensure one member of staff is the single point of contact for a vulnerable customer. Where appropriate, it refers customers experiencing vulnerability to a network of professionals for help with their situation. This includes referrals to financial counsellors, lawyers, community service workers and family violence support agencies.

Using customer-specific data to identify vulnerability

As COBA and EY Australia highlighted in their *Spotlight on customer vulnerability* report, financial institutions are uniquely well equipped to identify vulnerability risk factors in their customers due to the nature of the data they collect and hold.

When used appropriately and ethically, customer data can provide valuable insights into a person's financial circumstances and banking habits. This includes whether they are experiencing vulnerability. Importantly, data can alert financial institutions to instances where a customer experiencing vulnerability is at risk of harm or detriment from financial abuse, fraud, or other financial crimes.

Of the 49% of subscribers who use customer-specific data to identify vulnerability, most said they monitor transactions for unusual patterns or behaviours. This may include uncommonly large and/or frequent transactions, or transactions that occur at locations or for products that do not fit the customer's profile. (One Category B subscriber provided an example of a 70-year-old customer using their debit card to buy hundreds of dollars' worth of video games.)

Some subscribers reported they have identified cases of abuse by a Power of Attorney through transaction monitoring activities. Monitoring picked up unusual transactions on customer accounts, such as frequent withdrawals of large sums of cash.

One Category D subscriber outlined some of the 'red flags' it looks for when analysing customer data for signs of vulnerability:

- erratic use of payment instruments
- repeated requests to reset online banking access
- frequent card reorders due to lost cards
- overdrawn accounts
- dishonoured direct debits for important services such as utilities or insurance
- international money transfers or SWIFT payments to overseas accounts (sent or received) where the account holder is on a pension
- sudden changes to loan repayments.

Several subscribers reported they use customer data to detect whether an account holder has been the victim of fraud or other financial crime – an indicator of vulnerability, particularly in elderly customers and those from non-English speaking backgrounds. In most cases, the subscriber's financial crime or anti-money laundering/counter-terrorism financing (AML/CTF) teams are alerted to suspicious transactions which are investigated and addressed.

One Category B subscriber reported it was able to identify several victims of modern slavery by using customer data which showed people's salaries were being withdrawn at ATMs just minutes after hitting their account.

While very few subscribers provided details about whether their controls for monitoring customer-specific data are automated, two institutions (a Category A subscriber and a Category D subscriber) advised they manually monitor customer transactions for signs of

vulnerability. Both reported they rely on appropriately trained staff to identify customers experiencing vulnerability when reviewing information such as loan applications and account transactions.

Using in-house data to identify vulnerability

Just four subscribers reported they use in-house data from all customers to identify potential vulnerability risk factors and then apply this to identify individual customers at risk. This includes general data on customers' age, their demographics (such as whether they reside at a retirement home or aged care facility), member history data, and transactional data.

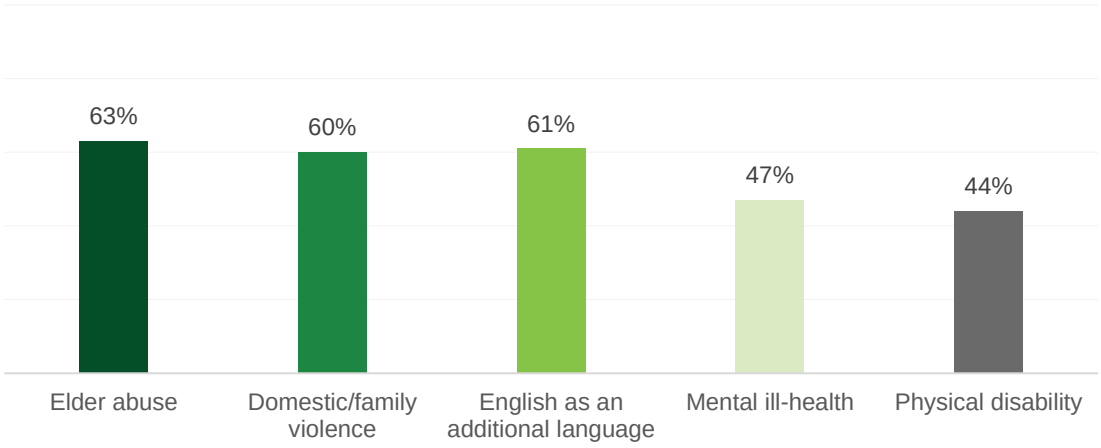
Policies and processes for addressing vulnerability

The Inquiry sought to find out about the policies and processes subscribers have in place to ensure they address different types of vulnerability their customers may experience, and to determine their readiness to meet the obligations for addressing vulnerability in the 2022 Code.

As part of the questionnaire, the Committee provided a list of vulnerability examples aligned with instances of vulnerability outlined in the 2022 Code. Subscribers were asked to select all for which they have a specific policy or process, and to add any others as appropriate. This was followed up during the ACS Verification Program, where subscribers were asked to provide additional detail about their vulnerability policies and processes.

A snapshot of subscribers' vulnerability policies

Percentage of subscribers with policies to address vulnerability



Five most addressed reasons for vulnerabilty

The questionnaire results showed around two-thirds of subscribers reported having policies/process in place to address vulnerability relating to ***elder abuse*** (63%), ***domestic/family violence*** (60%), and ***English as an additional language*** (61%).

Just under half reported having policies/processes to manage customers experiencing vulnerability due to ***mental ill-health*** (47%) and ***physical disability*** (44%), and just under one-third reported having policies/processes for addressing vulnerability in customers living with other (non-mental health-related) ***serious illness*** (31%).

Around one-quarter of subscribers said they have policies/processes to address customers experiencing vulnerability, including ***First Nations Peoples*** (28%) and customers who are ***unfamiliar with banking products and financial services*** (21%). A similar proportion of subscribers (28%) said they have a policy or process for ***working with financial counsellors, community representatives and/or other specialists*** to assist customers experiencing vulnerability.

In their ACS verification interviews, some institutions – predominantly those from larger size categories – described quite detailed and specific vulnerability-related policies. One

Category AA subscriber listed several resources it has to help address vulnerability both directly and indirectly, including:

- ‘customer capacity to act’ guideline
- financial abuse and misuse of Power of Attorney guideline
- joint account guideline
- vulnerable customer guideline
- fees and charges exemption guideline
- fees and charges waiver procedure
- breach of acceptable use procedure
- dealing with self-harm procedures
- public advocate or public guardian powers
- state-based guardian role guideline
- AFCA common issues for financial abuse of a vulnerable customer
- elder abuse fact sheet
- financial hardship brochure
- LGBTIQ inclusive language talk kit
- supporting ‘at risk’ customers guideline.

