Chartered Insurance Institute

Standards. Professionalism. Trust.

Managing customer vulnerability in insurance and personal finance

A practical implementation guide

cii.co.uk

Foreword

Effective vulnerability management delivers benefits far beyond regulatory compliance. It creates value for customers, strengthens businesses, and supports a fairer, more resilient society.

According to the Financial Conduct Authority (FCA) Financial Lives survey, up to half of UK adults show characteristics of vulnerability at any given time, and most of us will experience some form of vulnerability during our lives. This isn't a niche segment. When firms serve vulnerable customers well, they serve all customers well.

Building robust vulnerability management takes commitment. It may require investment in data infrastructure, systems, processes, as well as building a culture of continuous improvement. But the long-term benefits are clear. Firms that anticipate and respond to the evolving needs of vulnerable customers can reduce operational costs, build stronger loyalty, and enhance their brand reputation.

More broadly, firms that identify and support vulnerable customers contribute to wider wellbeing and social inclusion. They help ensure that people who most need protection and advice can access it, particularly when circumstances make them most at risk of harm.

This guidance comes at a time when the FCA is intensifying its focus on evidencing outcomes for vulnerable customers. As Charlotte Clark, director of cross-cutting policy and strategy, has stated, there is now a "deliberate move from prescription to principles with proof." Firms must demonstrate that communications move vulnerable consumers into better value products.

The Chartered Insurance Institute (CII) is committed to strengthening professional standards and supporting firms in turning principles into practice. We hope this guidance helps translate regulatory expectations into action.

Matthew Hill,
CII Chief Executive

Contents

1 Executive summary

Many firms are making good progress in meeting the FCA's Consumer Duty aims of strengthening consumer protection standards and driving culture change. This guide contributes to these aims by addressing two interconnected areas where challenges remain: managing customer vulnerability across the product lifecycle and translating principle-based regulation into practical action.

Developed through extensive collaboration with vulnerability experts, customer experience practitioners and input from people with lived experience of vulnerability, this guidance has been rigorously peer-reviewed to ensure it meets the sector's needs.

What this guide covers

The guide provides practical guidance, including checklists and real-world examples, covering:

- **Understanding vulnerability**: how potential harms arise from the interaction between customer circumstances and firm activities, the dynamic nature of vulnerability and the severity grades of vulnerability a customer might experience.
- **Operational frameworks**: a 6-step vulnerability management framework (i.e. identify and classify, quantify, monitor, support, adapt and report), mapping customer circumstances to harms and needs, risk assessment for addressing poor outcomes, and outcome reporting approaches.
- **Data and systems infrastructure**: structured taxonomies, system requirements and good practice for data sharing.
- **Enabling elements**: leadership commitment, culture change, training effectiveness and creating disclosure-friendly environments.
- **Implementation pathways**: proportionate approaches for firms of different sizes and complexity.

Filling the gap

CII research indicates that data is the most significant implementation challenge for firms[1] and it is not adequately covered in existing published guidance. This guide addresses this gap by providing actionable recommendations on the data structures, processes and systems needed to identify vulnerabilities, deliver tailored support, measure outcomes and evidence Consumer Duty compliance.

This is particularly timely as the FCA moves toward "principles with proof", requiring firms to demonstrate through evidence (not just processes) that vulnerable customers achieve good outcomes.

Setting a high bar

Consumer Duty sets ambitious standards. This guidance maintains that ambition. We recognise this may ask firms to go further than their current practice. This is intentional; genuine culture change and improved customer outcomes require stretching beyond the comfortable minimum. As the regulatory bar rises, so must our collective aim.

We hope this guide provides practical support for your firm's Consumer Duty and vulnerability management journey.

1. Consumer Duty Board Reporting: one year on (September 2025). https://media.umbraco.io/ciigroup-dxp/x24f5ya1/260925-one-year-on-consumer-duty-roundtable.pdf

2 Context and scope

2.1 Regulatory background

On 7 March 2025, the FCA published findings from its Review of firms' treatment of customers in vulnerable circumstances. It acknowledged positive steps (for example, increased awareness and cultural changes) taken by firms driven by existing guidance but also noted that significant gaps remain, including:

- Monitoring and action on outcomes: most firms lack the data needed for adequate monitoring and/or action on outcomes for customers in vulnerable circumstances.
- Product and service design: most firms have not made meaningful progress in embedding the needs of their customers in vulnerable circumstances into the design of products and services that are intended for all customers.
- Training gaps: nearly half of firms have only provided vulnerability training to front-line staff and not beyond this.
- Communication barriers: failures exist in providing clear and accessible communication channels for customers in vulnerable circumstances, with insufficient testing for customer understanding.
- Encouraging disclosure: firms should proactively engage with customers in vulnerable circumstances to enable them to disclose their needs, so they can provide appropriate support.
- Tailored support: firms should respond flexibly and tailor support to diverse customer needs, leading to good customer outcomes.

2.2 Purpose and scope

The UK Government's Financial Inclusion Committee has a clear mission: to make sure that people can access affordable financial products and services that will support their financial well-being. The scope is across digital access and banking, credit, insurance, problem debt, financial education and savings sectors, and will tackle topics including accessibility, mental health and economic abuse.

Previous customer vulnerability guidance was introduced by the FCA in FG21/1 Guidance for firms on the fair treatment of vulnerable customers (2021) and then embedded into the regulator's FG22/5 Final non-Handbook Guidance for Firms on the Consumer Duty (2022). This represented many years of consultation, commencing in 2015, with Occasional Paper No. 8: Consumer Vulnerability.

However, market feedback reveals that translating regulatory principles into business-wide practices is a challenge and can lead to fragmented implementation of vulnerability management.

What this guide covers

This guide tackles this challenge by providing practical steps to operationalise regulatory expectations holistically, with particular focus on the data management and systems infrastructure needed to support all customers and evidence outcomes.

The approaches outlined in this guide represent proven practices rather than exhaustive solutions. Firms should apply these principles proportionately based on:

- The size and nature of their business.
- Their position in the distribution chain.
- The complexity and risk profile of their products.
- The characteristics of their customer base.

Firms may also adopt alternative methods that equally satisfy FCA expectations, and which suit their specific operational contexts.

What the guide does not cover

- **Artificial Intelligence (AI)**: while AI offers potential applications in vulnerability identification and monitoring, this field is still in its infancy. Guidance on the responsible use of AI in vulnerability management will be addressed in separate resources as the technology matures.
- **UK General Data Protection Regulation (UK GDPR) compliance**: the guide addresses data protection requirements throughout. However, detailed guidance on UK GDPR compliance for vulnerability data will be addressed in a separate document.
- **Training implementation**: the guide outlines at a high level the recommended scope of vulnerability training programmes, as well as ways of measuring its effectiveness. It does not replicate the extensive training guidance and methodologies already available from the FCA, Money Advice Trust, and other sources (listed in section 7 references).

2 Context and scope

- **Inter-firm data sharing**: the guide emphasises the importance of sharing vulnerability data across the distribution chain to enable holistic customer support, however the technical implementation of inter-firm data sharing presents significant challenges. The CII is convening a cross-sector taskforce to develop data sharing standards, protocols, and contractual frameworks to address these challenges.

