



Submission by the
Financial Rights Legal Centre
Care Financial Counselling and Consumer Law Centre
Consumer Credit Legal Service (WA)

Australian Banking Association

Better Banking for Vulnerable Customers
March 2019

May 2019

About the Financial Rights Legal Centre

The Financial Rights Legal Centre is a community legal centre that specialises in helping consumers understand and enforce their financial rights, especially low income and otherwise marginalised or vulnerable consumers. We provide free and independent financial counselling, legal advice and representation to individuals about a broad range of financial issues. Financial Rights operates the National Debt Helpline, which helps NSW consumers experiencing financial difficulties. We also operate the Insurance Law Service which provides advice nationally to consumers about insurance claims and debts to insurance companies, and the Mob Strong Debt Help services which assist Aboriginal and Torres Strait Islander Peoples with credit, debt and insurance matters. Financial Rights took close to 25,000 calls for advice or assistance during the 2017/2018 financial year.

Financial Rights also conducts research and collects data from our extensive contact with consumers and the legal consumer protection framework to lobby for changes to law and industry practice for the benefit of consumers. We also provide extensive web-based resources, other education resources, workshops, presentations and media comment.

This submission is an example of how CLCs utilise the expertise gained from their client work and help give voice to their clients' experiences to contribute to improving laws and legal processes and prevent some problems from arising altogether.

For Financial Rights Legal Centre submissions and publications go to www.financialrights.org.au/submission/ or www.financialrights.org.au/publication/

Or sign up to our E-flyer at www.financialrights.org.au

National Debt Helpline 1800 007 007
Insurance Law Service 1300 663 464
Mob Strong Debt Help 1800 808 488

Monday – Friday 9.30am-4.30pm

About Care Financial Counselling Service and Consumer Law Centre

Care Financial Counselling and Consumer Law Centre has been the main provider of financial counselling and related services, for people on low to moderate incomes, in the ACT since 1983. Care's core service activities include the provision of information, advice, support and advocacy for people experiencing financial difficulty.

Care also provides a Community Development and Education program, makes policy comment on issues of importance to its client group and operates the ACT's first No Interest Loans Scheme, established in 1997. Care offers legal advice on credit, debt and fair trading matters through the Consumer Law Centre. Across Care's service delivery programs, the agency responds to over 2,000 new requests for assistance every year.

About Consumer Credit Legal Service (WA) Inc

CCLSWA is a not-for-profit specialist community legal centre based in the Perth metropolitan area. CCLSWA advises and advocates for consumers on consumer credit issues.

CCLSWA operates a free telephone advice line service which allows consumers to obtain information and legal advice in the areas of banking and finance. CCLSWA provides ongoing legal assistance to consumers by opening case files when the legal issues are complex and CCLSWA has capacity to do so. CCLSWA aims to create awareness, knowledge and understanding of consumer issues relating to financial services.

CCLSWA's mission is to strengthen the consumer voice in WA by advocating for, and educating people about, consumer and financial, rights and responsibilities.

Introduction

Thank you for the opportunity to comment on the *Every Customer Counts - Better banking for vulnerable customers* consultation paper on developing a new industry guideline (**the consultation paper**). This submission has been prepared by the Financial Rights Legal Centre (**Financial Rights**), Care Financial Counselling and Consumer Law Centre (**Care**), and the Consumer Credit Legal Service WA (**CCLSWA**) have endorsed this submission and concur with the concerns raised.

We are pleased that over recent years, many financial services businesses have recognised that an appropriate response to assist customers who are experiencing vulnerability goes further than financial hardship processes. More businesses are recognising that:

- many customers could be at risk of experiencing vulnerability, due to illness, loss of job, death of a partner, family violence or other personal circumstances;
- risks to customers experiencing vulnerability can arise due to product design and business processes, so should be considered when developing new products and communications channels;
- many customers will not proactively disclose to their bank if they are experiencing things like family violence, elder abuse, mental ill-health, gambling or other circumstances, however there may be indicators of these issues that can be attained through data analysis and appropriate staff training; and that
- tailored, individual responses are often required for these customers: for example, some institutions have introduced a flag on their IT system indicating that family violence may be occurring, so that additional protections or safeguards are applied to private information.

A new Guideline must recognise that vulnerability is a very broad concept. Given the wide array of factors that can contribute to a person's temporary, permanent, situational or sporadic vulnerability, virtually any customer at some point in time during their relationship with their bank could feasibly experience some form of vulnerability that impacts upon the relationship with the bank.

Banks must fully acknowledge the role they can themselves play in creating and maintaining customer vulnerability through inappropriate product and service design. This understanding of vulnerability should result in significant shifts on the part of banks. Addressing vulnerability is not just introducing training for frontline staff and developing appropriate specific processes to assist several specific subsets of vulnerable customer, but involves making fundamental cultural and practical changes so as to make addressing the needs of people experiencing vulnerability part of banks' core business.

Responding appropriately to these complex issues requires a comprehensive guideline and a firm commitment on the part of ABA members to meet these standards. The ABA should investigate which parts of the planned Guideline are appropriate to be referenced or even duplicated in the Banking Code and made enforceable.

Recommendations

Guiding Principles

1. Financial Rights generally supports the proposed Guiding Principles, and recommends the principles must be reflected throughout the entirety of the Guideline.
2. Relevant sections of the Guiding Principles should be incorporated as enforceable provisions of the Code.
3. Financial Rights recommends an additional principle under the “Trust and confidence” section: “we will work with you with empathy, and with consideration of your particular needs”

Definition of vulnerability

4. The Guideline should address a broad range of demographic factors that can feed into financial exclusion and vulnerability, including but not limited to work status, age, gender, geographic location, language, Aboriginal and/or Torres Strait Islander status, disability, addiction, and homelessness.
5. The Guideline should set out the need for banks to take a flexible, broad approach to vulnerability rather than a strict step-by-step check-box system for assisting people who fit within various categories of vulnerability.
6. The Guideline should recognise the role that banks often play themselves in creating and maintaining customer vulnerability.
7. Rather than defining the term “extra care”, the Guideline should provide several examples of what extra care might constitute, and stipulate that these options are not exhaustive.
8. The Guideline should refer to “people experiencing vulnerability” rather than “vulnerable customers”.

Communicating with customers

9. Financial Rights supports the proposal that the Guideline should commit banks to make available an easy to understand explanation of their commitment to customers experiencing vulnerability.
10. The easy to understand explanation of banks’ commitments to customers experiencing vulnerability must be made available in banks’ branches and on their websites, as well as discussed directly with customers by bank staff.
11. The explanation cover page should consist of a clear one-pager containing all of the most vital information, and a phone number for customers to call for further information relating to vulnerability.
12. The explanation should include examples of steps banks must take in response to vulnerability, both in terms of product design, and in terms of direct assistance to individuals who are indicated as experiencing some form of vulnerability.

Product and service design

13. Financial Rights recommends that the Guideline should incorporate practical measures for considering people experiencing vulnerability in product design.
14. Banks should be obliged to identify a series of vulnerable groups of people and consumer-test all new products with a variety of types of customers.
15. All banking terms and conditions should be straightforward, easy to understand and not misleading.
16. Banks must audit all current products and processes to assess their suitability for customers experiencing vulnerability, and whether or not those products and processes would cause further harm to a customer experiencing vulnerability.

Identifying vulnerable customers, data analysis and privacy

17. The Guideline should include the principle:

If a bank collects any information relating to a customer's vulnerability, that information should not be used to discriminate against that customer or used in a way that causes them detriment. Similarly, it is important that any data gathered about customers' vulnerability is not used for direct marketing purposes or primarily for banks' own financial gain.

18. Banks should ask customers a series of questions relating to indicators of potential vulnerability and needs, including an open-ended question asking of any further specific needs:

"Is there anything else that we should know about you to help us give you appropriate services and support?"

Do you, for example:

- *require an assistance animal to accompany you to our branches;*
 - *require Auslan or other interpretation;*
 - *have a mental illness or addiction and require blocks on certain retailers or maximum daily limits?"*
19. Banks should deploy data analysis techniques to pick up on indicators of potential vulnerability or need and initiate more appropriate services to meet those needs. In the rare case where there is a requirement to raise the issue directly with a customer this should always be done so with the utmost care, tact and empathy.
 20. Customer vulnerability information should, as far as possible, be recorded in banks' systems in terms of customers' specific needs rather than the type of vulnerability that they are experiencing.
 21. Customers should be able to give or withdraw consent for their data to be stored and used at any time.
 22. Banks must have a written policy on personal information to ensure a clear and consistent approach, which should be communicated to staff, who should be trained to explain it to customers.
 23. Banks should never, even with customer consent, share customer vulnerability information to other financial service providers.