A second Category AA subscriber explained it publishes a guide on its intranet for staff to access when they identify a customer potentially experiencing vulnerability. The guide contains information about the various types of vulnerability, the processes staff should follow (including how to record and escalate the matter), and how to respond to and communicate with the customer experiencing vulnerability or their representative.

The subscriber also has a staff-assisted account balance process designed to help First Nations customers. This includes policies outlining the steps for staff to take when a customer has difficulty communicating in English; and policies and procedures for dealing with Powers of Attorney and Administration Orders.

Some subscribers, while not necessarily having discrete policies addressing specific types of customers experiencing vulnerability, described policies and processes incorporating ways to address vulnerability more generally. For example, some institutions said they have a single policy, such as a financial hardship policy designed to cover a range of vulnerability types. This includes those experiencing family violence, elder abuse, or serious illness.

Other subscribers reported having a specific process for responding to customers with carers and those who are hearing impaired.

Case study

Introducing resources to help improve customers' financial wellbeing

One Category AA subscriber created a new team dedicated to identifying and responding to customers who may be struggling financially. This followed a customer survey, conducted over a six-month period. The aim was to find out how customers felt about their financial wellbeing. This led the subscriber to launch a Financial Knowledge Centre – a collection on online courses, articles, and other resources to help customers improve their financial literacy and overall financial wellbeing.

Elder abuse and family violence policies and processes

Despite almost two-thirds of subscribers reporting their vulnerability policies cover customers experiencing domestic/family violence and elder abuse, only nine subscribers (16%) said they have a separate policy specifically addressing the needs of these customers. A further 10 subscribers (17%) reported they are either in the process of implementing, or planning to implement, a separate policy covering elder abuse and/or domestic/family violence. Some reported they address, or plan to address, the topic of elder abuse within their domestic/family violence policy.

Many subscribers (58%) reported they don't have a policy specifically focusing on elder abuse and/or included in a family violence policy. In most cases, these types of vulnerability are addressed in another policy, such as a financial abuse policy, a Power of Attorney policy, or an overarching policy for customers experiencing vulnerability.

For example, a Category A subscriber explained that although it doesn't have a specific elder abuse policy, guidance on assisting customers who are, or may be at risk of, experiencing elder abuse is addressed in the vulnerable consumer program policy as well as Power of Attorney processes and procedures. (More detail about subscribers' Power of Attorney policies and processes is included below.)

"For many years we have had a policy on assisting a person with a disability. Over the years this has been expanded to cover elder abuse and domestic violence, and more generally any case of vulnerability. We have endeavoured to keep all cases of vulnerability within the same documents, as the approach of staff should be the same for all cases: action from a place of kindness, with discretion, and a genuine concern to assist a person who is in need."

— Category D subscriber

Some institutions explained while they don't have family violence or elder abuse policies per se, these issues are covered under financial abuse policies or guides for staff. This includes

sections on how to identify a customer who is or may be the victim of financial abuse, including the elderly or someone experiencing family violence.

In the case of a Category B institution, elder abuse is addressed at length within its fraud risk management and financial hardship policies. Whilst a Category E subscriber addresses family violence and elder abuse in other policies, including its internal dispute resolution policy.

One Category AA subscriber reported it's reviewing all vulnerability policies, procedures, and practices to better support its staff and customers. The subscriber plans to consolidate its existing vulnerability policies into one overarching policy addressing all vulnerable customer categories.

Power of Attorney policies and processes

Customers who have given another individual or individuals Power of Attorney over their financial affairs are among the most vulnerable. These customers are often elderly or living with a disability, which increases their risk of suffering financial abuse. Abuse can occur through a family member or friend coercing the customer into appointing them as POA, and/or by misuse of the customer's finances without their approval or knowledge.

Considering the number of customer-owned banking institutions that have customers in the aging demographic bracket, it's vital for all Code subscribers to have robust policies and processes for managing POAs. The Committee was therefore pleased to note all but two subscribers reported having documented policies and processes relating to POAs.

Most institutions' POA policies are underpinned by processes designed to protect customers experiencing vulnerability from financial abuse and to assist staff to manage POAs appropriately. These processes generally commence from the time the POA is applied for. Many subscribers reported their staff are trained to understand the correct procedure for accepting and verifying POAs, as well as applying them to a customer's account.

One Category AA subscriber reported its frontline staff receive comprehensive on-the-job training in the POA process. This includes the purpose of a POA, the different classes of POA, and the various ways in which a POA may be structured. Similarly, staff at one Category C institution are provided with documented procedures describing different types of POA's and their features, as well as the steps to take when an Attorney wishes to transact on a customer's account, and when a POA is cancelled or revoked.

"We have an in-depth policy and process for dealing with Powers of Attorney. The process looks at matters from onboarding to ongoing assistance, as well as monitoring for elder and financial abuse. Our policy outlines what action is to be taken during disputes and concerns of abuse. We align our Power of Attorney process with our external lawyer's guide on POAs."

— Category A subscriber

Two subscribers – a Category C institution and a Category E institution – reported their POA policies require staff to sight original documentation, including evidence of the POA and

identification from the Attorney, along with affirmation from the customer (either in written or verbal form) prior to accepting the POA.

At one Category AA subscriber, individuals who are given Power of Attorney over a customer's financial affairs are provided with a copy of the institution's POA policy. This includes an information sheet outlining the Attorney's responsibilities. Another Category AA subscriber has a POA registration process that includes the method of operation for the Attorneys, and a matrix staff can reference to check how an Attorney is to act on the customer's behalf.

Some institutions reported all POAs are referred to a specialised team to manage or review. For example, at one Category A institution, a central team within the Banking Operations department manages all POAs in accordance with a documented procedure and compliance manual. This is to ensure that only staff with the appropriate skills and knowledge are assessing and accepting POAs.

Two Category C subscribers explained their Risk, Compliance and Legal team reviews all POA applications to check for validity. Some other subscribers reported they escalate only complex or problematic POAs to their Risk, Compliance and Legal team.

A number of subscribers in the C, D and E size categories reported they rely on guidance from external sources to manage POAs. This includes COBA, the NSW Government Ageing and Disability Commission, specialised law firm DB Legal, and GRC Solutions (for training modules relating to POAs).

Board and executive oversight of customer vulnerability matters

1 IN 4 **SUBSCRIBERS REPORT VULNERABILITY MATTERS TO THEIR BOARD/EXECUTIVE COMMITTEE**

LESS THAN HALF USE DATA ANALYTICS TO IDENTIFY VULNERABLE CUSTOMERS

To ascertain the level of executive oversight of vulnerability matters, subscribers were asked whether they have a process for regularly reporting customer vulnerability matters to the Board and/or executive committee.

Around one in four subscribers (26%) confirmed they do, while almost one in six (17%) said they were establishing or planning to establish a regular process for doing so at the time of responding to the inquiry.