Terminology

The guide generally uses terminology as defined within the FCA regulations. However, for ease of reading and brevity we refer to 'vulnerable customers' as shorthand for 'customers in vulnerable circumstances.'

2.3 Who is this guidance for?

This guide is for all UK regulated firms within the insurance and personal finance sectors, including:

- Financial advisers and planners (both sole practitioners and larger firms)
- Mortgage brokers (both sole practitioners and larger firms)
- Insurance brokers (retail and commercial)
- Insurance providers (life, general and health)
- Networks and distributor groups
- Third-party administrators and service providers who form material parts of the value chain

While focused on the UK insurance and personal finance sectors, most of the principles will apply to financial services firms more broadly.

Self-assess your customer vulnerability management maturity using the checklist in Appendix 1.

3 The nature of vulnerability

3.1 Definition and dimensions of vulnerability

3.1.1 The FCA's definition

The FCA defines a vulnerable customer as: "someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care."

This definition has two components: the customers' 'personal circumstances' and their 'susceptibility to harm'. Too often, the focus is only on the circumstances (the vulnerability itself) without considering the specific harm these could lead to.

To operationalise this definition most effectively, and determine the adequate support firms should be providing to customers, it is useful for firms to answer three questions when devising their customer vulnerability strategy:

1. **Vulnerable to what?** Identify the specific potential harms the customer faces because of both their circumstances and their interactions with your firm.
2. **Supported how?** Determine the practical support or adjustments required to mitigate potential harm to the customer.
3. **If not us, then who?** If the required support is beyond your firm's scope, signpost the customer to an appropriate third-party (for example, a charity or support service).

GOOD PRACTICE

Adhering to UK GDPR, firms should identify and record the customer's circumstances, the associated potential harms, support on offer, and if the support was offered and adopted. This is covered in detail in **Section 5.2.4 - Data structures**.

3.1.2 Indicators of vulnerability

The FCA organises customer vulnerability into four drivers: health conditions, life events, low resilience, and low capability. The below table offers a non-exhaustive list of indicators for each driver:

Health conditions	Life events	Low resilience	Low capability
Physical or mental health conditions that reduces someone's ability to manage everyday tasks or decision-making	A major change or shock in someone's personal life	A limited ability to absorb financial or emotional shocks	Gaps in the knowledge, confidence or skills needed to understand information or make decisions
Indicators • Long-term or severe illness • Physical disability • Sensory impairment (for example, sight or hearing loss) • Mental-health conditions • Addictions • Cognitive impairment, dementia • Learning difficulties • Progressive health conditions (for example, cancer, MS, HIV)	**Indicators** • Bereavement • Relationship breakdown, separation or divorce • Serious accident • Large financial loss or gain • Job loss, redundancy or retirement • Caring responsibilities • Maternity, paternity • Changes in family circumstances • Domestic abuse, including economic abuse • Migration • Criminal conviction • Change in care circumstance • Seeking asylum • Human trafficking, modern slavery	**Indicators** • Erratic or insufficient income • Over-indebtedness, heavy credit use, mortgage arrears • No or very low savings/safety net • Low emotional resilience (stress, anxiety)	**Indicators** • Low numeracy or literacy • Limited knowledge of financial products • Low confidence in managing money • Poor digital skills • Limited English language capability • Learning difficulties

3 The nature of vulnerability

There is a fifth area of vulnerability which the FCA does not list but is included in its definition: "when a firm is not acting with the appropriate levels of care", which the following example illustrates:

Example

- **Circumstance**: A customer discloses visual impairment to a broker and receives accessible documents from the broker.
- **Firm practice**: The broker doesn't pass this new information to an insurer. The insurer sends standard renewal documents to the customer, which they cannot read.
- **Result**: The customer who disclosed their needs and expected appropriate support becomes vulnerable to policy lapses due to the firm's failure to share data effectively.

In this example, appropriate care would include structured data sharing which ensures that the customer's support needs are documented and catered for.

Vulnerabilities can both overlap and compound. For example, a single indicator like a bereavement (a life event) can snowball, triggering mental health challenges (health condition) and creating financial strain (low resilience), making the customer's situation more complex. This is covered in Section 5.2.8 - Interactions between circumstances of vulnerability.

GOOD PRACTICE

The FCA does not require firms to report on these specific categories (health conditions, life events, low resilience and low capability): they are there as examples. Firms should build vulnerability management around what exists in their customer base and target markets.

In line with the 'fifth' driver of vulnerability ("not acting with the appropriate levels of care", mentioned above) firms should also consider what practices, policies, and processes they might have (or not have) which can inadvertently create or exacerbate customer vulnerability.

3 The nature of vulnerability

3.1.3 Vulnerability is not binary

Vulnerability exists on a spectrum, from mild to severe, and may be temporary, recurring or permanent. Binary 'yes' or 'no' labels do not capture the complexities of vulnerabilities nor determine ways to deal with these. As the potential for harm varies with severity, and differs across products and services, firms should record vulnerability on a scale (for example, 'not at all vulnerable' to 'extremely vulnerable'). This will allow firms to determine:

- **The extent of, and/or urgency of, support**: higher-severity vulnerabilities need faster, more hands-on interventions.
- **The type of intervention**: the same vulnerability may call for very different adjustments depending on its position on the spectrum, for example, mild compared to severe.
- **Prioritisation**: capturing severities lets firms focus their resources where need is most likely and, in doing so, can demonstrate proportionality to the regulator.
- **Cost and risk management**: understanding severity helps firms allocate appropriate resources proportionate to customer need, manage regulatory and reputational risk by prioritising high-severity cases, and predict operational costs more accurately when planning vulnerability support programmes.

GOOD PRACTICE

Firms need robust systems, processes and taxonomies to record and act on severity levels, including:

- Standardised taxonomies which define customer vulnerability categories, potential harms and severity scales.
- Defined processes that specify how severity levels will trigger different interventions, escalation procedures and resource allocation.
- Ongoing review mechanisms to ensure that taxonomies remain current and processes adapt to emerging vulnerabilities.

See Section 5.2 - Effective data management and systems for more information.

Example

Advisory scenario

A customer approaches a financial planner for help with managing their pension after their spouse has died.

Step 1. Assess severity: The adviser evaluates the client using a vulnerability assessment tool. A client in their late 70s, newly bereaved, visibly distressed, and with no prior experience managing finances is flagged as high severity due to both emotional and capability vulnerabilities. A bereaved client with established investment experience would likely rate lower on the spectrum.

Step 2. Tailor support: Approaches addressing high-severity vulnerability might include priority face-to-face appointments, with extended time. Plain language, a slower pace of communication, and the presence of a family member can also help improve the outcome of the meeting. Another support is to schedule a check-in after six months.

Lower-severity clients, meanwhile, might receive digital resources, a comprehensive one-off meeting and a routine follow-up.

Insurer scenario

A customer informs their insurer that their partner has recently passed away.

Step 1. Assess severity: The firm uses a vulnerability scale to evaluate impact. Losing a partner who was the primary income earner and policyholder scores in higher severity than losing a parent, reflecting greater financial and emotional disruption.

