Risk Policy Overview – Vulnerable Customer

2023

The co-operative bank

1 Introduction

1.1 Aims

The aim of this document is to outline the steps that need to be undertaken to ensure that The Co-operative Bank plc (The Bank) is considering and supporting customers during times of ongoing or temporary vulnerability.

Vulnerability is a key focus area for the Financial Conduct Authority (FCA), and by supporting our vulnerable customers we are also aligning to the Co-operative Bank's Values and Ethics, ensuring that our customers are treated fairly.

The FCA expects the fair treatment of vulnerable customers to be embedded in our culture, processes and policies. In order to do so, this guidance must be adhered to in all areas of The Bank, including any processes that may be handled on our behalf by third parties.

The intention of this document is to build and improve on processes to ensure that any customers who may be vulnerable can reach the most appropriate outcome for their circumstances.

1.2 Definitions

The Co-operative Bank's definition of vulnerability

A customer who requires additional support or reasonable adjustments to ensure they receive a good outcome when engaging with the Bank's products or services, as a consequence of permanent or temporary vulnerability.

Other organisations helpfully define vulnerability, and the Bank's definition is drafted to ensure that it covers the spirit of these.

The FCA definition of vulnerability

Someone who, due to their personal circumstances, is especially susceptible to detriment, particularly when a firm is not acting with appropriate levels of care.

Lending Standards Board (LSB) in Standards of Lending for Business Customers

- Reference to an individual means a person who, when taking into account information available to the firm about the how the business is structured and operates, is able to exert significant control over the way in which it is run.
- Reference to vulnerability is in relation to the individual rather than the business itself, for example, a business in financial difficulty would not necessarily be considered to be vulnerable for the purposes of these Standards.

Therefore based on this definition, the business itself cannot be classed as vulnerable and vulnerability needs to be considered in relation to individuals who are responsible for and, or, run the business.

2 Application and Sources of Risk

2.1 Application

The Policy applies to:

- All business units and functions within the Bank

- All regulated entities, including any subsidiaries or Joint Ventures in which the Bank has a 50 % or greater interest
- All employees of the Bank whether permanent, contract or temporary, including employees of any subsidiary in which the Bank has a controlling interest
- All organisations and people working on behalf of the Bank

2.1.1 Third Party Suppliers

This Policy applies to all Third Party suppliers engaged by the Bank in any activity, to the extent that they need to comply with the Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA) or other regulatory requirements on behalf of the Bank, during the provision of those activities or services.

2.2 Sources of Risk and Scope

2.2.1 Sources of Risk

While it is good business to deliver good customer outcomes and service, it is the FCA which sets the scope in terms of what is ultimately expected in relation to Vulnerable Customers. Material failures would be subject to investigation and potential fines.

2.2.2 Risks in Scope

Implementation and adherence to this guidance is mandatory for all areas of the business, including third parties who operate on our behalf, and all activities that the bank undertakes that impact both personal and business customers.

The scope includes:

- All customer products:
  - From design through to implementation and any changes to existing products.
  - Including, but not limited to, personal and business current accounts, savings accounts, mortgages, loans and credit cards.
- All customer interactions:
  - Including all digital and non-digital channels.
- Customer Promotions / Advertisements.
- Any other interactions on our customers' accounts:
  - E.g. fraud checks etc.
- Any processes or services that have been outsourced to a third party.

Product Design

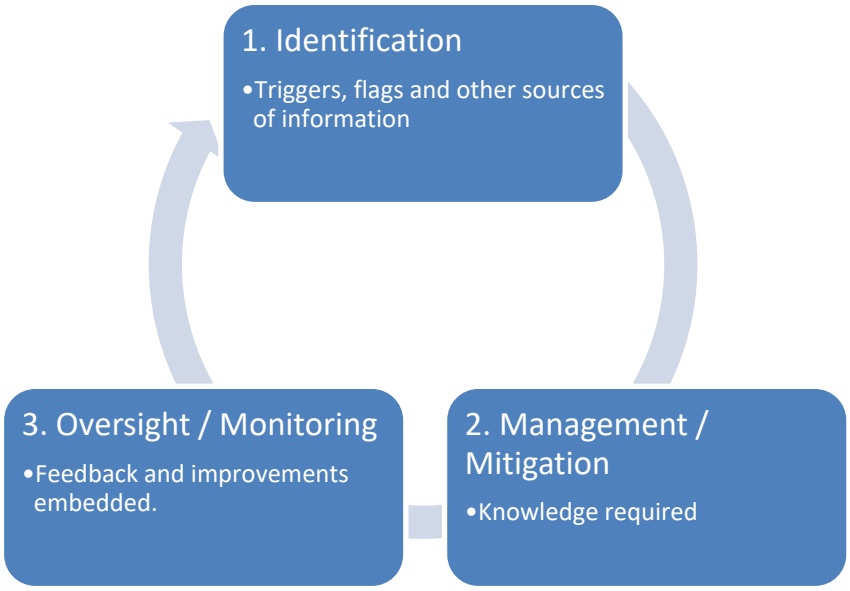
At the heart of product design should be the goal of enabling customers with vulnerabilities to achieve the same outcome as customers who do not exhibit vulnerability.