Almost half (46%) revealed they do not have a process for reporting matters about customers experiencing vulnerability to the Board and/or executive committee. These subscribers explained that matters are often escalated to management, who may then report up the chain of command.

Reporting pathways

Subscribers with a process for ensuring executive oversight of vulnerability matters described a range of different reporting pathways.

Smaller and mid-sized institutions are more likely to regularly apprise their Board of customer vulnerability matters. This is often via the Board Risk Committee or through direct updates from the Chief Risk Officer (CRO) or Customer Advocate. One Category C subscriber revealed incidents of customers experiencing vulnerability are reported to the Board and senior executives at least once a month. A Category D subscriber explained its CRO/Head of Compliance has a direct reporting line to the Board Risk Committee and acts as the Committee's Chair from time to time.

"We have a process of reporting to all staff throughout the organisation when a potential vulnerable abuse situation arises. That way, all staff are aware of what has occurred."

— Category E subscriber

The reporting pathway at larger institutions tends to involve the executive committee being advised of customers experiencing vulnerability matters via periodic or ad hoc reporting. Boards are generally only informed on an 'as needs' basis. One Category B subscriber reported matters about customers experiencing vulnerability on an 'issue specific' basis to

management committees, which include representatives from the executive team who inform the Board if required.

Indirect reporting of vulnerability matters

Several subscribers revealed matters relating to customers experiencing vulnerability are made known to the Board and/or executive committee through other forms of reporting, such as complaints reporting or financial crime/fraud reporting.

Two Category AA subscribers gave examples of this. One said its senior executive group receives regular reports from the financial crime unit about any potential instances of financial abuse of customers experiencing vulnerability. The other reported its financial crime division advises the Board Risk Committee and Management Operational Risk Committee about any customers who have been identified as victims of scams or fraud.

Similarly, the CRO at one Category B subscriber provides the Board with a regular report on instances of fraud within the institution. This includes demographic data about the customers involved, such as their age and whether the fraud was the result of elder abuse.

"We have no specific vulnerability reporting. It forms part of our Complaints and Financial Crimes reporting, where relevant."

— Category AA subscriber

Some subscribers said matters relating to customers experiencing vulnerability are not reported as a separate line item to the Board or executive committee. Rather, they are included within data about customer complaints, dispute resolution reporting and credit reporting.

According to one Category AA subscriber, regular incident, complaint and breach reporting to the Board and executive committee may include vulnerability and customer aggression scenarios. The executive committee is advised about any financially vulnerable customers who have loans or credit with the institution and who may need credit assistance.

One Category A institution explained statistics relating to customers experiencing vulnerability are included within the dispute resolution report. This is provided to the Board. Another institution of the same size said matters involving customers who have been identified as victims or potential victims of domestic violence, elder abuse or other financial abuse are made known to the Board as part of complaints reporting.

Internal reporting systems for tracking and monitoring vulnerability

A handful of subscribers revealed they have, or plan to implement, systems or registers for recording and monitoring cases of customers experiencing vulnerability to improve executive oversight and intelligence sharing.

At the time of responding to the inquiry, one Category AA subscriber was developing a vulnerability framework that includes a new complaints management system with the ability to flag when a customer is experiencing vulnerability. Once the system is operational, the subscriber intends to provide the Board with intelligence about customer vulnerability, including the institution's response and areas of emerging risk or concern.

"Executive management is updated on any cases of vulnerability. The Board is informed if there are any financial impacts."

— Category D subscriber

A second Category AA subscriber reported it was developing a customer relationship management program to track and record interactions with customers experiencing vulnerability. The program data will be analysed and reported to the executive committee each month. While the subscriber currently reports major cases of customer vulnerability, the new program will enable executive oversight of every instance.

Three Category C institutions said they use incident registers, located within their governance, risk and compliance software, to record, report and monitor customers experiencing vulnerability. Incident reports are extracted from the register and provided to the Board and/or executive committee each month for review and discussion.

Leading from the top

Why Boards need to know about customer vulnerability matters

To have effective oversight and discharge their duties, Board directors need access to information on a wide range of topics. This includes information about non-financial risks that could lead to poor outcomes for customers, such as the failure to support customers experiencing vulnerability.

In their discussions about executive oversight of matters relating to customer vulnerability, the focus for many subscribers in reporting these issues to the Board was the potential financial impact on the business, rather than having strategic discussions about the role and performance of the bank in improving outcomes for vulnerable customers.

Vulnerability matters can certainly pose a financial risk to customer owned banks (especially where financial crime is involved) and should be reported to the Board for prudential management. However, Boards are also responsible for the governance of non-financial risks, and for ensuring everyone in the business is complying with their Code obligations and doing the right thing by customers. As the 2022 Code has more detailed obligations relating to institutions' management of vulnerable customers, subscribers will need to provide their Boards with a more complete picture of customer vulnerability and how it is being addressed within the organisation.

Vulnerability training for customer-facing staff

95% **SUBSCRIBERS PROVIDE, OR ARE PLANNING TO PROVIDE VULNERABILITY TRAINING PROGRAMS**

A consistent theme in earlier chapters of this report is customer owned banking institutions' reliance on their frontline staff to identify and respond to customers experiencing vulnerability. Based on subscribers' responses to the question, "Do you provide training on vulnerability to all customer-facing staff?", the majority appear to be providing their frontline employees with some of the skills required to recognise and address vulnerability.

Seventy-nine per cent of subscribers confirmed that they provide their staff with vulnerability training, while a further 16% reported that staff vulnerability training is in the pipeline. Just three institutions reported that they do not provide any vulnerability training to their customer-facing staff. Since we conducted the research for this paper, COBA has established free training for its members on vulnerability, run by Uniting Kildonan.

Training content

In most cases, the content of the training described by subscribers was comprehensive and covered a range of vulnerable customer types, including:

- customers vulnerable to other parties
- customers with reduced decision-making capacity
- customers with special needs
- elderly customers at risk of financial abuse
- customers experiencing relationship breakdowns and domestic violence
- Powers of Attorney
- loans and guarantees.

Many subscribers reported they use GRC Solutions' six-module training program, 'Protecting vulnerable customers from potential financial abuse', which covers several of the topics listed above. This was most popular with mid-sized institutions but used by subscribers from all size categories.

Some subscribers (mainly those in Category D) also reported using training materials from the SALT compliance learning management system, purchased through GRC Solutions. Other training sources include DB Legal compliance notes, and regular bulletins from COBA and GRC Solutions. One Category D subscriber reported it emails staff a monthly SALT topic, which staff must confirm they have read and understood.

Several larger institutions reported they have built vulnerability training into their inhouse training programs. One Category A subscriber explained it includes vulnerability training as a learning module within its 'Customer First' training program. A second Category A subscriber said all frontline staff must complete a dedicated training program involving learning how to interact with customers to understand their circumstances, challenges and needs.