Step 2. Tailor support: High-severity cases might receive a single point of contact and support from a specialist bereavement team that manage policy changes and claims on their behalf, with relaxed documentation deadlines.

Lower-severity customers might receive clear guidance and online self-service options.

3 The nature of vulnerability

3.2 Understanding harms and needs

Customer vulnerability is contextual. People are not always inherently vulnerable; harm can arise, for instance, when customer circumstances intersect with a firm's specific services. By example, a customer with a gambling addiction faces less potential harm when buying life insurance cover, which can be cancelled later, than when offered high-risk investments or instant credit.

GOOD PRACTICE

The table below maps links between circumstances, firm activities, potential harms, support needs, implementation and outcomes, providing a more detailed account of the relationship between these elements.

Step	What to capture	Example
Circumstances	Health, capability, life events, financial resilience.	Early-stage dementia is affecting the customer's short-term memory and comprehension.
Firm activities	Product, channel, moment in journey.	The customer's home insurance policy is due for annual renewal. Renewal documents are sent by email with a requirement to confirm any changes and pay the premium by a set date.
Potential harm	Foreseeable detriment if no adjustment is made.	The customer may overlook the email or forget to act, causing the policy to lapse. • If the policy automatically lapses, any subsequent claim (for example, fire or theft) would be declined, creating severe financial loss. • Late disclosure of material facts (for example, new high-value items) could invalidate cover.
Customer support need and implementation	Practical adjustments that remove or reduce potential harms.	There are many options, for example: • Set up third-party authority so a trusted relative also receives renewal notices and can confirm cover details. • Provide multi-channel reminders (letter and text message) well before the lapse date. • Offer auto-renewal with a cooling-off period, reducing the chance of unintentional lapse. • Use plain-language summaries and a dedicated helpline to walk the customer (and carer) through any changes. • Ensure auto renewals don't progress year-on-year without confirmation they are still appropriate.
Outcome	The outcomes measures	Lapse data

3 The nature of vulnerability

Some scenarios like major shock events might require temporary but urgent interventions.

Case Study: house fire and insurance claim

Circumstance: a single parent experiences a major house fire that destroys their home and possessions, leaving the family displaced with no immediate financial resources.

Firm activities: the insurer processes the major loss claim, coordinating multiple parties (loss adjusters, contractors, accommodation providers, etc.). Standard procedures require the customer to provide detailed evidence, respond to multiple assessors, and navigate technical claim processes while displaced from their home.

Potential harms:

- **Communication barriers**: multiple contacts from different parties using technical jargon overwhelm the customer.
- **Repeated trauma**: the customer is forced to retell the traumatic details to each contact, reliving the event unnecessarily.
- **Extended displacement**: delays in approving temporary accommodation or protective works (scaffolding, boarding up, etc.) prolong the family's housing instability and worsen property damage.
- **Financial strain**: facing increased costs (temporary housing, replacing essentials, etc.), the customer experiences financial pressure while awaiting claim settlement.
- **Isolation**: insufficient signposting to emotional and financial support leaves the family managing complex trauma alone.

Support needs:

- **Single point of contact**: assign a dedicated claims handler who communicates in plain, empathetic language.
- **Urgent temporary accommodation**: fast-track suitable alternative housing ensuring stability for the family.
- **Trauma-informed evidence gathering**: consolidate evidence requests into one conversation, offer written statement options instead of repeated verbal accounts, and allow flexible timing for information provision.
- **Proactive vulnerability assessment**: check for additional impacts, for example, childcare needs, financial strain and mental health impact, and offer appropriate assistance or signposting.
- **Support signposting**: connect the customer with relevant support services.

Outcome measures:

- **Claim cycle time**: improve time from notification to property reinstatement compared to benchmark.
- **Complaint rates**: reduce complaints per major loss claim.
- **Customer feedback scores**: post-claim satisfaction focusing on 'felt supported during difficult time.'
- **Long-term retention**: customer retention x months after major claim.

4 Operationalising regulatory requirements

4.1 Regulatory requirements

UK regulatory requirements span two FCA documents: FG21/1 Guidance for firms on the fair treatment of vulnerable customers (2021), which focuses on individual customer treatment, and FG22/5 Final non-handbook guidance for firms on the Consumer Duty (2022), which sets higher standards at the firm level and incorporates vulnerability principles. Firms need to comply with both.

In a speech at the Personal Investment Management & Financial Advice Association (PIMFA) Customer Vulnerability Conference on 24 October 2024, the FCA competition director Graeme Reynolds said that having a vulnerability strategy is "good practice" to support strategic direction and a culture that delivers good outcomes for vulnerable customers. He emphasised that the foundational step is identification, stating that:

"You can't begin to think about how to deal with vulnerability, how to meet your clients' needs, if you haven't first considered which of your clients might be vulnerable and why."

GOOD PRACTICE

The FCA considers the following framework as a good-practice approach firms can adopt operationalise regulatory requirements:

1. **Identify:** determine which customers may be in a vulnerable circumstance and then understand the drivers of that vulnerability. Firms should use this knowledge to build a customer vulnerability strategy which identifies the most at-risk customers, prioritises interventions and establishes clear policies.
2. **Quantify:** understand the scale and types of vulnerable circumstances customers (within their target market) might experience.
3. Monitor: continuously measure the impact of these actions on customer outcomes to confirm whether they work as intended.
4. **Support:** provide appropriate support to vulnerable customers to remove or reduce any potential harms.
5. **Adapt:** firms should adapt their products and services when their monitoring identifies poor outcomes.
6. **Report:** demonstrate that vulnerable customer cohorts are achieving outcomes as good as non-vulnerable customers, including evidence of actions taken when outcome gaps are identified.

The following pages cover this framework in detail.

Although not defined by the FCA, to be able to monitor and support customers effectively, firms need consistent data. This can be achieved by adopting a method for classifying customer circumstances and vulnerabilities.

Section 5.2 – Effective data management and structures covers this in detail.

4 Operationalising regulatory requirements

4.2 Operationalising customer vulnerability management within the firm

Both firm-level data and individual customer-level data can be used for vulnerability management:

- **Firm-level data** is required for reporting to help quantify, prioritise and plan improvements. Firm-level customer vulnerability management includes the stages of quantification, identification, monitoring and adaptation of products and services previously outlined.
- **Consumer-level data** is required to support each vulnerable customer. Vulnerable customer management at this level includes the stages of identification (including classification), monitoring, support and reporting.

Consumer-level data can be aggregated to provide firm-level data. Some firm-level data can be obtained by surveys and similar means.

4.2.1 Identify customers in vulnerable circumstances

4.2.1.1 Philosophical approach

According to the FCA's Financial Lives survey (2022), around 50% of UK adults display at least one characteristic of vulnerability at any given time and all individuals face vulnerabilities throughout their lives[2].

Given this prevalence, firms should adopt the perspective that all customers have an 'unknown' vulnerability state until assessed, meaning that any customer could be experiencing vulnerable circumstances at any time.

Where vulnerability is identified, firms should record this information systematically to ensure that appropriate support can be provided across touchpoints and over the product lifetime.