24. Systems should be adopted to ensure that notes relating to the needs of people experiencing vulnerability are most useful, by compelling bank staff to actually read all vulnerability notes and flags in customers' files prior to and/or during each interaction with that customer.
25. Information relating to vulnerability should be recorded with the knowledge that any customer can request to access and read any notes on them taken by the bank, at any time.
26. Banks should be compelled to work collaboratively rather than competitively, towards a best practice approach to balance privacy and protection of customers experiencing vulnerability.

Staff training

27. Financial Rights supports the inclusion of the proposed staff training provisions in the Guideline.
28. Training on vulnerability for bank staff must be broad, comprehensive and flexible, so as to fully equip staff to make appropriate choices outside of a uniform check-box approach.
29. Training on vulnerability must be provided from the Board down, to every staff member, in banks, so as to imbue an understanding of vulnerability throughout organisational culture.
30. The Guideline should specifically require that all staff undertake regular cultural safety training.
31. The Guideline should require that all customer-facing staff receive training in trauma-informed customer engagement and in vicarious trauma.
32. The Guideline should require that banks will have employee assistance programs in order to adequately support staff impacted by vicarious trauma.

Formal arrangements

33. Financial Rights endorses the positions taken in the submission by the Consumer Credit Legal Service WA regarding the recommendations of the Australian Law Reform Commission.
34. Financial Rights supports all suggested inclusions relating to third party authorisation forms in the Guideline.
35. Third party authorisation forms should explicitly ask how long the authorisation should stand for, and in cases where the duration of the authorisation is longer than six months, how often the bank should check back in with the customer.
36. The Guideline should stipulate that where there is uncertainty relating to a third party authorisation, the bank must contact the customer directly.
37. All third party authorisation forms should be customisable; customers should be empowered to specify which authorisations they wish to provide to a third party.
38. Third party authorisations must, where possible, require a face to face meeting between the bank and the customer, including ensuring that there can be private communication between the bank and the customer.

Unsecured debt and collections

39. Financial Rights supports the inclusion of collections arrangements in the Guideline.
40. Financial Rights supports the expansion of existing arrangements for customers who are victims of domestic violence to customers experiencing other forms of abuse where the debt is related to the abuse.

41. Financial Rights recommends the adoption the general principle:

if a customer's vulnerability caused a debt to be incurred, that vulnerability is ongoing, and/or there is no prospect of the money being recovered, then the bank should not sell that debt to a collections agency.

42. The Guideline should stipulate, and the Code should make enforceable, that all collections agencies engaged by banks must be committed to familiarity and compliance with the Guideline.

Scams

43. Financial Rights supports including industry level guidance on preventing scams in the Guideline.

44. In order to prevent scams, banks should be obliged to do far more checking in with customers relating to any transactions that appear unusual.

45. The Guideline should include a comprehensive step-by-step guideline for banks to assist customers that have been victims of fraud to recover.

1. Guiding Principles

Do you agree with our proposal to use these Guiding Principles to underpin the Guideline?

Financial Rights generally supports these guiding principles. However, we believe in order for guiding principles to carry weight they must be reflected throughout the entire Guideline, with relevant enforceable sections incorporated in the Banking Code. If these guiding principles are not adequately reflected throughout the Guideline or in part in the Code, then there is the potential that they merely function to promise vulnerable consumers a level of protection that in reality they may not be provided.

Under the “Trust and confidence” section of the Guiding Principles, we suggest the addition of a principle along the lines of “we will work with you with empathy, and with consideration of your particular needs”.

Recommendations

1. Financial Rights generally supports the proposed Guiding Principles, and recommends the principles must be reflected throughout the entirety of the Guideline.
 2. Relevant sections of the Guiding Principles should be incorporated as enforceable provisions of the Code.
 3. Financial Rights recommends an additional principle under the “Trust and confidence” section: “we will work with you with empathy, and with consideration of your particular needs”
-

2. Definition of vulnerability

Are there additional issues relating to ‘vulnerability’ that should be considered in defining the concept of vulnerability? Note, we encourage stakeholders to provide examples and case studies that assist interpretation.

Vulnerability is a very broad concept and can impact virtually anybody at any time

The discussion paper states that:

“Anyone can be vulnerable and vulnerability can be temporary, permanent or situational.”

This is an important point and one that we believe must underpin banks’ understandings of vulnerability.

Financial Rights recognises the broad scope of the term ‘vulnerability’, and posit that a large proportion of any given bank’s customers in a given period could feasibly experience vulnerability. As such, banks should acknowledge that approaching and addressing vulnerability is a project larger than having processes in place to deal with specific circumstances of vulnerability as they arise. Addressing vulnerability requires that banks rethink their core culture and practices, to account for the impact that their products and processes may have for people experiencing a wide variety of forms of vulnerability.

Factors driving vulnerability and financial exclusion

The current examples of circumstances that may indicate vulnerability provided in the Banking Code include:

- *“age-related impairment;*
- *cognitive impairment;*
- *elder abuse;*
- *family or domestic violence;*
- *financial abuse;*
- *mental illness;*
- *serious illness; or*
- *any other personal, or financial, circumstance causing significant detriment.”*

This recognises a range of vulnerable circumstances, across the temporary, permanent or situational spectrum, and some of which could impact anyone in the population. However, in our view this does not sufficiently address demographic factors which feed into systemic financial exclusion and which by extension can drive vulnerability in engagements with finance institutions.

Some such demographic factors include:

- *Work status:* People who are looking for work, working part-time, unemployed students or undertaking home duties make up a substantial proportion of those who are financially excluded. However, nearly a quarter of those who are financially excluded are employed full-time and can be classified as the ‘working poor’. This highlights a need for more appropriate products for full-time employed people who may not be eligible for current mainstream financial products due to low income or other factors.
- *Age:* There should be reference to both older people and younger people. We note that the consultation paper references “age-related impairment” and “elder abuse”, both of which are important for ABA members to take into account. However, younger people aged 18-24 make up 36% of the financially excluded population in Australia, and yet there is not a broad, consistent approach to providing financial products and services specifically targeted at that demographic.
- *Gender:* Due to the gender pay gap, women are on lower incomes than men, particularly those women whose only or primary work is unpaid domestic labour. A 2016 study into

women and payday lending indicated that women are increasingly seeking payday loans, with a 110 per cent rise since 2005. This rise is greatest for women in family groups. Further, women are more likely to experience financial abuse. We note that the Code references both “family or domestic violence” and “financial abuse”, both of which greatly intersect with gender. However, there should be recognition of gender as a factor in financial exclusion even aside from the issues of family/domestic violence and financial abuse.

- *Geographic distance*: Remote, regional and rural areas can all lack access to appropriate financial services due to distance: they both are far less likely to have bank branches, and are far more likely to have poorer phone and internet connectivity.
- *Language*: Language barriers to financial inclusion in Australia remain significant. Recent research into the use of pay day loans shows a significant growth in first or second generation migrants to Australia with English as a second language.
- *Aboriginal and/or Torres Strait Islander status*: Aboriginal and Torres Strait Islander peoples are marginalised as a result of structural racism with respect to health, housing, education, employment and contact with the criminal justice system. Aboriginal and Torres Strait Islander peoples face significant disadvantages that other demographics within the Australian community do not experience. Financial exclusion can be significant for Aboriginal and Torres Strait Islander people and communities, not just in remote communities but also in regional and rural areas, in towns and in major cities.
- *Disability*: People with various types of disability have a wide range of specific needs, and may experience financial exclusion in various forms. In our experience, there are many customer-owned banks that have nothing formal in place to assist deaf people or people with cognitive impairments to communicate. In our experience, appropriate assistance for such customers is often ad hoc, and may simply be a case of whether or not the bank happens to have an employee who speaks Australian Sign Language or is appropriately trained to communicate in a clear and respectful manner with customers with a cognitive disability.
- *Addiction*: Customers with addictions to gambling and alcohol are also vulnerable to significant financial hardship. The accounts of such customers will generally have clear markers indicating such addictions, meaning that customer owned banks can be well-placed to identify customers experiencing these problems and take steps to assist them where appropriate. We note that “mental illness” is already referenced in the Code, and that addiction can be a form of, or a symptom of, mental illness, however we believe that addiction should be explicitly referred to.
- *Carers*: Customers who provide unpaid care work to family members have a specific set of needs that banks should work to address. For instance, they may be far more time-poor than other customers, they may be more financially strained, and they may be managing multiple people’s bank accounts.
- *Bereavement*: Customers who have recently lost their spouse may be vulnerable both due to grief and its impacts, and due to the financial cost that can be incurred through

the potential loss of a second income, through having to pay for funerals and more. This is a type of situational and generally temporary vulnerability that impacts a huge number of banking customers.

- *Homelessness*: If a customer is homeless or at risk of homelessness, this is an indicator of, and driver of, significant vulnerability.

It is important that both the Banking Code and the Guideline is updated to account for these additional factors as potential drivers of vulnerability.