In addition to using the online GRC Solutions training modules, one Category AA subscriber provides customer-facing staff with internal coaching. It uses scenario-based learning to identify and manage customers experiencing vulnerability, with a particular emphasis on listening to what customers are saying.

A Category C subscriber said it creates a different presentation each year to teach staff about vulnerability. The presentations usually include examples of customer vulnerability identified within the organisation, as well as those from external sources, such as COBA or the wider industry.

"All customer-facing staff have completed training on customers experiencing family violence and have been provided with resources to help them assist these customers. Further training regarding vulnerable customers and those experiencing age-related impairment, or at risk of elder abuse, is being prepared and will be provided to all customer-facing employees."

— Category AA subscriber

Some subscribers reported they require staff from different areas of the business to complete vulnerability training.

For example, one Category A subscriber provides its Credit Control team with additional coaching in how to handle customers experiencing vulnerability with sensitivity. Whilst a Category B subscriber reported its lending specialists are required to complete specific training to identify signs of vulnerability in customers during the lending process.

A handful of institutions said they have specifically focused on providing customer-facing staff with training in how to recognise and respond to customers experiencing elder abuse and/or family violence. One Category C subscriber explained elder abuse is an area of particular concern, given the ageing demographic of its membership base.

Frequency and format of training

In general, subscribers provide vulnerability training to customer-facing staff on an annual basis, with new staff trained during their induction. A handful of institutions reported they conduct refresher training as required, and some also use staff meetings and team huddles as an opportunity to discuss and learn from real-life scenarios of customers experiencing vulnerability.

One Category E subscriber reported it conducts formal vulnerability training at least twice yearly for its staff. They discuss cases of actual customers experiencing vulnerability, and how best to manage them, during staff meetings. In addition to ensuring its frontline staff receive vulnerability training, the institution's CRO undertakes more comprehensive online vulnerability training.

A Category D subscriber flagged the importance of monitoring customer-facing staff once they have received vulnerability training to ensure they are correctly applying it on the job and to identify any training gaps. At this institution, branch and call-centre staff are monitored

by their managers, who can provide additional guidance and support for responding to a customer experiencing vulnerability if required.

Overwhelmingly, subscribers reported customer-facing staff undertake formal vulnerability training via online/eLearning platforms, particularly where the GRC Solutions training program is used.

A small number of institutions said they also provide face-to-face/classroom training on vulnerability wherever possible.

Dedicated vulnerability teams

1 IN 5 **SUBSCRIBERS HAVE A DEDICATED TEAM OR STAFF MEMBER TO MANAGE VULNERABILITY**

Around one in every five Code subscribers (19%) reported having either a team or a single member of staff dedicated to overseeing the identification and management of customers experiencing vulnerability. A further 7% reported they were in the process of appointing (or planning to appoint) a specific vulnerability team. Whilst 9% said they have an alternative arrangement for oversighting vulnerability in their organisation.

The majority of subscribers (65%) said they do not have a specific team or individual to manage vulnerability.

Subscribers with a dedicated vulnerability team

Eleven subscribers reported having a dedicated vulnerability team, although during their ACS verification conferences, most clarified that 'team' refers to a single staff member dedicated to overseeing the management of customers experiencing vulnerability.

One Category A subscriber has implemented a tiered approach. A Tier 3 vulnerability specialist with extensive training, skills and knowledge is engaged to manage customers experiencing vulnerability. The specialist provides expert advice for vulnerability matters unable to be dealt with by Tier 1 staff (frontline employees) or Tier 2 consultants (managers with a higher level of vulnerability training). Such matters include complex scenarios involving significant risk, and cases where the customer experiencing vulnerability has multiple product holdings with the institution.

As part of a review of the subscriber's Vulnerable Consumer program, the Tier 3 specialist's scope will be expanded to include case management of high-risk vulnerabilities, including domestic violence, elder abuse, mental health, and situational circumstances (for example, relationship breakdowns or repeated instances of scamming).

A Category AA subscriber reported it had recently established a senior customer vulnerability specialist within its customer relations team. Part of the specialist's role is to develop and strengthen the processes around vulnerability to help frontline staff identify and manage vulnerable and potentially vulnerable customers.

One Category C subscriber reported it has a vulnerable member review team consisting of the Member Experience Manager, Administration Services Manager, Risk and Safety Officer and other employees determined by the Chief Executive Officer (CEO) or CRO.

At one Category E institution, responsibility for identifying customers experiencing vulnerability has been assigned to the Assistant General Manager, who does this by observing customer interactions and through discussions with customer service staff. The Assistant General Manager also meets regularly with the institution's CRO to discuss matters relating to vulnerability, such as emerging areas of concern, training materials and industry guidance.

While noting all employees have a responsibility to deal with customers experiencing vulnerability, one Category B subscriber said it appointed a member of staff whose role includes monitoring transactional activity and Powers of Attorney to identify and manage potentially vulnerable customers.

Subscribers without a dedicated vulnerability team

Almost two-thirds of subscribers reported they have not appointed a specific team or individual to manage vulnerability. These subscribers were evenly spread across the various size categories.

Larger institutions reported customers experiencing vulnerability were generally managed within frontline teams (i.e., branch staff and customer service/contact centre staff), with support available from other areas of the business. This includes Governance, Hardship and Fraud. Several subscribers in categories AA, A and B said staff who identify a customer is experiencing vulnerability can report the matter to their line manager or team leader, with further escalation to the Risk, Compliance and Legal department when required.

One Category AA subscriber reported all client-facing staff are trained to identify vulnerable clients and understand the steps required to assist them. The National Retail Manager is recognised as a subject matter expert and provides additional support and/or management of vulnerability cases when required. The Complaints team, Internal Dispute Resolution Committee and Credit Assistance staff can also step in to support vulnerable customers where required.

“As our staff live and operate in the remote communities we serve, we don’t feel it is necessary to have a specific vulnerability team.”

— Category E subscriber

Smaller institutions reported they do not have the available resources or enough customers to warrant appointing a specific vulnerability team or individual. Most believe their size means they have a close enough relationship with their customers for appropriately trained frontline staff to identify and assist those who are experiencing vulnerability. According to some Category C, D and E subscribers, complex matters are referred to a branch manager in the first instance, with further escalation to someone at executive level, such as the CRO, Chief Operating Officer or CEO.

One Category E subscriber explained having a small team provides greater flexibility and allows staff to quickly adapt to the needs of different customers.

Subscribers with alternative arrangements

A handful of subscribers reported that whilst they don’t have a dedicated team or individual with sole responsibility for managing vulnerability, they do have teams or individuals across the business whose job includes advocating for customers experiencing vulnerability.

For example, the Deceased Estate Administrator at one Category A subscriber also oversees the management of vulnerable customers and the institution’s vulnerability process. This person reports to Finance and works closely with all departments – particularly Legal, Risk and Compliance – to identify solutions for customers who may be vulnerable.