During the design process, products should be reviewed from a vulnerable customer perspective with a consideration of any positive or negative impacts of a product and service on vulnerable customers. Any potential issues must be identified and resolved before the product is brought to market.

Products, communications and services should be reviewed periodically to check whether they are continuing to meet the needs of vulnerable customers.

2.3 Key Policy

The key policy outlined in this section revolves around three areas of focus. These can be seen in the diagram below:



This illustrates a continuous cycle of learning and development. The outcome of the oversight and monitoring should directly impact and improve the measures that are in place to identify and manage the needs of our vulnerable customers.

2.3.1 Identifying Vulnerability

It is critical for the Bank to recognise and identify the potential triggers or signs of vulnerability, as without doing so, it is unable to make reasonable adjustments or support additional needs.

Table 1: The 4 key drivers of vulnerability and the types of characteristics of vulnerability they may cause

Health	Life events	Resilience	Capability
Physical disability	Caring responsibilities	Low or erratic income	Low knowledge or confidence in managing finances
Severe or long-term illness	Bereavement	Over indebtedness	Poor literacy or numeracy skills
Hearing or visual impairment	Income Shock	Low savings	Low English language skills
Poor mental health	Relationship Breakdown	Low emotional resilience	Poor or non-existent digital skills
Addiction	Domestic Abuse		Learning impairments
Low mental capacity or cognitive impairment	People with non-standard requirements such as people with convictions, care leavers, refugees		No or low access to help or support
	Retirement		

Helpfully the FCA has identified four drivers of vulnerability i) Health, ii) Life Events, iii) Resilience, and iv) Capability - these are the drivers that the Bank refers to in the first instance.

Examples can be seen in the table below – please note this list, provided by the FCA, is not an exhaustive list.

It is also recognised that all of our customers sit within a spectrum of vulnerability. Within this spectrum some customers are at greater risk of harm than others. Those customers disclosing or displaying any or multiple drivers of vulnerability are likely to require more support. Early action is vital to prevent and reduce the risk of harm to our customers.

2.3.2 Triggers

Triggers of vulnerability can be revealed within conversations with our customers. These should serve as flags to the advisers, who should then ask searching questions to uncover the full extent of the vulnerability.

These flags in conversation could include disclosure of:

- Long term underlying illness;
- Physical or mental disability;
- Bereavement of family member or close friend;
- Loss of income;
- Large amount of debit;
- Struggling with financial matters / obligations;
- In financial difficulty;
- Business restructure.

Other flags could be discovered in conversation with the customer, such as:

- Difficultly understanding simple financial matters;
- Difficulty retaining information – including over multiple interactions;
- Relying on a third party for advice;
- Avoidance of certain types of customer platforms, indicating lack of skills in that area –e.g. digital.

Time, consideration, sympathy and flexibility should be key tools in handling the initial discussions.

Extra care should be taken if several of the flags overlap, as this would indicate a vulnerability that may require extensive and or external support to achieve a good customer outcome.

Customer Help and Support

The Bank works with external organisations like Citizens Advice and have developed a referral programme for customers who are experiencing difficulties. Get Free Financial Help from Citizens Advice | The Co-operative Bank

For some customers who find themselves in an emergency situation we have a Hardship Fund available which can provide a one off payment of £100, providing immediate support. There are no requirements to re-pay this support. Financial help | The Co-operative Bank

We want to help our customers when they need us the most, from major life events to everyday financial hints and tips. We have created an online money management hub, offering help and advice on managing finances with links to helpful tools and internal and external support.

We have created online support information for people experiencing Economic Abuse, the information contains advice such as how to stay safe online and signposts to support. The information will not show in the search history for safety. We have also created a digital disclosure form so customers can let us know if they are experiencing abuse and tell us what they need.