We note that several of the demographic factors discussed above can present as temporary, situational or permanent: for instance, addiction can be one person's lifelong vulnerability, while can be another's situational, temporary response to a particular stressor. This points to the need for flexible, individual needs-based approaches rather than a one-size-fits-all approach to customers flagged as experiencing a certain type of vulnerability.

Accounting for some of these additional factors will require a broader-brush approach on the part of banks than for the more specific, often temporary or situational factors such as domestic and family violence, or elder abuse. Fully appreciating and working to overcome financial exclusion – for instance, acknowledging the gendered, geographic or age-based patterns in financial exclusion – requires broad cultural and practical shifts on the part of finance institutions. Banks and all banking staff must become far more attuned to the factors that drive financial exclusion for various demographics; this must become a core part of mandatory staff training related to vulnerability.

Banks' role in detriment to people experiencing vulnerability

Part of the Financial Conduct Authority UK's (FCA's) definition of "vulnerable customer" is acknowledgement of the potential role of financial institutions in exacerbating detriment to vulnerable consumers. The FCA definition reads:

*"A vulnerable consumer is someone who, due to their personal circumstances, is especially susceptible to detriment, particularly when a firm is not acting with appropriate levels of care."*¹

This is referenced in the consultation paper:

"It is not the role of the bank to solve a customer's underlying problem however banks acknowledge our actions can contribute to customer circumstances."

The FCA Occasional Paper 8: Vulnerability states:

"Vulnerability is not just to do with the situation of the consumer. It can be caused or exacerbated by the actions or processes of firms. The impact of vulnerability is strong and many people are trying to cope with difficult situations and limited resources, energy and time. Stress can affect state of mind and the ability to manage effectively. In such conditions, being confronted by a complex telephone menu system that gives no option of talking to a person; a 'computer says no' response; a call handler without time or inclination to listen, or a system that fails to record what may be distressing circumstances and forces the customer to

¹ FCA, Occasional Paper No.8, Consumer Vulnerability, February 2015

repeat themselves at every point of contact, can all create a spiral of stress and difficulty, resulting in detriment.”²

It is important that any Guideline relating to vulnerability in the Australian context has a similar or stronger understanding of the role that financial institutions themselves can play in consumer detriment. The recent Royal Commission has uncovered rampant misconduct and mistreatment of consumers, including vulnerable consumers. This misconduct is a symptom of an underlying malaise that has gripped the entire finance industry, in particular our large and previously trusted institutions such as the banks. This has come about as a result of a fundamental shift from an individual customer service based industry, with strong public accountability including in some cases public ownership, to a private profit-based sales culture which focuses on products and portfolios.

To fully address the detriment to vulnerable consumers that can arise as a result of banks’ own conduct will require more than specific guidelines around assisting customers experiencing certain types of vulnerability: it will require comprehensive cultural and practical shifts and a value-realignment to prioritising customer wellbeing over profits.

Two-pronged approach to, and understanding of, vulnerability

We see a holistic approach to addressing customer vulnerability as requiring two prongs:

1. Changes to banks’ products and processes so as to both account for people experiencing various forms of vulnerability or financial exclusion, and reduce the extent to which banks themselves create and maintain customer vulnerability.
2. The adoption of additional, flexible, staff training and processes to better assist people experiencing certain specific forms of vulnerability.

Are there other terms in this context which you think would benefit from an agreed definition, for example “extra care”?

Rather than defining terms such as “extra care”, the Guideline should provide several examples of steps banks could potentially take to assist customers in certain circumstances, which may constitute extra care. Definitions have the potential to become restrictive or prescriptive, and can at times offer loopholes to banks not to act. The commitments within the Guideline, such as to take “extra care” should remain broad.

The Guideline should include examples of both

- product design steps that they will take in order to not cause harm to customers experiencing vulnerability (discussed further below in section 4), and
- steps they will take in response to customer disclosure of, or red flags of, vulnerability factors such as family violence or elder abuse (discussed further below in section 5).

² Financial Conduct Authority, *Occasional Paper No. 8 Consumer Vulnerability*, February 2015.

The Guideline should stipulate explicitly that these examples are not exhaustive and that banks should be consistently developing processes for assisting customers experiencing vulnerability.

For example, a suite of potential protections constituting “extra care” for a customer experiencing family violence could include:

- increasing protections around her contact data such that her abusive partner or ex partner cannot find her;
- not contacting her via phone or at certain hours of the day;
- extending hardship arrangements;
- never asking her to obtain information, documents or other evidence from her abusive partner; and/or
- assisting her to sever joint accounts.

Should the ABA change the term ‘vulnerable customer’ in the Code, and other industry guidance, and if so, what expression or term is preferred by stakeholders?

‘People experiencing vulnerability’ is superior to ‘vulnerable customers’ for several reasons:

1. Banks should have in place processes and staff training to accommodate and support people experiencing vulnerability even before they become a customer of that bank. Banks should be cognizant of vulnerability for prospective customers.
2. This alternative phrasing emphasises that people experiencing vulnerability are people first and foremost, who happen to be in difficult circumstances, be those circumstances permanent, sporadic or temporary.

Recommendations

4. The Guideline should address a broad range of demographic factors that can feed into financial exclusion and vulnerability, including but not limited to work status, age, gender, geographic location, language, Aboriginal and/or Torres Strait Islander status, disability, addiction, and homelessness.
5. The Guideline should set out the need for banks to take a flexible, broad approach to vulnerability rather than a strict step-by-step check-box system for assisting people who fit within various categories of vulnerability.
6. The Guideline should recognise the role that banks often play themselves in creating and maintaining customer vulnerability.
7. Rather than defining the term “extra care”, the Guideline should provide several examples of what extra care might constitute, and stipulate that these options are not exhaustive.
8. The Guideline should refer to “people experiencing vulnerability” rather than “vulnerable customers”.

3. Communicating with customers

Do you support the proposal that the Guideline should commit banks to make available an easy to understand explanation of their commitment to vulnerable customers? Do you have any additional suggestions about what else this explanation should include? What practical measures or examples should be included in the explanation?

Any Guideline is only as useful as the extent to which it is understood and followed. Regardless of any actual commitments made to customers in a vulnerable customer guideline, in order for it to be effective it must be accessible and comprehensible by customers experiencing vulnerability. Financial Rights supports the inclusion of an obligation that banks write, make available and promote an easy to understand explanation of their various commitments to customers experiencing vulnerability.

While it is important that an easily understandable explanation of the commitments within this Guideline is made available in bank branches and on banks' websites, the onus should not be solely on the customer to proactively seek out this information. There should be an obligation on the part of banks to provide this information verbally. Bank staff should be obliged to inform a new or prospective customer about the Guideline, give a very brief rundown of the types of commitments contained within it, and hand them the brochure explaining the commitments within the Guideline, rather than simply having copies of the explanation brochure available in branches for customers to pick up themselves.

The explanation should include a cover page that sets out the most core vital information in a clear one-pager: what vulnerability is, how understanding the Guideline would be useful to the customer, and a phone number for someone who can answer any customer questions about vulnerability.

This explanation should then broadly and in plain English set out the products, processes and services available to customers experiencing various types of vulnerability, including but not limited to:

- particular products such as basic bank accounts,
- hardship arrangements and variations,
- examples of specific protections available for customers in situations such as family violence, addiction, or elder abuse.

As discussed above in section 2, the Guideline itself should include examples of steps banks must take in response to vulnerability, both in terms of product design, and in terms of in response to indicators or disclosure of particular vulnerabilities. Some of these should be replicated in communications to customers about the obligations contained within the

Guideline. At least one example of an appropriate approach on the part of banks under each of these categories should be included in communications to customers about the Guideline.

Recommendations

9. Financial Rights supports the proposal that the Guideline should commit banks to make available an easy to understand explanation of their commitment to customers experiencing vulnerability.
10. The easy to understand explanation of banks' commitments to customers experiencing vulnerability must be made available in banks' branches and on their websites, as well as discussed directly with customers by bank staff.
11. The explanation cover page should consist of a clear one-pager containing all of the most vital information, and a phone number for customers to call for further information relating to vulnerability.
12. The explanation should include examples of steps banks must take in response to vulnerability, both in terms of product design, and in terms of direct assistance to individuals who are indicated as experiencing some form of vulnerability.

4. Product and service design

Do you think practical measures for considering vulnerable customers in product design should be incorporated in the Guideline? If yes, do you have any suggestions about what these measures could be? Do you have examples of banking product design that means the needs of vulnerable customers are not met / and or have contributed to a customer experiencing vulnerability?

Financial Rights recommends that the Guideline should incorporate practical measures for considering customers experiencing vulnerability in product design. People experiencing vulnerability are not a small subset of customers that the bank can simply tweak behaviours to account for. Almost any person could at some point in their life, and in their relationship with their bank, be in vulnerable circumstances. This means that all products and services should be designed in such a way as to not harm, and to be appropriate for, people experiencing vulnerability.