They also train staff to identify vulnerability ‘red flags’, investigate cases of financial abuse, review new applications for POAs, and assist with any cases where a customer may be at risk of financial abuse from their POA.

Similarly, the role of the Banking Operations team at one Category C institution includes assisting customers who may be vulnerable due to fraud, financial hardship, bereavement (deceased estates) or POA matters.

Partnering with community organisations

FEWER THAN ONE-THIRD OF SUBSCRIBERS HAVE PARTNERED WITH A COMMUNITY ORGANISATION THAT SPECIALISES IN HELPING VULNERABLE PEOPLE

Even with rigorous vulnerability training, staff may not always know the best way to assist customers experiencing vulnerability. Each case can have unique and complex circumstances requiring expert handling, not least where domestic violence or elder abuse is involved.

There is an array of external support services for people experiencing vulnerability. These range from government agencies, customer advocacy groups, charities, and community organisations. The Committee is aware from our work with subscribers that many refer customers to these services for assistance. As part of this Inquiry, we were interested to learn whether subscribers themselves seek guidance and support to deal with customers experiencing vulnerability through partnerships with these external support services.

Engaging with organisations who can share 'lived experience' of the vulnerable people they represent helps institutions to identify gaps in staff training, products and service delivery that can cause poor outcomes for vulnerable customers. It also improves employees' understanding of the challenges and struggles vulnerable customers face, and the role employees can play in supporting them.

Given their deep community connections and their 'members first' approach, customer owned banking institutions are well placed to form meaningful and mutually beneficial partnerships with community organisations specialising in helping vulnerable people.

According to their survey responses, 32% of subscribers reported they have formed partnerships with community organisations who can provide them with expert support and advice on dealing with vulnerability. A further 5% said they were in the process of or planning to form partnerships. Whilst 12% said they have other advice and support arrangements in place. The remaining 51% of subscribers have not partnered with a community organisation for help with managing vulnerability.

Subscribers with partnerships

Examples provided by subscribers that reported having partnered with community organisations included the following:

- A Category A subscriber has links to a network of community organisations specialising in a broad range of vulnerabilities. Staff can seek support and advice from these organisations in how to manage vulnerable customers, as well as provide customers with access to these services when required. Acknowledging there will always be complex vulnerability cases exceeding the organisation's expertise and capability, the subscriber is working to extend its partnership network to include more external specialists.

- A Category C subscriber has a range of community and charitable partners which it both supports and seeks guidance from to assist elderly customers, customers living with a disability, families of war veterans, vulnerable children, customers experiencing financial hardship, those living with drug or alcohol dependence, and those experiencing family violence.
- One Category AA subscriber is piloting CareRing, a support program run by community service organisation Kildonan to empower customers experiencing vulnerability. In addition to referring its own customers to the program, the subscriber's staff have access to advice from CareRing experts on managing customers experiencing vulnerability. The subscriber also has a partnership with an external not-for-profit financial counselling service from which it seeks guidance on responding to customers experiencing family violence and financial abuse. It often engages with Financial Counselling Australia for advice.
- A Category D subscriber with a large rural membership has partnered with the Rural Adversity Mental Health Program to help it provide better outcomes for vulnerable and potentially vulnerable customers.
- A Category B institution sponsors the Zahra Foundation, a not-for-profit organisation that empowers and supports women and children who have been affected by family violence. As part of the sponsorship arrangements, the foundation helps the subscriber's staff to identify and assist customers who are or may be experiencing family violence.
- Having identified a number of its customers who are returned services members suffering from post-traumatic stress disorder, one Category A subscriber established its own charitable foundation to provide assistance dogs to support these customers.

"A focus area of our Foundation is to partner with organisations in the fields of aged care, disability, affordable housing and financial wellbeing. Through these partnerships we are able to shape and inform our business approach to helping vulnerable customers. We also have two days a year when our staff can volunteer in the community with our partner organisations."

— Category AA subscriber

Partnerships vs financial support for vulnerability-related causes

Some subscribers appeared not to recognise the difference between providing financial support to a vulnerability-related charity or cause and partnering with a community organisation to identify and support customers who are vulnerable.

Sponsoring a vulnerability-related cause is admirable. However, a successful partnership that provides holistic support for the most vulnerable in the community requires working together and learning from each other.

A successful partnership between a customer owned banking institution and a community organisation involves working together to overcome vulnerability in the

community and should benefit both parties. For the organisation, this might be financial support from the institution as well as vulnerable-customer referrals. For the institution, it should include access to guidance and support from experts within the organisation on how to improve outcomes for customers experiencing vulnerability.

Subscribers with no partnerships

Institutions that have not sought partnerships with community organisations generally have a policy of referring vulnerable or potentially vulnerable customers to an appropriate external support service, such as:

- local police
- 1800 RESPECT
- Family Relationship Advice Line
- Lifeline
- National Debt Helpline
- Relationships Australia
- WIRE
- Women's Domestic Violence Court Advocacy Services
- ELDERHelp
- National Relay Service
- Cyberwatch
- Scamwatch
- IDCARE.

"Frontline employees can suggest that a customer contact an external legal and support organisation. It is the customer's choice whether they seek help or not."

— Category C subscriber

In many cases, information about these resources, including contact details, is published on subscribers' websites for customers to access. Some subscribers reported their frontline staff have brochures and other material containing information about specialist support services they can hand out to customers experiencing vulnerability. One Category D institution provides staff with a state-by-state schedule outlining relevant external services and support for different types of customers experiencing vulnerability.

Many subscribers who reported they do not have any active community partnerships. Instead have extended relationships with legal services providing them with guidance and advice on how best to support customers experiencing vulnerability. In most cases, these are government services, such as the Office of the Public Advocate, State Administrative Tribunals, and the various state commissions for ageing and/or disability.

One Category AA subscriber said t although it does not partner with any external support services, it calls upon various government departments and community organisations for expert advice and specialist support in helping to deal with vulnerability. These include

guardianship tribunals, ageing and elder abuse hotlines, police services (for customer wellbeing checks) and the NDIS.

Some subscribers expressed concern about breaching a vulnerable customer's privacy when referring them to external support services and commented that helping customers experiencing vulnerability within the parameters of the Privacy Act can sometimes be a challenge. Others pointed out the services to which they refer customers experiencing vulnerability are often overstretched and unable to provide assistance within a timely manner.

For example, a regional-based Category D subscriber observed that the external support network for its community's most vulnerable members is often thinly stretched – particularly the aged care network and local GPs.

Some case studies

As part of the ACS Verification Program, Code subscribers described many instances where they have assisted customers experiencing vulnerability. This chapter includes a selection of short case studies of subscribers identifying and responding to customers experiencing a range of different vulnerabilities.