4.2.1.2 Who is responsible for assessing customers' vulnerabilities?

In an intermediated market, the manufacturer, the intermediary, or a specialist third party, can conduct the customer vulnerability assessment. Whatever the model, data-sharing protocols and contractual terms should make clear who captures, stores, updates and uses vulnerability data, as well as how customer consent is managed. Assuming that it is another firm or person's responsibility means that no one could be doing it.

4.2.1.3 Data collection: direct versus indirect

Firms can gather vulnerability information by engaging with customers directly or by using indirect data sources.

- **Direct (customer-led)**: this can be done through questionnaires, scripted calls, online self-disclosure and front-line observation. This approach is subject to customers disclosing their circumstances and requires suitable systems to record, and act, where vulnerabilities are identified.
- **Indirect (data-led)**: this can be inferred, for example through internal transactions, open-banking feeds revealing patterns such as gambling spend or from credit files and arrears alerts. This approach provides an 'always-on' early warning system and is generally reliant on financial data. This means it offers little insight into non-financial indicators such as most health issues and negative life events.

Indirect techniques have a role in identifying vulnerable customers and assembling data, but profiling customers 'behind their backs' can also undermine trust. Direct, transparent engagement remains the gold standard.

2. This is the driver or existence of a characteristic/circumstance that means that someone may be vulnerable to harm. It does not mean they are experiencing harm currently or will go on to. It is a risk factor for harm, rather than a guarantee of it.

4 Operationalising regulatory requirements

4.2.1.4 Identification: reactive versus proactive

Firms can employ reactive and proactive approaches to collecting customer vulnerability data. The table below explores the practical differences between the two methods.

Aspect	Proactive identification	Reactive identification
What are they	Delivered through planned outreach using scheduled reviews, surveys and systematic data analysis.	Triggered by customers' interactions with front-line staff or red-flag events – including voice or text analytics.
How to depoy	**Systematic outreach programmes:** • Vulnerability surveys sent to customer segments • Scheduled review calls based on risk (for example, quarterly or annually) • Life-event monitoring through publicly available records (for example, deaths or change of address) • Financial stress indicators from transactional data analysis **Data analytics approach*:** • Behavioural pattern analysis (for example, spending changes or missed payments) • Demographic profiling for life-stage transitions • Predictive modelling for vulnerability likelihood **Any inferred insights should be verified directly with the customer* **Targeted interventions:** • Automated surveys triggered by severity indicators of life events • Proactive outreach to customers who are approaching retirement • Health and financial resilience questionnaires • Regular check-ins for previously identified vulnerable customers	**Technology solutions:** • Call monitoring software with keyword detection (for example, distress, financial difficulty, health mentions) • Chat analytics for emotional tone and vulnerability indicators • CRM system flags for complaints patterns or service usage spikes • Staff alert systems for immediate escalation **Process implementation:** • Equip front-line staff with customer vulnerability identification skills • Create standardised handover protocols for specialist teams • Implement same-day response procedures for high-severity cases • Establish clear escalation pathways with defined timeframes **Staff training:** • Role-play scenarios for recognising verbal and written distress cues • Active listening techniques for phone and face-to-face interactions • Documentation of requirements for vulnerability indicators • Empathy training and appropriate response protocols
Suitable for	**Optimal for:** • Prevention and early-intervention strategies • Identifying hidden vulnerabilities which customers haven't disclosed • Long-term relationship management and support planning • Understanding emerging vulnerability trends across your customer base • Customers who may not proactively seek help due to pride, stigma or lack of awareness **Best deployed when:** • You have stable, long-term customer relationships • Your products or services have long-term impacts (for example, mortgages, pensions, investments) • You want to build comprehensive vulnerability intelligence	**Optimal for:** • Immediate support needs • Acute vulnerability episodes requiring urgent response • Customers who actively seek help or express distress • Situations where timing is critical (for example, bereavement) • Building staff expertise through real-world experience **Best deployed when:** • You have strong frontline customer interaction • Customers regularly contact your firm • Your products or services have high emotional impact • You need to respond quickly to prevent harm

GOOD PRACTICE A hybrid model of both proactive and reactive identification methods typically delivers the best outcomes and enables comprehensive monitoring of those outcomes. Proactive identification ensures that all customers are approached to be assessed, while reactive identification is useful for picking up changes.

4 Operationalising regulatory requirements

4.2.2 Quantify the scale and circumstances of vulnerability

Firms are required to understand the "nature and scale of characteristics of vulnerability that exist in their target market and customer base" (FG21/1 p.9). Several methodologies can be used to meet this requirement:

Aspect	Customer surveys	Aggregated individual identification	Internal data	External data	Existing research
What it entails	Using market research and surveys to understand customer vulnerability in a 'top-down' approach.	This is a 'bottom-up' approach, which aggregates data from individual customers to build a comprehensive understanding of customers' vulnerabilities over time.	Analysing a firm's current customer data, open banking information and transactional data to identify indicators of customers' vulnerabilities.	Using external data sources, such as financial or credit information, to identify customers' vulnerabilities.	Using current research on the prevalence of issues in the general population, for example, the FCA's Financial Lives survey.
Considerations	When designed correctly, with the appropriate questions and algorithms, a survey can accurately size the extent of both permanent and temporary vulnerabilities and provide a granular understanding of underlying drivers.	Requires a consistent method for capturing and analysing customer vulnerability data.	Access to open banking can provide financial vulnerability information, and transaction data can indicate changes in life event triggers (for example, a change of address or bereavement) that can prompt customer engagement. However, this is far less effective in determining health conditions or low capability.	Typically, strong on financial vulnerabilities but poor on health and lifestyle. Bereavement information and change of address databases provide specific information.	For many firms with large customer bases the proportion of issues in the general population is likely to be reflected within their customer base.
Best suited for	Larger firms, those without direct customer engagement, or those managing 'back-book' portfolios.	Firms with direct customer interactions.	Monitoring changes over time for firms with transactional data (for example, banks and investment firms).	Identifying financial vulnerabilities on an ongoing basis; useful for monitoring.	For smaller firms that might never (or rarely) come across issues; though they can still use research to prepare for such events.

Socioeconomic data can be used to model where customers may be more likely to experience vulnerability - for example, in less affluent regions or areas with higher unemployment. This type of data can be useful for targeting outreach programmes to identify individuals who may be at a higher risk due to their personal circumstances.

However, socioeconomic profiling has limitations: correlation at the population level does not always reliably predict individual circumstances. Under UK GDPR, firms should not record assumptions based solely on socioeconomic proxies as factual vulnerability data. Such inferences may fail data accuracy requirements unless verified through direct contact with the individual customer.

4 Operationalising regulatory requirements

GOOD PRACTICE

For larger firms and product providers, rather than relying on a single method of gathering vulnerable customer data, the most robust strategy is often a hybrid.

For example, a firm might use transactional data to identify customer segments that may be at higher risk, then deploy targeted surveys or direct engagement to verify the customer's actual circumstances and needs before recording vulnerability data or adapting service delivery.

Smaller firms (for example, advisers and brokers) are more likely to understand individual customers and collate individual data to form firm-level data.