Two fundamental problems cause banking products to be either inappropriate for, or actively harmful for, people experiencing vulnerability. The first of these is that banks will often design products without the customer as first priority: the profit motive comes before the genuine needs and best interests of customers. The second of these is that when banks design products with customers in mind, the customers that they design products, processes and service styles

for are generally comfortably employed, middle-class, able-bodied white men in metropolitan areas.

It is vital that banks design products, processes and service styles for the broad diversity of customers and potential customers. In order to do this, consumer testing for all new products must involve consumers of a variety of backgrounds. Banks should be obliged to identify a series of vulnerable groups of people and consumer-test all new products with a variety of types of customers. For instance, products should undertake consumer testing specifically to gauge whether or not they will be appropriate for, and whether or not they will be harmful for, customers struggling with addiction, or customers living in remote communities.

Another element in appropriate product design is broad staff training relating to vulnerability. It is important that any staff training relating to vulnerability is not limited to frontline customer service staff but is provided from the board down to every staff member, such that much-needed cultural shifts can occur throughout the banks. This includes staff training for all staff involved in designing products. We discuss staff training more comprehensively below in section 6.

Financial Rights have identified many banking products that clearly were not designed with catering for customer vulnerability in mind. In our view, many of the problematic products and processes discussed below should not have been designed, and potentially would not have been designed if the principle of product design with vulnerable consumers in mind had been followed.

- *Albert machines*: Several years ago, Commonwealth bank introduced a new type of eftpos terminal with a touch screen. This machine was clearly not designed with the needs of some types of people experiencing vulnerability in mind: the machine is close to entirely unusable by blind customers. These customers at the point of purchase are backed into a corner where they can either forego purchasing the items, or disclose their pin code to another person. This is clearly deeply inappropriate. Consumer testing of this product with various demographics of customers could have avoided this.
- *Inaccessible ATMs*: There are still many ATMs that are not accessible for people with various types of vulnerabilities – due to their height, lack of facility for blind customers, or other reasons. There are also some remote communities where customers need to enter a pub in order to access an ATM – this can make them inaccessible for customers under 18, or for alcoholics who must avoid establishments that serve alcohol.
- *Bank branch privacy*: We know of many branches where customers are not provided a private place to make phone calls or have sensitive conversations. If, for instance, a customer comes into a branch with a concierge (a style of bank that is more and more common) and reveals they are in financial hardship and having trouble making their credit card repayments, bank staff have advised them to make a phone call in the open space of the branch to a bank representative. They are not provided with a private place to make that call. This then leaves a vulnerable customer even more vulnerable, without the privacy to which they should be entitled when discussing their personal financial hardship. Branches should put resources into making their spaces and processes friendly and inclusive, including providing privacy.

- *Arranging or cancelling direct debits:* Financial Rights hear of consumers having difficulty with accessing and implementing basic functions on their credit cards. The ANZ's Frequent Flyer Black credit card, as an example, automates most elements of the card, however in order to set up, amend or cancel a direct debit the customer is required to print out a paper form, fill it out by hand and then fax it to the credit card provider. This is an obvious obstacle put in place where it should not be. It is inappropriate that some elements of a credit product – largely which benefit the bank, such as increasing credit limits, or opening new accounts - can be implemented entirely online, while other things that feasibly could be automated, are made deliberately difficult for the consumer.
- *Fee structures:* Fees can have harsh and disproportionate impacts upon lower income customers. A \$40 default fee for a consumer on Newstart earning less than \$14,000 per year equates to approximately 7.6 per cent of their fortnightly income; the same fee for someone earning an \$80,000 annual income is just 1.3 per cent of their fortnightly income. Fees can have little deterrence value where the consumer's problem is not disorganization but insufficient funds. Many fees are regressive, and are both incurred more often by consumers who are struggling, and impact on those customers more than on other customers due to the size of the fee in relation to their income.
- *High interest credit accounts:* We have had many low income, vulnerable clients that have been in inappropriate, high interest accounts. It should never be the case that a banking customer is caught in a cycle of only ever being able to pay interest and never make headway on paying down the actual debt.
- *Term deposits:* The fact that term deposits can renew automatically to less favourable terms is inappropriate and can be detrimental to customers.
- *Joint accounts:* There is potential for significant harm from some joint account setups, when domestic violence arises – particularly in terms of granting one account holder information relating to the other account holder. All joint accounts should be designed with consideration of the implication of that account should domestic violence arise between the account-holders.

The FCA has recommended in the UK context that banks should audit existing products and practices to see if they meet the needs of people in a range of vulnerable circumstances, ensure that those products and practices would not cause harm to a customer in vulnerable circumstances, and evaluate whether their policies around fair treatment are actually implemented by frontline staff.³ Financial Rights supports a similar requirement for banks here in Australia, and for this to be stipulated in the Guideline.

³ Financial Conduct Authority, *Consumer Vulnerability*, Occasional Paper No. 8, February 2015, p. 45.

Terms and conditions

Even consumers with good levels of literacy can struggle to understand contractual terms for a lot of financial products. Research conducted by the **FCA** in the UK has identified confusion as an early warning indicator of bias leading to potential consumer mistakes and detriment.

“If consumers with particular biases are vulnerable to specific product features or sales tactics, it is possible for firms to exploit this to increase profits. This research notes that behavioural biases can affect how consumers react to information.

Research (Consumer Focus, 2011) has found that degree-level education was necessary to understand a high street bank’s loan agreement and PhD level in order to understand payment protection insurance details.⁴ Other research (Which?, 2012) has criticised the time it would take consumers to read the terms and conditions of standard bank accounts for the main providers.⁵

The FCA’s research revealed that a very common characteristic of feeling vulnerable is ‘having your mind elsewhere’. When people have to deal with pressing and difficult issues in their life, they have less capacity to dedicate time and energy to navigate complex products and processes, and lengthy or complex information. Consumers with low levels of financial literacy, with mental health issues and learning disabilities are particularly at risk. This is an issue that faces all consumers. Dealing with complex financial information is therefore particularly problematic and increases the risk of detriment.”⁶

It is vital that as part of banks’ commitment to making products suitable and fair, they ensure that the terms and conditions attached to *all* products are straightforward, easy to understand and not misleading.

Case study – Anna’s story

Anna is living in a women’s refuge in South Australia. She is from Pipalyatjara in the APY lands; English is her second language with Pitjantjatjara as her first language. She is a single mother and suffers from depression and anxiety. In 2015 it is alleged she entered into a

⁴ Consumer Focus response to HM Treasury on the Draft Financial Services Bill, September 2011: “Compounding this lack of basic understanding is the complex nature of many financial product contracts despite years of effort by regulators to improve disclosure. Three examples: the consumer documentation from a major high street bank for a personal loan requires degree level education to understand; the standard text describing a PPI product requires PhD level education to comprehend; and it takes 55 minutes to read a standard consumer credit agreement, let alone understand it. It would therefore be unreasonable to argue that where a consumer has failed to fully read through and fully understand a complete set of terms and conditions they should automatically receive a lower level of protection. Problems of this kind were for example behind the recent Payment Protection Insurance scandal.”

⁵ “Only one in ten Which? members surveyed told us they had read their bank’s T&Cs thoroughly when they opened their account, which is unsurprising when our research suggests it would typically take between 25 minutes and over an hour and a half to read a set of terms and conditions from the ten major banks”.

⁶ Financial Conduct Authority, *Consumer Vulnerability*, Occasional Paper No. 8, February 2015, p. 45.

contract for funeral insurance, with direct debits of \$34.42 per fortnight.

Anna could not afford this; the insurance provider made 17 dishonoured direct debits, incurring bank fees each time. After the School Kids Bonus was deposited in Anna's account, the insurer deducted \$590.56. She had also at this stage incurred \$127 in fees from her bank.

Financial Rights raised a dispute with the insurer and sought a refund of the premiums taken. They were refunded. Financial Rights also sought a refund of the dishonor fees after raising a complaint that the bank:

1. applied its policies and/or its discretion inconsistently in allowing Anna's account to become overdrawn by direct debit entries in a way that amounts to maladministration;
2. used Anna's protected Australian Government payments to clear these unarranged overdrafts, including at times taking more than 10 per cent of these payments contrary to the Department of Human Services Code of Operation; and
3. failed to cancel direct debits by an Insurer from our Anne's account after being advised that Anna did not authorise these payments, contrary to the PDS and its obligations under the Code of Banking Practice.

The bank did not admit wrong doing and refunded on a good will basis.

Source: Financial Rights Legal Centre

Case study – Peter's story

Peter is a 46 year old Aboriginal man living in regional Western Australia. He is homeless and regularly travels between towns in WA. Peter's case worker contacted the Financial Rights Mob Strong Debt Help Peter's was refused a bank account by all the banks in his local area. The Banks in his area believed Peter had "behavioural issues." Peter has substance abuse issues.

Without a bank account, Peter is unable to access his finances. Peter is forced to go to Centrelink on a daily basis to obtain a debit card of \$40. He has not got full access to his Centrelink payments. The situation is akin to a guardianship order without a court order in place to do so.