Customers experiencing domestic/family violence

The branch manager at a Category D institution suspected a customer was suffering from cognitive impairment after noticing he had begun to behave erratically (for example, providing repeated and inconsistent instructions over a short period of time, refusing to believe his own handwritten instructions to the branch, and being abusive towards branch staff). From observing interactions between the customer and his wife, the manager also suspected that domestic violence was occurring.

The manager sought advice from the Chief Risk Officer, and a strategy was put into place whereby the CRO kept the customer engaged in conversation. This allowed the branch manager to discreetly offer assistance to the customer's wife. However, the wife made it clear she was uncomfortable discussing the matter and did not wish to take it any further. Branch staff now provide the customer with a spare interview room to write out his instructions, which are collected by staff and processed, then returned to him with written confirmation of the actions taken.

After noticing bite marks on the arms of an elderly customer who had been flagged as vulnerable, staff at a Category AA institution gently and sensitively asked the customer a series of questions to ascertain what was going on. They also reached out to the customer's authorised carer and requested local police conduct a welfare check. These actions led to the customer receiving additional help with their living arrangements.

Customers who are victims of elder abuse

A Category AA subscriber detected an elderly customer was being financially abused by his tenants. The customer's wife had passed away several decades ago and as he had no government support, he had taken on tenants to survive but did not have any rental agreements with them. Having identified the customer's account was in arrears, the subscriber's support and recoveries team investigated and found his tenants had taken advantage of him to the tune of $60,000.

The subscriber connected the customer with a financial counselling service and put in place a hardship arrangement. Taking a 'big picture' approach to the situation, it also determined the customer was struggling in his personal life and referred him to a personal counsellor for assistance.

The support and recoveries team presented this as a case study to other areas of the business to help them learn about different ways to assist customers experiencing vulnerability.

An elderly customer visited the branch of one Category AA institution to question the balance on his accounts. During a conversation with branch staff, he revealed that a friend who was living with him had recently been added as an authorised signatory to his account.

It was revealed that over a four-day period, amounts totalling $6,000 had been withdrawn from the customer's account and deposited directly into the friend's account.

During subsequent dealings with the customer, he was confused and often angry, and did not recall recent conversations and agreements being made. The subscriber placed a high-priority message on the customer's profile, advising he speak to the branch manager, whom he had a good relationship with and who was familiar with the matter. Following a positive discussion with the branch manager, the customer consented to being contacted by a local support service. This resulted in a guardianship application being made and the NSW Trustee and Guardian being appointed the customer's financial manager.

Branch staff at a Category B institution noticed unusual transactions on an elderly customer's account when the customer came in to do their banking. The customer knew nothing about the transactions and revealed they had not been receiving any account statements from the bank.

The customer later confirmed the transactions had been made by their Power of Attorney for their own personal use. The Attorney had been using the customer's debit card, which they had access to for paying the customer's medical bills and had cancelled the delivery of account statements to the customer's home.

Staff acted immediately by placing a restriction on the card and escalating the matter to Risk, Compliance and Legal for further investigation. The investigation established the Attorney had misused a large amount of the customer's funds and had stolen their identification to restrict their banking activities.

It was also revealed the customer was co-habiting with their Attorney but wanted to move out. The subscriber put the customer in touch with community organisations who helped them relocate and provided support to change the Power of Attorney on their accounts.

An elderly customer of a Category B subscriber, who lived in a small country town and was showing signs of Alzheimer's disease. She had appointed her granddaughter as Power of Attorney. The subscriber identified as soon as funds were credited to the customer's savings account, her granddaughter would transfer them straight out or make various transactions inconsistent with the customer's previous spending history.

The granddaughter and her boyfriend applied to the subscriber for a home loan and advised they also wanted the elderly customer's name on the loan. The customer had more than $250,000 in a term deposit and the granddaughter advised her grandmother would contribute this money, along with funds from the sale of her unit, towards purchasing a property that included a granny flat for the customer to live in. Suspicious of this arrangement, the subscriber declined the loan application and contacted another family member – the customer's daughter – who was concerned money was being withdrawn from her mother's account. The granddaughter was removed as Power of Attorney and the Public Trustee issued administration orders to the customer's account.

Customers experiencing vulnerability who have been scammed or defrauded

A customer phoned the contact centre of one Category A institution to ask about the maturity of her term deposit, saying she wanted to lend $70,000 to a tradesman who was working at her property, so he could buy a new ute. She also called the contact centre to ask if she could give her bank card and PIN to a friend to do her shopping for her. On each occasion, contact centre staff advised her against doing either of these things, and noted her repetition of the same questions each time strongly indicating she was experiencing memory loss.

The subscriber referred the matter to its financial crimes team, which continues to monitor activity on the customer's accounts. The subscriber also engaged an external vulnerability specialist for advice on how to assist the customer and prevent her from financial abuse. The vulnerability specialist is working with the Office of the Public Guardian to investigate whether the customer has capacity over her own affairs, and whether she is being financially exploited.

Customers experiencing financial hardship

A Category AA subscriber identified a customer experiencing vulnerability was in financial hardship through the customer's interaction with the credit control team. The customer's financial position was reviewed, and the customer was offered and accepted the following hardship assistance:

- a three-month financial hardship arrangement
- cancelling the customer's $5,000 overdraft facility to prevent further debt
- freezing interest charges on the overdraft
- fortnightly payments of a set amount aligned to the customer's Centrelink benefits until the debt is repaid in full, to commence at the end of the three-month hardship period.

Customers experiencing homelessness

Branch staff at one Category A subscriber identified a customer as vulnerable and may be experiencing homelessness. While the customer is generally very reserved and reluctant to speak, one member of staff built up a rapport with him over time, earning his trust. Occasionally, the customer comes into the branch accompanied by another person who appears to have some influence over the customer's actions. The subscriber has engaged the police to perform welfare checks on the customer, who also suffers from a medical condition causing him to fit.

A Power of Attorney has been appointed for the customer; however, the Attorney refuses to involve themselves in the customer's finances. The subscriber has submitted two referrals to the Office of the Public Guardian (OPG), noting the customer lacks capacity and the Attorney is reluctant to help him. The subscriber's compliance office is assisting the OPG with its investigations and is hopeful these efforts will lead to appropriate support for the customer. In the meantime, the subscriber continues to provide a safe and supportive environment within its branch for the customer.

Suggested further reading

Much has been written about consumer vulnerability in recent years. The Committee encourages all Code subscribers to consider different resources as they decide how to define vulnerability, recognise the various risk factors, and respond to customers experiencing vulnerability. Here are a few of the papers and report that subscribers might find useful, in addition to the **new international standard ISO 22458,** which we recommend as providing much practical guidance on identifying and supporting consumers in vulnerable situations, as well as thinking about inclusive design of products and services.