We ensure colleagues have the skills to support customers through regular training from external providers such as Surviving Economic Abuse & GamCare. Financial Abuse and Economic Abuse | The Co-operative Bank

3 Roles and Responsibilities

The Bank's Three Lines of Defence (3LOD) governance model is designed to ensure appropriate responsibility and accountability is allocated to the management, reporting and escalation of risks.

Fair treatment of vulnerable customers must be embedded into the Bank's culture.

Senior Leaders within the Bank play a key part in defining the Bank's culture due to the important decisions they make and should take the lead in embedding the vulnerable customer culture. By doing so, the needs of vulnerable customers will be a key consideration when making important decisions, ensuring these customers receive good outcomes in their dealings with the bank.

The embedding of this culture must continue in all other areas of the organisation. The level of information and training provided should be proportionate to the level of interactions with vulnerable customers the role in question requires. An example of this might be providing specialist training to frontline advisers.

3.1 1st Line of Defence (LOD)

The first line of defence (1LOD) are responsible for:

- Implementing this guidance; providing appropriate staff training and creating and maintaining processes and procedures to ensure that vulnerable customers are identified and appropriate action is taken to demonstrate good customer outcomes;
- Ensuring that proportionate oversight (e.g. quality assurance) activity is undertaken in line with the RMF and the effectiveness of the systems and controls are assessed to confirm that they continue to be effective.
- All staff who are interacting with customers should periodically and at least annually, receive training to identify vulnerability. This training can be tailored to their role and should signpost to tools that the adviser can access to help them further.
- A culture of support for customers and staff must be maintained at all times with a clear focus on treating the customer fairly, ensuring that they receive a similar outcome as other customers.

3.2 Second Line (The Risk Function)

The second line of Defence (2LOD) are responsible for:

- Providing technical advice and guidance to 1LOD to support the implementation of this policy guidance.
- Independent oversight of the systems and controls that have been put in place.

3.3 Risk Framework Owner (RFO)

Vulnerable Customer is an important element of Conduct Risk and the RFO in the 2nd LOD is the Director of Compliance. The RFO for Conduct Risk is responsible for:

- Upkeep of the Risk Policy and necessary Control Standards
- Defining risk appetite and measurement
- Implementing appropriate oversight and assurance

Compliance provide oversight and challenge to the 1st LOD management of Conduct Risk on a risk based resource allocation to provide:

- Forward looking assessment and challenging where appropriate to ensure Conduct Risk appetite is considered and incorporated in Strategic and Business planning
- Reviewing and evaluating all aspects of risk identification
- Providing expert advice on Regulatory and Conduct Risk issues
- Undertaking reviews to ensure Conduct Risks are managed effectively and in accordance with this Policy
- Reviewing and where appropriate, challenging the effectiveness of the 1st LOD's monitoring, reporting and resolution of breaches of risk appetite or Policy

3.4 Third Line of Defence

Internal and External Audit act as the third line of defence (3rd LOD). They independently monitor the embedding and report on progress to the Executive and Audit Committee. On an ongoing basis, Internal Audit will form an independent view on the Bank's management of risk, based on BAU audit work, issue assurance and business monitoring. This will include activity of both the 1st LOD and the 2nd LOD. Internal Audit may review specific elements of Information and Data in line with the Audit planning process, and also include within relevant wider audits.

4 Compliance

All areas of the Bank are expected to evidence compliance with this Policy unless specifically excluded within the Scope section.

4.1 Waivers and Dispensations

No waivers (permanent exceptions) will be agreed outside any area excluded within the Scope section of this Policy.

A temporary dispensation is the action / decision to exclude temporarily a Business Unit, process or activity from the scope / requirements / principles of all or parts of the Policy. This will increase the risk profile and the likelihood is this will result in a specific risk outside appetite. Requests must be sent to the appropriate RFO setting out the rationale, expected impact and duration.

An Issue must be raised in the Bank's Operational Risk Management System with an action plan designed to achieve compliance. Where there is no action plan and therefore the risk falls into the criteria of a risk acceptance, the Bank's Risk Acceptance process must be followed.

4.2 Breaches

A breach is classified as non-compliance with any requirement of Policy where there is no approved modification or exception in place. In situations where breaches of Policy arise, it is essential that there are clearly defined, efficient and appropriate processes to get the risk back within appetite and this should be made clear in an Issue and Action plan. The RFO must be informed of any breaches who will escalate a confirmed breach through governance.

5 Policy Ownership and Approval

This Policy is owned by the Director of Compliance and approved by Operational, Compliance and Financial Crime Risk Oversight Committee.