Peter remains in limbo. He is unable to purchase groceries and unable to save to work his way out of homelessness.

Source: Financial Rights Legal Centre

Recommendations

13. Financial Rights recommends that the Guideline should incorporate practical measures for considering people experiencing vulnerability in product design.
 14. Banks should be obliged to identify a series of vulnerable groups of people and consumer-test all new products with a variety of types of customers.
 15. All banking terms and conditions should be straightforward, easy to understand and not misleading.
 16. Banks must audit all current products and processes to assess their suitability for customers experiencing vulnerability, and whether or not those products and processes would cause further harm to a customer experiencing vulnerability.
-

5. Identifying vulnerable customers, data analysis and privacy

Where a customer is identified as potentially being vulnerable, what actions should banks take (i.e. what would constitute “extra care”)? What ethical and privacy issues should banks consider where deploying data analysis techniques to proactively identify customers who may be vulnerable?

Should banks, with the explicit permission of customers, record information about vulnerability that banks discover or customers disclose in their internal records e.g. through flags / notes in the internal bank system? If yes, what kind of information should be collected and how should it be used? How should banks balance the desire to support customers fully and ensure they don’t have to repeat their story, with the customer’s right to privacy? Should banks take more active steps to seek personal information from customers, such as whether they are Indigenous or receive Government support payments? Are there any other questions banks should ask customers when they open an account to assess if they may be at risk of being vulnerable? Are there any further measures or principles which should be included in the Guideline with respect to data collection?

Issues surrounding vulnerability are complex and nuanced; vulnerabilities can overlap with one another and it is impossible to put in place a totally prescriptive approach for flagging and responding to vulnerability. Data collection and use is a fraught area, and we acknowledge that balancing customer protection and privacy is a difficult endeavour.

We recommend the following principles be supported:

If a bank collects or identifies any information relating to a customer's vulnerability or needs, that information should not be used to discriminate against that customer or used in any way that causes them detriment.

Similarly, it is important that any data gathered about customers' vulnerability is not used for direct marketing purposes or primarily for banks' own financial gain.

We understand that this is not straightforward: if a customer attempts to apply for a joint home loan with her partner and is denied on the basis that data analysis has indicated that she is potentially experiencing domestic violence, this may constitute discrimination and – particularly if the data analysis was wrong – could cause her detriment. However, we believe the principle outlined above is a good starting point to ground the discussion of the balance between customer protection and privacy.

Identifying customers who may be experiencing vulnerability or who have certain needs should involve both direct data collection from customers (i.e. asking questions), and deploying data analysis techniques for indicators of certain needs.

Gathering vulnerability information: asking questions

Financial Rights is aware of a common misconception that questions relating to Aboriginal or Torres Strait Islander status, whether or not a customer receives a government payment, or other questions relating to vulnerability, cannot or should not be asked by banks.

We disagree with this sentiment, and believe that banks absolutely must explicitly ask questions relating to vulnerability. Customers are within their rights to refuse to answer, but banks should be asking these questions. Along with specific questions relating to types of vulnerabilities or needs that customers might have, there should be a general open-ended question along the lines of:

"Is there anything else that we should know about you to help us give you appropriate services and support?"

Do you, for example:

- *require an assistance animal to accompany you to our branches;*
- *require Auslan or other interpretation;*
- *have a mental illness or addiction and require blocks on certain retailers or maximum daily limits?"*

This open-ended question should prompt customers to share other specific needs they may have with their bank, and the bank should be obliged to accommodate these needs as far as possible.

Gathering vulnerability information: data analysis

While we believe that banks must ask questions relating to vulnerability so as to gather as much information as possible directly from customers, we also acknowledge that it is unreasonable to assume that customers will always self-disclose vulnerability.

Many customers are themselves unaware of their “vulnerable” status or are unable to articulate their unique needs. Many more, for a variety of reasons, are extremely hesitant to mention their vulnerability. Vulnerability is often shown to financial institutions through a range of subtle hints or indicators. The onus should be on financial institutions to then take the initiative to make further appropriate enquiries, understand the situation and offer the customer the support they need.

Banks should be empowered to deploy data analysis techniques that will indicate when a customer may be experiencing a certain type of vulnerability, most notably family violence, elder abuse, mental illness or addiction. If the banks meet the principles outlined above, then this can be done in a positive, non-intrusive manner.

In most cases, proactively identifying hardship issues, vulnerabilities or needs should not lead to an invasion of privacy by say the bank proactively calling the customer to tell them that they have suspicions of domestic violence. Rather proactive identification should lead to the development of more appropriate rendering of services to meet their needs – through the offering of basic bank accounts; noting that certain customers require the use of an interpreter or TTY service; or extra sensitivity is required because of a bereavement event.

In the rare case where there is a need to raise the issue directly with a customer this should always be done so with care, tact and empathy. For instance, rather than just making a phone call to a customer that systems has flagged as potentially vulnerable, it may be more appropriate to take a customer aside when they attend a branch and have a well-trained staff member tactfully raise the concern with the customer and offer any appropriate support.

In most cases, data analysis will identify an issue that may not require any direct customer contact in order to solve. For instance, if an individual’s account indicates \$2.50 in ATM fees several times a week, this may indicate that there is a geographic area in which that bank has no ATM, and point to a need for that bank to install an ATM in that customer’s community. If in the following example a customer pays the minimum amount off on their credit card every month for over 20 years, surely a flag should have been raised and the bank should have offered the customer a way out of her predicament with a more appropriate product and a proactive debt waiver.

Case study – Catherine’s story

Catherine took out a \$1500 credit card in 1996. At the time, her source of income was the carer’s pension. She used it to buy some Christmas presents for her children. She missed a repayment a few months later, and the card was cancelled. She entered into an arrangement with the bank to make monthly repayments of \$30. From 1997 until 2018, she paid \$30 each month. Due to interest charges, late payment fees, over limit fees and annual fees, she was unable to pay off the principal. Her source of income later changed from carer’s pension to the disability support pension.

She contacted the bank several times over the years to see if there was anything which could be done to help her, and was simply told, no, you have to pay it off. This happened as recently as September 2017. When she contacted the NDH she was very stressed about

this debt and had seen on her monthly statements that she still had another 10 years of repayments. The balance of the card was approximately \$1000. After requesting statements from the bank and confirming the information Jill provided to us, we requested that the bank waive the outstanding balance on compassionate grounds, and refund up to twenty years worth of repayments, around \$7900. The bank offered to refund \$2400 and waive the balance of the credit card. Jill accepted this offer. She is now much happier with her situation resolved.

Source: Financial Rights Legal Centre

Case study – Andrew’s story

Andrew is 55 years old and on the disability pension. He came to Financial Rights when he was in financial hardship on his mortgage. He was also having difficulty paying off a car loan.

The cause of his hardship was a prior work related injury . He also has severe depression – during the course of this case he attempted suicide and was placed in a mental health ward.

After Andrew’s injury he tried different types of part time and casual work, and also tried renting out his property. He made some large lump sum payments into the mortgage from his savings, and later from a personal injury payment. Unfortunately, Andrew’s former partner accessed a large portion of the personal injury payout and gambled it away too. He ultimately fell behind on his mortgage and tried asking for an extension.

He then started receiving letters from the bank’s solicitors, which he had trouble understanding. He took one such letter to a branch of his bank to ask for an explanation. They told him conflicting things; they assured him the mortgage was up to date, and said that they did not know who the letters were from. They later refused to talk to him and referred him back to the solicitors, but he was having trouble talking to the solicitors. Andrew needed time to decide whether he could save the house from a successful claim on his home.

Source: Financial Rights Legal Centre

Approaching vulnerability as needs-based rather than identity- or category-based

Financial Rights supports the general adoption of a needs-based flag system for vulnerability support, rather than an identity- or category-based flag system. By this, we mean, in most cases, banks’ notes about customer vulnerability should be focused on the type of additional

support that customer needs, rather than on categorising the customer as within a specific vulnerability category. For instance, needs-based flags may include:

- Auslan interpreter
- Longer appointments needed
- No contact via telephone
- Quiet or private area for meeting
- Wheelchair access
- Phone call confirmation of transactions above \$200
- Restrictions on transactions to particular retailers.

The adoption of this type of system for flags and notes relating to customer vulnerability is superior on several bases:

- Many people who may fit in the same broad category of vulnerability may have different actual needs. For instance, different deaf customers may have different needs: some may need an Auslan interpreter; some may need a hearing loop; some may have other needs. It is therefore more specific and appropriate to have a needs-based flag system.
- A needs-based flag system can help to protect customer privacy. For instance, there are a significant number of reasons why a customer may need to have no contact by telephone, such as simple preference, or them being hard of hearing, or them being in an abusive relationship, or many other factors. A needs-based flag system can ensure customers get the type of service that they need, while protecting their privacy as far as possible.