Financial services specific vulnerability resources

Spotlight on customer vulnerability

Customer Owned Banking Association (COBA) and EY

www.customerownedbanking.asn.au/storage/Reports/Vulnerability/coba-report-spotlight-on-customer-vulnerability-december-2020-16074089710zN6V.pdf

Industry Guideline: Preventing & responding to family and domestic violence

Australia Banking Association (ABA)

www.ausbanking.org.au/wp-content/uploads/2021/03/ABA-Family-Domestic-Violence-Industry-Guideline.pdf

Insurance in Superannuation: Developing a vulnerable member policy

Association of Superannuation Funds of Australia (AFSA)

www.superannuation.asn.au/ArticleDocuments/265/BP_Vulnerable_Consumers_Paper_v3.pdf.aspx?Embed=Y

Cross-economy vulnerability resources

Exploring regulatory approaches to consumer vulnerability: A report for the Australian Energy Regulator

Consumer Policy Research Centre (CPRC)

https://cprc.org.au/wp-content/uploads/2021/12/Exploring-regulatory-approaches-to-consumer-vulnerability-A-CPRC-report-for-the-AER.pdf

Consumer vulnerability: A business guide to the Australian Consumer Law

Australian Competition & Consumer Commission (ACCC)

www.accc.gov.au/system/files/consumer-vulnerability.pdf

Vulnerability resources from UK financial services

Vulnerability Inclusion Handbook

Capital One UK

www.capitalone.co.uk/images/pdf/Vulnerability_Inclusion_Handbook.pdf

FG21/1 Guidance for firms on the fair treatment of vulnerable customers

Financial Conduct Authority (FCA)

www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf

Conclusion

Overall, the Committee is pleased with Code subscribers' commitment to identifying and responding to customers experiencing vulnerability. Many institutions suggested they have mature vulnerability frameworks in place. Although the current Code lacks any specific direction on how to manage vulnerability, it appears from the Inquiry's findings they are well on their way to meeting the more detailed vulnerability provisions in the 2022 Code.

Some subscribers provided examples relating to how they respond to customers experiencing elder abuse or domestic/family violence. The Committee would like to see all institutions sharpen their focus on providing better outcomes for these customers. This includes implementing specific documented policies and processes where possible and providing specialised staff training on dealing with these types of vulnerability.

Subscribers to the Code vary significantly in size, and there is no single right way to approach the new vulnerability requirements that will work for all of them. But it is important all think about how to define vulnerability and then put in place necessary policies, processes, resources, monitoring arrangements and governance. This can enable consistently identifying and responding to a diverse range of vulnerability risk factors.

Subscribers' Boards should take a more strategic and proactive role in relation to customers experiencing vulnerability, and banks should work with external support services and community organisations that can assist with a range of vulnerability issues (including how to respond to customers experiencing domestic/family violence).

As we approach the commencement date for the 2022 Code, the Committee will continue to monitor subscribers' compliance with the new vulnerability obligations. In the meantime, we encourage all Code-subscribing institutions to consider the findings and case studies contained in this report, as well as our suggested further reading and the practical guidance set out in the new international standard, ISO 22458.

Appendix 1: 2021 questionnaire regarding vulnerability

The following is the questionnaire which formed part of the 2021 Annual Compliance Statement (ACS) to inform the Committee how Code subscribers define vulnerability and deal with issues concerning domestic and family violence and elder abuse.

F.1 Does your institution define vulnerability? *[please select ONE only and provide details]*

- ☐ YES *[please provide details]*
- ☐ No *[please provide details]*
- ☐ In the process of/planning *[please provide details]*
- ☐ Other *[please provide details]*

F.2 Do you have specific policies and processes in place in relation to the following examples of vulnerability? *[please select ALL that apply]*

- ☐ Domestic/Family Violence
- ☐ Elder Abuse
- ☐ Mental Health illness
- ☐ Serious illness
- ☐ Disability (physical)
- ☐ English (second language)
- ☐ Unfamiliar with Banking Products and Financial Services
- ☐ Indigenous Australian and/or Torres Strait Islander
- ☐ Working together with financial counsellors, community representatives and/or other specialists *[please provide details]*
- ☐ Other *[please provide details]*

F.3 How do you identify vulnerability? *[please select ALL that apply and provide details]*

- ☐ Using in-house data (e.g. demographics) *[please provide details]*
- ☐ Using customer specific data (e.g. payment history, communication) *[please provide details]*
- ☐ Staff is trained to listen to what individual customers tell them and/or observe how they behave *[please provide details]*
- ☐ Customer self-identification *[please provide details]*
- ☐ Other *[please provide details]*

F.4 **Do you have a specific vulnerability team?** *[please select ONE only and provide details]*

- ☐ YES *[please provide details]*
- ☐ No *[please provide details]*
- ☐ In the process of/planning *[please provide details]*
- ☐ Other *[please provide details]*

F.5 **Do you provide training on vulnerability to all customer-facing staff?** *[please select ONE only and provide details]*

- ☐ YES *[please provide details]*
- ☐ No *[please provide details]*
- ☐ In the process of/planning *[please provide details]*
- ☐ Other *[please provide details]*

F.6 **Do you have any partnerships with community organisations etc who can provide you with expert support and advice on dealing with vulnerability?** *[please select ONE only and provide details]*

- ☐ YES *[please provide details]*
- ☐ No *[please provide details]*
- ☐ In the process of/planning *[please provide details]*
- ☐ Other *[please provide details]*

F.7 **Do you have a Power of Attorney process and/or policy?** *[please select ONE only and provide details]*

- ☐ YES *[please provide details]*
- ☐ No *[please provide details]*
- ☐ In the process of/planning *[please provide details]*
- ☐ Other *[please provide details]*

F.8 **Do you have a separate policy that specifically addresses elder abuse and/or is included in your family violence policy?** *[please select ONE only and provide details]*

- ☐ YES *[please provide details]*
- ☐ No *[please provide details]*
- ☐ In the process of/planning *[please provide details]*
- ☐ Other *[please provide details]*

F.9 Do you have any regular reporting process in place to your Board and/or executive team on matters regarding customers experiencing vulnerability? *[please select ONE only and provide details]*

- ☐ YES *[please provide details]*
- ☐ No *[please provide details]*
- ☐ In the process of/planning *[please provide details]*
- ☐ Other *[please provide details]*

F.10 Can you provide one example for how you identified and dealt with a vulnerable customer. *[please provide details]*

Appendix 2: 2021 data regarding vulnerability

The following tables reflect the data received via the 2021 questionnaire regarding vulnerability as shown in Appendix 1.

Categories of Code subscribers are defined by $amount in assets.