4.2.3 Monitor customers in vulnerable circumstances

FCA Consumer Duty requires firms to monitor vulnerable customers over the product/service lifetime, both reactively (for example, when issues arise) and proactively (for example, through planned reviews). Systems should record changes and maintain an evidence trail.

The frequency of proactive reviews should be proportionate to each firm and customer circumstances. Good starting points for proactive reviews can include:

- **Financial planners**: annual reviews that are aligned with existing review cycles with ad-hoc reviews triggered by significant life events (for example, divorce, bereavement or redundancy).
- **Annual insurance products**: reviews take place at renewal.
- **Long-term products** (for example, savings and protection insurance): reviews take place every few years unless customer circumstances change.
- **High-risk situations**: more frequent reviews for customers in arrears, making claims, or experiencing major life changes.
- **Technology-enabled monitoring**: automated triggers are increasingly available to alert firms when intervention may be needed. These can include:
  - Life event data (for example, bereavement registers, change of address and employment changes).
  - Transaction pattern changes (for example, income reduction and debt increase) where firms have access to transactional data (for example, banks and investment platforms).
  - Customer interaction patterns (for example, missed payments and increased contact frequency).

For smaller firms (for example, advisers and brokers) with regular customer contact, annual face-to-face or phone interactions may suffice, supplemented by reactive monitoring when customers disclose changes.

GOOD PRACTICE

The assessment of vulnerabilities requires ongoing monitoring of customer circumstances to track whether they have changed over time. The frequency of the assessments should be proportionate to the potential for harm: customers at risk of high-severity vulnerability levels or those using higher-risk products require more frequent review, while those with lower vulnerability indicators may need only periodic reassessment. This dynamic approach recognises that vulnerability is fluid and ensures firms can respond promptly when customer circumstances change.

4 Operationalising regulatory requirements

4.2.4 Adapt products and services

When poor outcomes are identified and customer vulnerabilities documented, firms should adapt their products and services. However, to mitigate poor outcomes in the first instance, products and services should (from the outset) be designed with vulnerable customers in mind. This is achieved through two complementary approaches:

Approach	Inclusive design	Personalisation
Philosophy	Designing for all.	Designing for the individual.
Goal	Make a product or service more usable for everyone, which may disproportionately benefit the vulnerable.	Adapt a product or service to meet a specific person's identified needs.
Method	Universal changes implemented for all users.	Tailored modifications for individuals based on their circumstances.
Example	Using plain English and accessible numbers in all communications.	Sending Braille documents to a customer who can read Braille.

In practice, those responsible for product and service development are better placed to do more by using 'inclusive design' on the products and the communication of the products. Advisers and brokers, meanwhile, will more likely use 'personalisation' approaches. Effective and efficient systems blend both approaches, using inclusive principles as the standard, while incorporating the flexibility to personalise support where needed.

GOOD PRACTICE

Inclusive design teams prioritise creating usable products, services and environments for as many people as possible, especially those traditionally excluded. Often, people with lived experiences are involved in the design process. In the context of financial services and vulnerability this means considering a wide range of needs from the outset, including:

- **Understanding customer vulnerability**: you first need to understand the characteristics of vulnerability that apply to your target market. Low financial resilience may not be an issue for your target market, but low financial capability could be.
- **Cognitive**: designing for different levels of literacy and cognitive processing, using clear and simple language, avoiding jargon and structuring information logically.
- **Sensory**: considering visual and auditory impairments, offering alternative formats (for example, large print, transcripts and audio versions) and ensuring sufficient colour contrast and clear audio.
- **Physical**: ensuring online interfaces are navigable by those using assistive technologies and that any physical processes are accessible.
- **Digital skills and access**: recognising varying levels of digital literacy and access to technology and providing offline alternatives or support to digital processes.
- **Language and culture**: considering diverse linguistic backgrounds and cultural contexts, ensuring clarity and avoiding culturally specific language or assumptions.

4 Operationalising regulatory requirements

4.2.4.1 Prioritising improvements based on identified poor outcomes

At any given time, firms may identify multiple poor outcomes requiring attention. Solutions may vary in complexity, from simple process adjustments to major changes involving distribution partners, outsourcers or sector-wide initiatives.

Before prioritising solutions, firms should understand why poor outcomes occur. These can include:

- **Identification failures**: customer vulnerability detection gaps that may exist at point of sale or at other critical touchpoints might require enhanced identification processes.
- **Implementation failures**: identification of customers' vulnerabilities is effective, but the support and adjustments provided to these cohorts is not. For example, firms successfully identify customers without wills and recommend legal advice, but uptake remains low despite a sound identification process.

GOOD PRACTICE

Larger firms can use risk-management principles to prioritise activities, using a two-stage approach:

Stage 1: impact assessment

- **Customer impact**: what is the severity of harm to individual customers?
- **Volume**: what are the number of customers affected?

Stage 2: implementation assessment

- **Cost**: what resources are required for a solution?
- **Feasibility**: what is the ease of implementation; considering the time, complexity and coordination requirements?

Firms can rank solutions by combining high impact/volume scenarios with low cost/high feasibility solutions. This approach maximises positive customer outcomes while ensuring efficient resource allocation.

Smaller firms may want to avail themselves of support organisations or systems which they can call on if they need specialist support.

4 Operationalising regulatory requirements

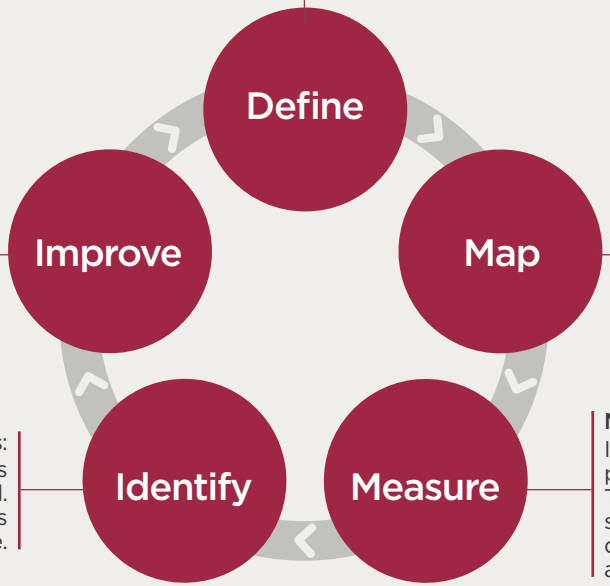
4.2.5 Report on outcomes

FCA Consumer Duty requires firms to report on outcomes for cohorts of vulnerable customers. In practical terms, firms should demonstrate that the outcomes for a particular cohort (for example, the bereaved, divorced, those suffering from domestic abuse, visually impaired, etc.) are as good as those for non-vulnerable groups.

When firms discover poor customer outcomes, they should identify the root cause and consider how to improve the product or service. Outcome reporting is a broad topic, and this document only addresses it with respect to customer vulnerability.

To monitor and act on outcomes, firms can use the following framework:

Define what 'good' and 'bad' outcomes look like:
Create a clear definition of success (the 'good' outcome) for your customers which you can embed across the business as a 'common lexicon' that everyone understands. Define the 'bad' foreseeable outcomes that you need to prevent.