We acknowledge that finding the balance between maintaining customer privacy and using information about customers to help them when they need it, is an extremely difficult issue to grapple with.

There may be some cases in which it is judged to be appropriate, on balance, to flag a customer as experiencing a particular form of vulnerability, rather than simply noting their specific needs. The type of notes and flags put down on each customer's file should be ascertained on a case by case basis based on a cost-benefit analysis for that particular customer.

For instance, in cases where a customer is experiencing domestic violence and is in fear for her life, the risk in not explicitly noting as such down in the bank's system has the potential to significantly outweigh concern for the customer's privacy. Making an explicit note of a customer's domestic violence situation can help to ensure that no bank staff deliberately or inadvertently reveal her whereabouts or contact information to an abusive partner or former partner who may be a joint account holder. In some cases, a failure to record private information about a person explicitly, could put that person at risk; in many others, a service can be provided without unduly recording private information and by instead recording that customer's needs alone.

In cases where, for example, the type of vulnerability a customer is experiencing is related to addiction or other mental health problems, it may be prudent to prioritise that customer's privacy by not making an explicit note that they are experiencing (or that data analysis suggests they might be experiencing) issues with mental health or addiction. For such customers it may be more appropriate to flag a particular type of service that may help them, for instance, setting up stricter daily limits for themselves or putting blocks on their account from making payments to particular retailers such as gambling sites or alcohol retailers.

In order to make the right decisions regarding the type of information recorded about customers experiencing various types of vulnerable circumstances, staff will need to be comprehensively trained on many factors that can drive customer vulnerability. It is important to acknowledge that at times, data analysis can be wrong – this can cause problems if there is a very rigid set of steps that staff must follow, rather than a range of ways to move forward that staff are appropriately trained to work within. We expand on staff training in section 6.

Recording vulnerability information

Financial Rights believes banks must have a written policy on personal information so as to ensure a consistent and transparent approach. This policy must then be adequately communicated to staff who need to be trained to explain it to customers.

Banks should adopt a principle of never, under any circumstances, sharing customer vulnerability information with other financial service providers. This cannot be a part of open banking, even with customer consent.

In our experience, as alluded to in the discussion paper, it is common that customers will disclose some form of vulnerability to their bank, and yet each time they interact with the bank they have to re-disclose. While we are cognizant of the concern that a more prescriptive system of notes and flags relating to customer vulnerability may make some customers feel like their privacy has been invaded, we are also aware of customer frustration with bank staff's common failure to actually read and act on vulnerability information that they have been provided. It is vital that information about the needs of customers experiencing vulnerability is recorded clearly and systematically, and that bank staff actually read all notes and flags in customers' files related to vulnerability prior and/or during each interaction with that customer.

Information recorded about customers should be stored with the requirements of the *Privacy Act* in mind, particularly the section stipulating that anything written about a customer can be requested by the customer to be accessed and read. Any notes or flags about customers should therefore be written with the knowledge that customers may be able to then read those notes themselves.

Some forms of vulnerability about which banks should take note, come under the *Privacy Act's* category of 'sensitive information'. 'Sensitive information' is defined in the *Privacy Act* to mean information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;

- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual preferences or practices;
- criminal record; or
- health.

Some of these elements, particularly around racial or ethnic origin (such as whether or not a customer is of Aboriginal or Torres Strait Islander background) or health (such as mental illness and addiction) are directly related to forms of vulnerability that we have described above and are widely acknowledged. The *Privacy Act* specifies additional safeguards for the recording of this type of sensitive information:

- ‘sensitive information’ may only be collected with consent, except in specified circumstances. Consent is generally not required to collect ‘personal information’ that is not ‘sensitive information’;
- ‘sensitive information’ must not be used or disclosed for a secondary purpose unless the secondary purpose is directly related to the primary purpose of collection and within the reasonable expectations of the individual;
- ‘sensitive information’ cannot be used for the secondary purpose of direct marketing; and
- ‘sensitive information’ cannot be shared by ‘related bodies corporate’ in the same way that they may share other ‘personal information’.⁷

These additional safeguards should not impede banks’ collection and use of data related to vulnerability that may be regarded as ‘sensitive information’.

Vulnerability information that constitutes ‘sensitive information’ should only be collected and recorded with customer consent. As with all vulnerability information, this should not be disclosed to any other body, and should not be used for primarily profit-creating purposes. Further, as we have discussed above, notes and flags in banks’ systems relating to the needs of customers experiencing vulnerability should ideally, as far as possible (though allowing for staff discretion) reference the needs of customers rather than their demographic factors or categories of vulnerability or potential vulnerability. Where data analysis indicates potential vulnerability which would constitute “sensitive information” under the *Privacy Act*, this should trigger communications between the bank and the customer in which vulnerability and needs are identified, and consent can be gained for these to be recorded.

“Don’t be creepy”

⁷ Australian Law Reform Commission, “The Privacy Act: Some Important Definitions”, ALRC, <https://www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/sensitive-information>

While firm principles or lines are difficult to define, implementation of the general principle applied in technology of “don’t be creepy” can help guide banks towards appropriate behaviour. There is a line between taking appropriate care, and “being creepy” particularly with respect to data, that banks should put effort into walking carefully. We are cognizant of the concern that consumers may be uncomfortable with data analysis techniques that potentially identify private information about their vulnerabilities. The ABA should investigate ways in which to put a principle along these lines in the Guideline.

Collaboration between the banks

The issue of data is a difficult one – and not one that can be clearly determined now. In this area, of working to finding the best possible balance between privacy and protection of customers experiencing vulnerability, banks must be collaborative and not competitive. The Guideline should encourage banks to regularly and proactively discuss these issues with one another, to skill-share and knowledge share, and to learn best practice from one another. Practices should be consistently evolving as understanding improves and approaches are tested, and banks should come together to provide the best possible outcomes for all of the banks’ customers.

Case study – Jo’s story

Jo is a single mother and a victim of domestic violence who contacted Financial Rights after she had left her abusive partner, but still had a joint mortgage with him. Alongside the mortgage, Jo had a further \$9,000 in debts.

Jo had always been the main contributor to the mortgage, and since the separation, Jo’s partner had not contributed at all towards the mortgage. Jo was struggling to pay the mortgage herself, but when she contacted Financial Rights she was just about managing to keep up with the payments. She had told the bank that she was struggling and requested a hardship arrangement. She told them of the abuse and the reason for the separation, and that she wanted to remove her ex from the mortgage and property title. Her bank denied her hardship request, and told her that if she was unable to pay the mortgage, they would contact her abusive former partner.

Financial Rights offered to provide Jo with the number for her bank’s assistance program for domestic and family violence, but Jo declined as she was tired of asking the bank for help. Jo is now working with a financial counsellor to negotiate with the bank on a hardship arrangement, and has been referred to a community legal centre for family law assistance.

Source: Financial Rights Legal Centre

Case study – Lauren’s story

Lauren was on Newstart benefits when she applied for a credit card. She wanted a credit limit of \$1,000 as she was a gambler and manages her finances by ensuring she does not have access to any large sums. She knew that having access to a large credit card would fuel and exacerbate her addiction and that she would never be able to pay off the debt. The bank instead approved a \$10,000 limit, on the basis of \$15,000 per year for income (approximately \$288 per week), and allowing for just \$5,352 per year for expenses (approximately \$103 per week).

The loan application form appears to have been completed by a bank employee putting Lauren’s details into their computer. Lauren asked for a copy of this form to be posted to her but the bank did not provide this.

Lauren continually received invitations to increase her credit limit over time, but always refused. She made some repayments on the card, which included large lump sum payments that were proceeds of her gambling.

Lauren was also sold consumer credit insurance, despite her loan application clearly stating her occupation as “home duties” and her transaction account showing Newstart benefits being deposited. As she was not working she could not claim on any unemployment or disability benefits. When she was asked to sign the consent form for the insurance, she asked that the document be printed out for her as she did not have her reading glasses and could not see the screen. She was told that this was not possible, but that they would post her a copy. She never received such a copy.

Lauren sustained a head injury two years ago, and thought the policy may have assisted her but it did not. The bank did, however, refund the \$1,500 in premiums she had paid, as a result of what appears to be a systemic review the bank conducted about the sale of these policies. However, this refund did not include interest despite the fact that the premiums were taken from Lauren’s credit card account.

Source: Financial Rights Legal Centre

Recommendations

17. The Guideline should include the principle:

If a bank collects any information relating to a customer’s vulnerability, that information should not be used to discriminate against that customer or used in a way that causes them detriment. Similarly, it is important that any data gathered about customers’ vulnerability is not used for direct marketing purposes or primarily for banks’ own financial gain.

18. Banks should ask customers a series of questions relating to indicators of potential vulnerability and needs, including an open-ended question asking of any further specific needs:

“Is there anything else that we should know about you to help us give you appropriate services and support?”