Table 1: Code subscribers by category and state as at 30 September 2021

$ amount in assets	*NSW*	*NT*	*Qld*	*SA*	*Tas*	*Vic*	*WA*	*Total*
Category AA[4] - Over $5b	2	-	2	2	-	1	1	**8**
Category A – Between $2b and $5b	3	-	2	-	-	2	-	**7**
Category B – Between $1b and $2b	6	-	-	2	1	2	-	**11**
Category C – Between $500m and $1b	5	-	2	-	-	1	-	**8**
Category D – Between $200m and $500m	7	-	2	-	-	2	-	**11**
Category E – Under $200m	5	1	-	1	-	5	-	**12**
Grand Total	**28**	**1**	**8**	**5**	**1**	**13**	**1**	**57**

Table 2: Does your institution define vulnerability? [Select one only]

	Cat AA	*Cat A*	*Cat B*	*Cat C*	*Cat D*	*Cat E*	*Total*
Yes	8	3	8	4	8	7	**38**
In process	**-**	2	3	3	3	5	**16**
No	**-**	1	**-**	1	**-**	**-**	**2**
Other	**-**	1	**-**	**-**	**-**	**-**	**1**

[4] Previously included in Category A Code subscribers.

Table 3: Do you have specific policies and processes in place in relation to the following examples of vulnerability? [Select all that apply]

	Cat AA	Cat A	Cat B	Cat C	Cat D	Cat E	Total
Domestic/Family Violence	4	4	9	2	9	6	**34**
Elder Abuse	5	3	9	2	11	6	**36**
Mental Health illness	4	2	6	-	10	5	**27**
Serious illness	3	3	6	-	3	3	**18**
Disability (physical)	4	3	6	-	8	4	**25**
English (second language)	2	4	4	1	4	3	**18**
Unfamiliar with Banking Products and Financial Services	1	2	3	-	3	3	**12**
Indigenous Australian and/or Torres Strait Islander	1	1	4	1	4	5	**16**
Working together with financial counsellors, community representatives and/or other specialists	-	1	3	4	-	3	**5**
Other	-	6	4	5	6	2	**7**

Table 4: How do you identify vulnerability? [Select all that apply]

	Cat AA	Cat A	Cat B	Cat C	Cat D	Cat E	Total
Using in-house data (e.g. demographics)	-	-	2	1	-	1	**4**
Using customer specific data (e.g. payment history, communication)	3	4	4	4	7	6	**28**
Staff is trained to listen to what individual customers	8	5	10	7	11	12	**53**

	Cat AA	Cat A	Cat B	Cat C	Cat D	Cat E	Total
tell them and/or observe how they behave							
Customer self-identification	8	4	5	4	8	5	**34**
Other	1	1	2	1	-	1	**6**

Table 5: Do you have a specific vulnerability team? [Select one only]

	Cat AA	Cat A	Cat B	Cat C	Cat D	Cat E	Total
Yes	1	2	1	2	2	3	**11**
In process	1	-	1	1	-	1	**4**
No	5	4	9	3	9	7	**37**
Other	1	1	-	2	-	1	**5**

Table 6: Do you provide training on vulnerability to all customer-facing staff? [Select one only]

	Cat AA	Cat A	Cat B	Cat C	Cat D	Cat E	Total
Yes	7	4	8	7	9	10	**45**
In process	1	1	2	1	2	2	**9**
No	-	2	1	-	-	-	**3**

Table 7: Do you have any partnerships with community organisations etc. who can provide you with expert support and advice on dealing with vulnerability? [Select one only]

	Cat AA	Cat A	Cat B	Cat C	Cat D	Cat E	Total
Yes	5	1	2	5	2	3	**18**
In process	2	1	-	-	-	-	**3**
No	--	4	7	2	9	7	**29**
Other	1	1	2	1	-	2	**7**

Table 8: Do you have a Power of Attorney process and/or policy? [Select one only]

	Cat AA	Cat A	Cat B	Cat C	Cat D	Cat E	Total
Yes	8	7	10	7	10	12	**54**
In process	-	-	1	1	-	-	**2**
Other	-	-	-	-	1	-	**1**

Table 9: Do you have a separate policy that specifically addresses elder abuse and/or is included in your family violence policy? [Select one only]

	Cat AA	Cat A	Cat B	Cat C	Cat D	Cat E	Total
Yes	3	1	2	1	2	-	**9**
In process	-	1	3	2	1	3	**10**
No	4	5	6	4	7	7	**33**
Other	1	-	-	1	1	2	**5**

Table 10: Do you have any regular reporting process in place to your Board and/or executive team on matters regarding customers experiencing vulnerability? [Select one only]

	Cat AA	Cat A	Cat B	Cat C	Cat D	Cat E	Total
Yes	-	2	3	1	3	6	**15**
In process	3	-	3	2	-	2	**10**
No	3	4	5	4	6	4	**26**
Other	2	1	-	1	2	-	**6**

Appendix 3: About the Code

The Code

The Customer Owned Banking Code of Practice (the Code) was developed by the Customer Owned Banking Association (COBA) and commenced operation on 1 January 2014. The Code replaces the 2010 Mutual Banking Code of Practice.

The Code has been revised to accommodate changes the Australian Securities and Investments Commission (ASIC) made to Regulatory Guide 221[5] *Facilitating digital financial services disclosures* and the *e-Payments Code*. The revised Code has been effective from 1 July 2016. A further update was published, effective 1 January 2018.

Through the Code, subscribing credit unions, mutual banks and mutual building societies voluntarily commit to fair and responsible customer owned banking.

Following a review starting in 2018, COBA developed a new Code which becomes effective 31 October 2022.

The Committee

The Code Compliance Committee (the Committee) is an independent compliance monitoring body established under the Code and the Code Compliance Committee Charter (the Charter). It comprises an independent chair, a person representing the interests of the customer owned banking sector and a person representing the interests of consumers and communities.

The purpose of the Committee is to monitor compliance with the Code. To achieve this, the Committee monitors Code compliance and shares recommendations for good practice, engages with stakeholders and analysis the external financial services' environment and ensures efficient and effective Committee operations.

The Compliance Manager

The Australian Financial Complaints Authority (AFCA) provides Code monitoring and administration services as Compliance Manager[6] to the Committee and COBA by agreement. AFCA has appointed a dedicated team of staff (Code Team) within its office to undertake that task.

For more information about the Code and the Committee, please visit www.cobccc.org.au.

Code subscribers

As of 30 April 2022, there are 56 Code subscribers.

For a list of current Code subscribers, please visit https://www.cobccc.org.au/code-of-practice/code-register/

[5] See https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-221-facilitating-digital-financial-services-disclosures/

[6] As per Customer Owned Banking Code Compliance Committee Charter section 4.4.

Customer Owned Banking Code Compliance Committee (COBCCC)

PO Box 14240 Melbourne VIC 8001

Email: info@codecompliance.org.au

Phone: 1800 931 678

www.cobccc.org.au

CUSTOMER OWNED BANKING
CODE COMPLIANCE COMMITTEE