Map how will you achieve it:
Outline the activities, processes and controls your firm uses to deliver these defined outcomes. This includes reviewing call centre conversations, training activities, policies and service delivery key performance indicators (KPIs).

Measure metrics to monitor outcomes:
Identify a limited set of relevant metrics which can prove that customers are experiencing good outcomes. To identify whether vulnerable customers interact with services differently, the FCA suggests sources such as direct customer feedback, complaint root-cause analysis and behavioural monitoring.

Identify those customers who experience poor outcomes:
Use metrics to identify, in a systematic way, individuals or groups who are not achieving the good outcomes you have defined. This is where the initial identification of vulnerable customers becomes critical and, without it, targeted analysis is impossible.

Improve by investigating, acting and re-monitoring:
Finally, close the loop by investigating the root cause of poor outcomes. This final stage, which the FCA refers to as the 'causal chain', requires taking corrective action to verify that the fix was effective, before restarting the monitoring cycle.

4 Operationalising regulatory requirements

GOOD PRACTICE

Using Objectives and Key Results (OKRs) to measure outcomes:

For larger firms to move beyond simply tracking activities (for example, number of staff trained), firms should adopt an outcomes-based measurement framework like OKRs. This provides a clear line of sight between the firm's actions and their impact on the customer.

- **Objective (the 'what')**: a qualitative, ambitious goal.
- **Key result (the 'how')**: a quantitative, measurable result which proves that the objective has been met.

Example OKR for vulnerable customer outcomes:

Objective: make sure that different vulnerable customer cohorts receive fair value consistently and are not disadvantaged by their circumstances.

Key results:

- **Reduce the 'vulnerability value gap'**: decrease the differential in claims acceptance rates between vulnerable and non-vulnerable cohorts from x% to below y% by year-end.
- **Improve understanding**: achieve a score of over x% on post-renewal comprehension surveys sent to those customers who have a vulnerability characteristic of low financial capability.
- **Enhance support**: reduce the average number of contact interventions required to resolve an issue for customers who have been flagged with a 'life event' vulnerability from x to y.

This framework shifts the focus from 'we have completed a task' to 'we have achieved a better outcome for customers.' It provides tangible evidence for both board reports and regulatory scrutiny.

For smaller firms (for example, advisers and brokers) the numbers of customers may be relatively small and some circumstances of vulnerability rarely experienced. Therefore, reporting by cohorts of vulnerability types will not be practical. Instead, they can report on an individual's outcomes.

The challenge for this approach is how to collate this within a distributed market where manufacturers need to understand the outcome of different cohorts.

4 Operationalising regulatory requirements

4.2.5.1 Customer outcomes versus customer experience

Customer outcomes differ from customer experience insights although the two may overlap. The Edmonds Experience versus Outcome Matrix is useful in helping firms identify the difference between measures that are service-related and those that are outcome-related. Here is an explanation of each quadrant:

- **Perfect match**: customers receive good outcomes and a good experience. For example, an insurance claim is settled promptly and fairly with empathetic, clear communication throughout the process.
- **Superficial satisfaction**: customers have a good experience but a poor outcome; and probably don't realise they have a poor outcome. For example, they may have great customer service from their insurer but are paying over the odds as they don't need the insurance, or the policy is automatically renewed at an inflated rate.
- **Painful satisfaction**: customers receive a good outcome but have a poor experience. For example, they receive a positive return on investment but experience poor response to communications.
- **Double trouble**: customers have a bad experience and a bad outcome. For example, policyholders not being paid out at the claims stage and who must hound firms to understand why.

This framework helps firms avoid the trap of measuring only customer satisfaction scores, which can mask poor outcomes hidden behind positive service interactions.

Edmonds experience vs. outcome matrix

4 Operationalising regulatory requirements

4.2.5.2 Vulnerability granularity for outcome measurement

The level of detail for measuring outcomes for vulnerable customer cohorts varies by firm and requires consideration of granularity versus practicality.

A broad categorisation (for example, 'all vulnerable customers') may capture approximately 50% of customers but it obscures the specific vulnerabilities which drive poor outcomes. This approach is insufficient to trigger targeted interventions[3]. The level of detail a firm will implement depends on four factors:

Size of the customer base	• Larger customer bases can support more granular segmentation. • Smaller customer bases may need broader categories for statistical significance.
Product risk profile	• Higher-risk products require more detailed vulnerability tracking. • Products with greater potential for customer harm need more granular monitoring.
Distribution chain data availability	• The data accessible from distribution partners will determine the level of detail firms can capture. • Quality and consistency of shared vulnerability data will determine the level of detail firms can capture.
Operational requirements	• Need to collect data to support customer service (for example, bereavement support or communication preferences). • Regulatory reporting obligations.

GOOD PRACTICE

- **Progressive refinement**: allows firms to increase granularity as both data quality and experiences improve.
- **Root cause focus**: firms should collect sufficient detail to identify the underlying causes of poor outcomes; this can enable targeted solutions rather than broad investigations.
- **Distribution chain considerations**: the lack of granular, quality data from distribution partners necessitates more resource-intensive deep dives to understand specific issues.

3. Using the FCA's Financial Lives survey as a benchmark, it identified 47% UK adults may become vulnerable at any given point in time.

4 Operationalising regulatory requirements

4.2.6 Examples of acting on outcomes

The following examples illustrate how firms can translate outcome monitoring into practical interventions, showing how identified poor outcomes drive specific improvements, and demonstrating what good outcomes look like when appropriate support is in place.

Insurance scenario: for a home contents insurance policy

Bad outcomes and required actions		
Bad outcome	**Vulnerability cohort**	**Action required**
Customers are unable to make a claim after a major home event due to lapsed policy.	Elderly or medically vulnerable homeowners who miss renewal dates because of hospital stays, cognitive decline or limited digital access.	Implement alternative renewal channels (for example, phone, in-person, trusted contact) and work with brokers to track and reduce non-renewals in this group.
Customers suffering severe financial loss due to fraudulent claims made in their name.	Victims of financial abuse where the abuser controls joint insurance accounts.	Introduce verification processes for significant policy changes, enable separation of joint policies, and flag unusual account activity for review.
Customers overpaying for cover they no longer need.	Recently bereaved customers who have not reviewed their policy after a change in household circumstances.	Introduce bereavement flags to trigger personalised renewal reviews, highlight cost-saving options and proactively contact customers where premium levels remain unchanged despite reduced risks.

Good outcomes when adequate support is in place		
Good outcome	**Vulnerability cohort**	**Support in place**
Customers' claims are settled quickly and without additional stress.	Recently bereaved customers making contents claims after burglaries.	Dedicated claims handler, clear communication and use of plain language leads to reduced stress and settlement within a week.
Customers avoided being underinsured after home improvements.	Customers with limited English proficiency and limited insurance knowledge.	Annual policy reviews conducted via an interpreter identified the need for higher cover and updated policies before loss occurred.
Customers avoided policy lapse and maintained full cover.	Customers with severe sight loss who missed email reminders.	Provided renewal documents in large print and confirmed renewal via phone calls, ensuring uninterrupted cover and peace of mind.