Do you, for example:

- *require an assistance animal to accompany you to our branches;*
- *require Auslan or other interpretation;*
- *have a mental illness or addiction and require blocks on certain retailers or maximum daily limits?”*

19. Banks should deploy data analysis techniques to pick up on indicators of potential vulnerability or need and initiate more appropriate services to meet those needs. In the rare case where there is a requirement to raise the issue directly with a customer this should always be done so with the utmost care, tact and empathy.

20. Customer vulnerability information should, as far as possible, be recorded in banks’ systems in terms of customers’ specific needs rather than the type of vulnerability that they are experiencing.

21. Customers should be able to give or withdraw consent for their data to be stored and used at any time.

22. Banks must have a written policy on personal information to ensure a clear and consistent approach, which should be communicated to staff, who should be trained to explain it to customers.

23. Banks should never, even with customer consent, share customer vulnerability information with other financial service providers.

24. Systems should be adopted to ensure that notes relating to the needs of people experiencing vulnerability are most useful, by compelling bank staff to actually read all vulnerability notes and flags in customers’ files prior to and/or during each interaction with that customer.

25. Information relating to vulnerability should be recorded with the knowledge that any customer can request to access and read any notes on them taken by the bank, at any time.

26. Banks should be compelled to work collaboratively rather than competitively, towards a best practice approach to balance privacy and protection of customers experiencing vulnerability.

6. Staff training

Do you agree with inclusion of the proposed staff training provisions in the Guideline?

Financial Rights believes it is necessary that the Guideline directs banks to fully commit to ensuring staff are adequately trained. In the UK context, the FCA paper on vulnerability states:

“Our interviews with firms and experts in vulnerability revealed that dealing with sensitive or difficult issues can be frightening and demoralising for staff if effective training and guidance is not in place. It was commonly reported by some firms that staff on the frontline and in specialist support teams feel more empowered and motivated if they feel they know how to help people. Research (Macmillan 2014, Demos 2013) shows that customer-facing staff can be embarrassed or panic when a customer tells them they have a cancer diagnosis. Fear of causing offence, or using the wrong words, can also prevent staff from getting into conversations (Money Advice Trust, personal communication 2014). Staff can feel deeply frustrated if they don’t have the skills to provide support or aren’t aware of where to direct people. Better training and support to staff could therefore boost morale and job satisfaction, improving retention.”⁸

Clearly it is vital that all banks provide comprehensive, adequate training relating to various forms of vulnerability, to all bank staff. The Guideline should set out the parameters and expectations for this training.

Do you think any additional guidance or provisions for staff training should be included in the proposed Guideline?

Broad, flexible training for all staff

It is important that the Guideline stipulate that staff training must be broad, comprehensive and flexible. It must be broad both in content and coverage. Staff training should not be targeted at training staff in specific step-by-step checklists for engaging with customers experiencing certain types of vulnerability. We understand that training staff on a rigid set of processes for assisting customers in a discrete set of vulnerable circumstances would be far less time-consuming and costly than providing every staff member comprehensive training and education around the multiplicity of factors that drive potential vulnerability. We contend that a check-box, uniform approach to assisting people in vulnerable circumstances is better than no approach or processes whatsoever, but will never be sufficient.

Staff training must not just be for frontline staff: it must be provided widely, from the board downwards to all staff, and to all banks’ solicitors. It is important that a thorough understanding of vulnerability is imbued throughout organisational culture and that all decision-makers, managers and more are fully across the issues. We are concerned that if training were provided to just frontline staff, decisions that they make from a perspective of care for customers experiencing vulnerability may be second-guessed by management who have not received the same level of training and do not have the same understandings of customers’ potential needs. Further, it is vital that appropriate training relating to vulnerability is provided to all staff involved in product and service design.

Staff education relating to vulnerability should be comprehensive, and provide staff with a general understanding of the nature of many circumstances of vulnerability. Ensuring staff genuinely understand vulnerability rather than are simply trained on a particular step-by-step approach is the only way to ensure flexible, appropriate responses from staff that can provide

⁸ Financial Conduct Authority, *Consumer Vulnerability*, Occasional Paper No. 8, February 2015, p. 73.

adequate assistance to customers experiencing a diverse range of vulnerabilities. This will enable bank staff to manoeuvre more safely and effectively in the grey areas that arise when assisting customers experiencing vulnerability, as they will be better equipped to make the right decisions without rigid guidelines for action.

Cultural safety

There should be an additional provision in the Guideline specifically mandating that all staff undertake regular cultural safety training to ensure that their approach to assisting Aboriginal and Torres Strait Islander customers and prospective customers is appropriate and culturally safe.

Trauma-informed customer engagement

The Guideline should also explicitly say that customer-facing staff must receive training in trauma-informed customer engagement for customers or prospective customers who may be experiencing or have experienced domestic and family violence. All customer-facing staff must also receive training in vicarious trauma.

Debriefing process

The proposed “appropriate ‘debriefing process’ to help manage the wellbeing of staff supporting customers through particularly vulnerable circumstances” is not strong enough. There should be commitments that banks will have comprehensive employee assistance programs so that employees affected by vicarious trauma can access counselling and proper support.

Recommendations

27. Financial Rights supports the inclusion of the proposed staff training provisions in the Guideline.
 28. Training on vulnerability for bank staff must be broad, comprehensive and flexible, so as to fully equip staff to make appropriate choices outside of a uniform check-box approach.
 29. Training on vulnerability must be provided from the Board down, to every staff member, in banks, so as to imbue an understanding of vulnerability throughout organisational culture.
 30. The Guideline should specifically require that all staff undertake regular cultural safety training.
 31. The Guideline should require that all customer-facing staff receive training in trauma-informed customer engagement and in vicarious trauma.
 32. The Guideline should require that banks will have employee assistance programs in order to adequately support staff impacted by vicarious trauma.
-

7. Formal arrangements

Do stakeholders support the implementation of the recommendations of the Australian Law Reform Commission relating to power of attorney reforms, a national register and an organisation to investigate 'good faith' reports of financial abuse?

Financial Rights supports implementing the recommendations of the Australian Law Reform Commission relating to power of attorney reforms, a national register and an organisation to investigate 'good faith' reports of financial abuse.

Recommendation 5-3

A national online register of enduring documents, and court and tribunal appointments of guardians and financial administrators, should be established after:

- (a) agreement on nationally consistent laws governing:
 - (i) enduring powers of attorney (including financial, medical and personal);*
 - (ii) enduring guardianship; and*
 - (iii) other personally appointed substitute decision makers; and**
- (b) the development of a national model enduring document.*

Nationally consistent laws on powers of attorney, enduring guardianship and other personally appointed substitute decision makers, and a national register of enduring documents are vitally important to ensuring consumer protection.

Recommendation 14-7

Adult safeguarding laws should provide that any person who, in good faith, reports abuse to an adult safeguarding agency should not, as a consequence of their report, be:

- (a) liable civilly, criminally or under an administrative process;*
- (b) found to have departed from standards of professional conduct;*
- (c) dismissed or threatened in the course of their employment; or*
- (d) discriminated against with respect to employment or membership in a profession or trade union.*

Financial Rights supports the adoption of this recommendation. If banks begin to engage in systematic data analysis to find indicators of potential abuse, staff should be able to assist in more ways than just specifically relating to customers' banking. They should be able to use information gathered by the bank to make a good faith report of potential abuse, and there should be an organisation equipped to investigate such reports. Banks are well-resourced and have access to a significant amount of information about customers – they are well-placed to spot potential abuse, in some cases before any other institution may identify the abuse. In order to make the most of this position, staff should be able to provide as much assistance to customers as possible.

Financial Rights endorses the positions taken in the submission by the Consumer Credit Legal Service WA (CCLSWA) in response to this question. CCLSWA have made the points that:

- The differences in legislation between states and territories makes it exceedingly difficult to perform adequate checks as to the validity of EPAs
- Due to the private nature of EPAs it is difficult to ascertain the actual extent of abuse of EPAs.
- In Western Australia, a done can withdraw all of the donor's savings and sell their property, all without being required to formally register the EPA.
- There is currently no way to confirm whether an EPA instrument is valid and has not been revoked.
- A national online register would assist in alleviating these issues, and will enable banks, financial institutions and other organisations such as community legal centres to verify the validity of EPAs and accordingly act in the best interests of clients and customers.
- In setting up a national online register, the administrative burden should be considered – this can include looking at how other jurisdictions that have implemented an EPA registration, such as the UK, have dealt with these issues.

Do you agree with our proposed inclusions relating to third party authorisation forms in the Guideline?

Financial Rights supports all suggested inclusions relating to third party authorisation forms in the Guideline.

Are there any changes or additional commitments relating to third party authorisation forms which you think should be included in the Guideline?

In addition to those listed in the consultation paper, Financial Rights suggests that forms should explicitly ask how long the authorisation form should stand for, and, in cases where the duration of the authorisation is longer than six months, how often the bank should check back in with customers to ensure the form still stands. Even in situations where the customer has indicated 'forever', the bank should still be obliged to regularly check back in.