4 Operationalising regulatory requirements

Advisory scenario: for a retail financial planning client

Bad outcomes and required actions		
Bad outcome	**Vulnerability cohort**	**Action required**
Clients make unsuitable investment decisions due to misunderstanding of key risks.	Clients with early-stage cognitive decline or limited financial literacy.	Implement self-assessment risk questionnaires with additional checks or support of a trusted contact.
Clients miss out on important tax allowances or deadlines.	Clients with serious illness or caring responsibilities struggles to keep track of complex timelines.	Roll-out tailored communications for time-sensitive actions.
Clients receive advice they don't fully understand, leading to poor investment decisions.	Clients with limited English proficiency.	Conduct meetings with interpreters, assistive technology or plain-language summaries.
Recently bereaved clients continue with a financial plan that no longer meets their needs.	Clients who have lost a partner and haven't reviewed their circumstances.	Ensure bereavement flags in the system trigger a proactive review or additional support.

Good outcomes when adequate support is in place		
Good outcome	**Vulnerability cohort**	**Support in place**
Clients' investment portfolio is adjusted appropriately after a change in capacity.	Clients with early-stage cognitive decline.	Introduced a trusted contact protocol and annual face-to-face reviews ensuring recommendations remain suitable.
Clients received timely tax planning advice despite personal challenges.	Clients undergoing medical treatment and struggling with admin.	Added phone reminders, offers to liaise with their accountant directly and extended appointment flexibility to meet key deadlines.
Clients fully understood the advice and acted with confidence.	Clients with hearing loss.	Arranged meetings with a British Sign Language (BSL) interpreter, provided plain-English written summaries and confirmed understanding through follow-up communications.
Clients' financial plan is realigned promptly after bereavement.	Recently bereaved clients	Added bereavement flags to trigger an automatic review, provided empathetic communication and ensured appropriate adjustments to reflect changed financial needs.

4 Operationalising regulatory requirements

4.3 Operationalising vulnerability management across the value chain

Firms are responsible for customer outcomes across the entire distribution chain, requiring active collaboration with partners to review outcomes and address any risk of harm.

4.3.1 The data-sharing imperative

Effective vulnerability management depends on sharing relevant information between firms in the value chain[4]. When vulnerability data is not passed along the chain, small information gaps early in the journey can compound into significant problems, creating the poor outcomes Consumer Duty aims to prevent.

A firm's ability to share data externally depends on its internal data maturity: robust data structure and governance are prerequisites for interoperability. Firms should think strategically about data storage; simply adding fields to legacy systems may solve immediate needs but hinder future data sharing capability.

4.3.2 The duty to collaborate and report non-compliance

The FCA has embedded a powerful mechanism within Consumer Duty to enforce collaboration between firms. Where a partner firm in the distribution chain does not cooperate in reviewing outcomes or rectifying issues, the FCA expects a clear response; this may include terminating the relationship between parties.

Furthermore, Consumer Duty introduces an element of market self-governance. As stated in the FCA's handbook under PRIN 2A.2.22 R, there is a regulatory obligation to report non-compliance:

"Firms must notify the FCA where they become aware that another firm in the distribution chain may not be complying with the Duty."

This requirement effectively asks the sector to self-police compliance. Failing to report known non-compliance in another firm can in itself be considered a breach of Consumer Duty.

Example

Scenario: adviser to insurer data sharing

A customer with sight and hearing impairments needs large-print documents and SMS notifications rather than phone calls for their protection policy.

- **Without structured data sharing**: the adviser records preferences in free-text CRM notes. When the policy transfers to the insurer via PDF, these accessibility needs are buried in unstructured text. The insurer's systems cannot automatically flag or act on this information, so standard format renewals are sent, the customer misses updates, and poor outcomes result.
- **With structured data sharing**: the adviser captures preferences in standardised fields (for example: "Communication format: large-print," "Contact channel: SMS"). These map to the insurer's system via API, triggering large-print documents and SMS reminders throughout the policy lifecycle. The customer receives consistent, accessible communication across both firms.

This example represents an ideal scenario where all parties in the value chain have systems and processes capable of capturing, transmitting, and acting upon structured vulnerability data. While this level of integration is not yet widespread, it illustrates an ideal end-state.

4 The technical implementation of inter-firm data sharing is outside the scope of this document and will be covered in future CII guidance.

4 Operationalising regulatory requirements

4.4 Customer journey touchpoints

Under Consumer Duty, it is a fundamental requirement to embed customer vulnerability management across appropriate touchpoints. Relying solely on reactive measures (for example, telephone calls and emails at the point of claim or complaint) is not sufficient. A proactive vulnerable customer strategy is an effective one.

GOOD PRACTICE

Firms should incorporate customer vulnerability assessments at appropriate touchpoints:

- **During onboarding:** firms should confirm that the recommended product is suitable for the customer's circumstances; ideally before completion of a contract. Exceptions can be made so long as the characteristics of vulnerability can be accommodated after the contract is agreed.
- **During the product lifecycle**: firms should reassess at reviews and mid-term adjustments or whenever there is evidence of a material change in a customer's circumstances.
- **On completion**, at claims stage or complaints.

The priority, frequency, and nature of all these activities should be guided by the risk to the customer, based on the type of product or service (and its potential to cause harm) and lead to supportive engagement rather than simply labelling customers.

To move from principle to practice, firms can use a combination of approaches tailored to their size, complexity, and customer base. The approaches explored below can be implemented individually or combined to embed vulnerability management across customer touchpoints.

4.4.1 Map customer journeys and identify key moments

Visually map every significant customer journey (for example, new business, renewals, claims, complaints, switching).

GOOD PRACTICE

For each journey, identify 'moments of truth' where customer circumstances are most likely to change or where they may need additional support. Prioritise the touchpoints where the risk of harm is highest.

4 Operationalising regulatory requirements

4.4.2 Develop empathetic questioning frameworks

Customers typically respond positively to empathetic questioning and are more likely to share personal information when proactively engaged and understand how and why their information will be used. Hence, the best practice is to:

- Not expect the customer to volunteer information.
- Explain why the information is required and how the outcome is for their benefit.
- Detail the extent of topics covered.
- Explain how personal data is managed (UK GDPR).

Certainly, go beyond a blunt question such as: "are you vulnerable?" .

GOOD PRACTICE

For digital channels:

Place suitable questions within the journey to identify vulnerabilities. This triage can move interactions from digital to verbal or face-to-face, where appropriate. For example:

- Provide a questionnaire to assess all potentially relevant circumstances.
- Provide an escalation prompt in a live chat/chatbot for certain topics, for example: "Sometimes it's easier to discuss these things over the phone. Would you like us to arrange a callback?"
- Include reminders, reinforcing messages within the digital journey, for example: "We want to ensure that our services work for everyone. Do let us know how we might best communicate with you or how we could serve you better?"