The Guideline should make clear that where there is any uncertainty whatsoever relating to a third party authorisation form, the bank must still contact the customer directly.

The discussion paper states:

“Banks should consider options for customers to limit the authorisations that are provided by third party authorisation forms – for example, transaction limits or open an alternative bank account with automated transfers to manage specific needs.”

In our view, this does not go far enough. All third-party authorisation forms should be made customisable, and all banks should be compelled to comply with this requirement. Customers should be empowered to specify the exact authorisations they wish to provide to a third party. There may be a customer who only wishes to provide one very specific authorisation to a third

party, related to a specific need or vulnerability of that customer. This should be facilitated by the bank, without the customer being pushed into handing away more power than they wish to.

Further, third-party authorisation forms should not be possible to complete without a face to face meeting, or at the very least a direct phone call where a face to face meeting is entirely impossible, between the bank and the customer. This can help to ensure that financial abuse is not in play and that the request for third party authorisation is legitimate. In order for this step to be most effective, there must be trained bank staff available to facilitate direct, private communication between the customer and the bank regardless of potential vulnerability on the part of the customer, for instance a language barrier or disability.

Recommendations

33. Financial Rights endorses the positions taken in the submission by the Consumer Credit Legal Service WA regarding the recommendations of the Australian Law Reform Commission.
 34. Financial Rights supports all suggested inclusions relating to third party authorisation forms in the Guideline.
 35. Third party authorisation forms should explicitly ask how long the authorisation should stand for, and in cases where the duration of the authorisation is longer than six months, how often the bank should check back in with the customer.
 36. The Guideline should stipulate that where there is uncertainty relating to a third party authorisation, the bank must contact the customer directly.
 37. All third party authorisation forms should be customisable; customers should be empowered to specify which authorisations they wish to provide to a third party.
 38. Third party authorisations must, where possible, require a face to face meeting between the bank and the customer, including ensuring that there can be private communication between the bank and the customer.
-

8. Unsecured debt and collections

Should collections arrangements be included in this Guideline?

If yes, what do you think are the appropriate parameters that should be applied to collections arrangements for vulnerable customers?

If yes, should these arrangements be applied to all categories of vulnerable customers?

Financial Rights supports the inclusion of collections arrangements in the Guideline. Debt collection is an issue that disproportionately impacts customers experiencing some form of vulnerability, and as such there should be strong, broad, industry-wide regulation of collections activities as relates to customers experiencing vulnerability, through both the Guideline and the inclusion of enforceable clauses in the Banking Code.

Defining the appropriate parameters for collections arrangements for customers experiencing vulnerability is complex. Taking into account the very many circumstances and demographic factors that can drive financial exclusion and vulnerability, it can be hard to draw clear lines around the types of vulnerability that should preclude a bank from selling on a customer's debt to a collections agency.

We strongly support existing arrangements regarding customers who are victims of domestic violence, and support the expansion of such arrangements to customers experiencing other forms of abuse such as elder abuse – where the debt is related to the abuse.

However, we note the difficulty in setting hard boundaries around other forms of vulnerability that may coincide with debt. Unemployment is a form of vulnerability that can give rise to financial hardship and debt issues. We acknowledge that in this circumstance it may be unrealistic to ask that any debt incurred as a result of, or related to, unemployment, be subject to the same arrangements as those in place regarding victims of domestic violence.

While 'vulnerability' is broad and can refer to a great number of things, we think that the following principle should be considered:

If a customer's vulnerability caused a debt to be incurred, and/or there is no prospect of recovering the money due to an ongoing vulnerability, then the bank should not sell that debt to a collections agency.

Customers in the circumstances above should not be subjected to continued harassment from debt collectors.

Further, the Guideline should stipulate, and the Code should make enforceable, that all collections agencies engaged by banks must also be committed to familiarity and compliance with the Guideline, including providing their staff with comprehensive training on engaging appropriately with customers experiencing vulnerability in the event that such debts are sold

in circumstances where the bank has not identified the vulnerability or the customer begins to experience vulnerability after the sale.

Recommendations

39. Financial Rights supports the inclusion of collections arrangements in the Guideline.
40. Financial Rights supports the expansion of existing arrangements for customers who are victims of domestic violence to customers experiencing other forms of abuse where the debt is related to the abuse.
41. Financial Rights recommends the adoption the general principle:
if a customer's vulnerability caused a debt to be incurred, that vulnerability is ongoing, and/or there is no prospect of the money being recovered, then the bank should not sell that debt to a collections agency.
42. The Guideline should stipulate, and the Code should make enforceable, that all collections agencies engaged by banks must be committed to familiarity and compliance with the Guideline.

9. Scams

Do you support including industry level guidance on preventing scams in the Guideline?

Financial Rights supports including industry level guidance on preventing scams in the Guideline. Vulnerable people are more vulnerable to scams in general, and are the most in need of points of friction in the system where scams may potentially occur, to stop them from happening.

In order to prevent scams, in general, banks should do far more checking in with people. Google, for instance, checks in whenever a person logs into their Google account from a new device. All that this check entails is an email notification that a log-in has occurred from a new device: if the login was by the customer, they can simply choose to disregard the email and go about their business. If it was, in fact, a hacker, then this is a very useful alert that something has gone wrong. This type of check in from banks would be very useful for preventing scams: if a strange-looking transaction occurs, or there is a log-in from an unfamiliar device, then some sort of notification should be immediately, automatically sent out to the customer. Some banks have some systems in place along these lines, but these should be made more comprehensive, particularly for customers that show indicators of vulnerability.

For larger or repeated odd-looking transactions, the Guideline should offer industry level guidance on ways to talk to customers, particularly those customers who may be experiencing vulnerability, about scams that they may be falling victim to.

The Guideline should also include a comprehensive step-by-step guideline for banks to assist customers with the various things that victims of fraud may need to recover. This can include getting money back where possible, increasing security on relevant accounts, closing relevant accounts, making amendments to credit reports and more. The Code should then be amended include an obligation on the part of the banks to comply with the required steps to assist consumers who have been victims of fraud.

Case study – John and Mary’s story

Both John and Mary are over 80 years old and on Centrelink pensions. They had almost \$15,000 stolen from their bank account through internet banking in September 2017.

John was contacted by a scammer pretending to be from the bank’s fraud department. He was sent SMS text messages with transfer codes, which he gave to the scammer. John and Mary notified their bank as soon as they saw the withdrawals from their account. The bank recovered sum, but not all. The bank took the position that John had breached the security of the account, and that their SMS messages stated not to reveal the code to anyone, even to the bank itself and therefore not obliged under the ePayments code.

Financial Rights assisted John and Mary to raise a dispute under the ePayments code, in our view the bank did not provide sufficient assistance in reviewing John and Mary’s matter.

Source: Financial Rights Legal Centre

Case study – Brita’s story

Brita was referred to Financial Rights by a financial counsellor. Brita spoke very little English, but explained to us that her daughter had become involved with a Nigerian Love Scam, stole Brita’s title deeds and obtained a reverse mortgage over her home soon after being released from a psychiatric hospital.

The financial counsellor had lodged in EDR for Brita before referring her to Financial Rights. The bank eventually provided Financial Rights with Brita’s mortgage documents, which were clearly not signed by Brita herself. We sought for the mortgage to be set aside.

Financial Rights collected specimen signatures including on a death certificate and other materials accrued over Brita’s lifetime, and many telegraphic transfers evidencing the funds moved offshore. The bank stated they had sighted Brita’s proof of age card in

verifying her identity when granting the mortgage. Brita does not have a proof of age card; Roads and Maritime Services certified that no such card had ever been issued to our client.

Soon before the matter was referred for handwriting analysis, the bank agreed to release Brita from the mortgage and return her title deeds.

Through the course of the dispute, it was clear the bank could have done more to prevent the fraud from occurring, for example, they:

1. ought not to have allowed our client's daughter to be the translator;
2. they ought to have obtained a translator for our client as early as possible when our client raised concerns that she did not receive the money and came to the bank in distress;
3. they ought not to have allowed the money be paid to an account in the daughter's name.
4. provided more proactive assistance to our client about what to do if there is fraud.

Source: Financial Rights Legal Centre

Recommendations

43. Financial Rights supports including industry level guidance on preventing scams in the Guideline.
 44. In order to prevent scams, banks should be obliged to do far more checking in with customers relating to any transactions that appear unusual.
 45. The Guideline should include a comprehensive step-by-step guideline for banks to assist customers that have been victims of fraud to recover.
-

10. Concluding Remarks

Thank you again for the opportunity to comment. If you have any questions or concerns regarding this submission please do not hesitate to contact Financial Rights on (02) 9212 4216.

Kind Regards,



Karen Cox

Coordinator
Financial Rights Legal Centre
Direct: (02) 8204 1340
E-mail: Karen.Cox@financialrights.org.au