For front-line staff:

Front-line staff should feel empowered and have the confidence (through training and/or supported by systems) to go off-script, using personal empathy on a case-by-case basis. They should preferably use open, layered questions which encourage disclosure, enabling staff to move beyond identification to starting a conversation. For example:

- Initial prompt, for example: "To make sure that we're providing the best service for you, we would like to ask you some questions to understand your personal circumstances."
- Reviews, for example: "Are there any particular needs or recent changes in your circumstances you'd like to make us aware of?"
- Reminders, for example: "Sometimes things like health issues or changes at work can make managing finances tricky. We have support options available, so please let me know if anything like that could help you."

4 Operationalising regulatory requirements

4.4.3 Launch proactive, risk-based outreach campaigns

Using customer data can help to identify those customer segments who may be at higher risk of harm because of products used, circumstances or changing economic conditions, and then design targeted communication campaigns to mitigate these potential risks.

Example

Insurance providers:

- Send a mid-year 'check-in' email to annual travel insurance customers to remind them that if their health status has changed they should declare it before their next trip to ensure that their cover remains valid.
- In response to high inflation in building costs, contact home insurance customers whose sum-insured value has not been reviewed for 2 to 3 years and prompt them to review their level of cover to ensure it remains adequate, explaining the risk of being underinsured.
- During a cost-of-living crisis, email customers who have previously missed payments to make them aware of forbearance options before they fall into arrears.
- During large scale events such as natural disasters, public health emergencies or severe weather events, email customers about the features of their products that may be relevant to the event.

Insurance brokers, financial planners and mortgage brokers:

- At onboarding, undertake a vulnerability assessment either digitally, over the phone or face-to-face to establish their circumstances.
- At annual reviews, product sales or other appropriate touchpoints, undertake a review of their circumstances to see if anything has changed.

4.4.4 Implement automated data-driven triggers

Continuously monitor customer data from both internal sources (for example, transaction patterns, digital behaviour or communications history) and trusted external feeds (for example, bereavement registers and credit scores) using algorithms which identify predetermined vulnerability indicators or any concerning patterns. Systems can generate flags that trigger protective measures; route cases to specialist teams; or initiate sensitive outreach processes when specific thresholds are met or risk factors combine.

Example

Possible examples include:

- A flag from a bereavement data service to automatically amend promotional marketing to bereaved individuals and a switch to a sensitive outreach process.
- Multiple failed direct debit attempts could prompt a notification to a specialist team to review the account and make contact with the customer before cancelling the policy.
- Several failed authentication attempts, combined with website or app visits to help pages, can trigger accessibility support outreach.

4 Operationalising regulatory requirements

4.4.5 Empower staff, using clear protocols and systems

To ensure thorough consistent customer vulnerability management, staff need systems support and training to know exactly what to do. Training alone is unlikely to be sufficient; staff also need the right tools. Systems can assist with identification, classification, monitoring, support and reporting.

GOOD PRACTICE

Firms should identify and record consumer circumstances, the firm's activities, the associated potential harms, the support offered and whether the support was taken up.

There should be clear, simple escalation paths for complex cases.

Some firms have appointed 'champions' or specialist teams who are available for consultation on systems which can automatically prompt next 'best steps' depending on relevant triggers.

4.4.6 Offer accessible disclosure channels

Provide a range of secure and accessible channels for customers to self-disclose information, recognising that digital-only solutions will exclude some customers and create foreseeable harm.

GOOD PRACTICE

Alongside a secure form within a customer's online account portal, firms should clearly signpost non-digital alternatives. This might include offering a dedicated telephone number to speak with a trained agent or providing the option for customers to request and return a paper form by post. This multi-channel approach ensures all customers, regardless of their digital capability or confidence, have a private and convenient way to share their circumstances.

4.4.7 Establish continuous feedback and quality assurance

Regularly gather customer feedback to test whether your processes work as intended.

GOOD PRACTICE

Use a combination of deep dives, call-monitoring, case file reviews and customer feedback surveys to assess both the process and the outcomes. Ask for examples: "How easy was it to get the support you needed from us?" or "How often were you required to retell your circumstances?"

5 Enabling elements

Firms may need to adopt practical and cultural approaches to embed adequate support for vulnerable customers. This might include ensuring that their leadership is visible and accountable, that systems and processes enable the right data to be managed compliantly, and that ongoing vulnerability training is embraced across the organisation.

5.1 Leadership, culture and governance

Effective leadership and culture are essential to embedding customer vulnerability management into a firm's strategy and decision-making, driving genuine customer centricity rather than existing as a tick-box exercise. This section explores elements across leadership, culture and governance and suggests good practices and actions that firms and individuals can take.

At this point it may be useful to self-assess your customer vulnerability management maturity using the checklist in Appendix 1.

5 Enabling elements

Element	What good looks like	Practical actions/evidence
Tone from the top	Board and executive committee explicitly state that fair treatment of vulnerable customers is a core measure of success.	• Annual board paper on customer vulnerability performance and forward planning. • Chair and CEO visible in internal campaigns. • Annual Consumer Duty board report.
Clear accountability (SM&CR)	A named Senior Manager function (usually SMF1, SMF3 or SMF17) which holds overall responsibility and individual business-unit leaders with secondary accountabilities.	• Management responsibilities are clearly identified. • Objectives and remuneration include customer vulnerability KPIs.
Governance structure	Regular governance forum (for example, a customer vulnerability steering committee) with cross-functional representation that reports into the conduct or risk committee.	• Standing agenda items covering management information, root-cause analysis, remediation and customer voice.
Culture & behaviours	All relevant staff (not just those at the front line) understand why customer vulnerability matters and feel empowered to act.	• Values and code of conduct reference customer vulnerability duties. • Reward and recognition for exemplary support cases. • Talking with staff about vulnerabilities that exist within the workforce.
Risk management integration	Customer vulnerability is included in the conduct risk framework and the Own Risk and Solvency Assessment (ORSA) for insurers. Material risks are recorded, owned and tracked.	• Risk registers show specific customer vulnerability risks with controls, owners and target dates.
Management information and escalation	Timely management information highlights exposure, trends and emerging harms. Red flags trigger rapid escalation to senior management.	• Dashboards segment outcomes by customer vulnerability drivers and severity. • Defined escalation matrix for urgent cases. • Board-level reporting includes a dedicated 'vulnerable customer outcomes dashboard' based on an Objectives and Key Results framework. To identify and challenge any outcome gaps, this dashboard should compare key results for vulnerable versus non-vulnerable cohorts.
Third-party oversight (for product providers only)	Brokers, advisers, third-party administrators and other suppliers should meet the product provider vulnerability standard. Service-level agreements, audits and reporting cover this explicitly.	• Due-diligence checklist and ongoing assurance reviews include customer vulnerability questions. • Sharing outcome data, and working on improving poor outcomes, when these are due to issues across the value chain.
Continuous learning	Governance forums commission deep-dive reviews following incidents. These insights feed policy, training and product design.	• Post-event reviews are documented and tracked to closure.

Application of the above-named approaches should be proportionate to the context of the firm's operations. Not every recommendation will apply in the same way for all firms and will vary by a firm's size and complexity and their position in the distribution chain.

5 Enabling elements

GOOD PRACTICE

There are multiple ways to influence organisation culture. Some typical examples regarding customer vulnerability include:

- Management promotes and champions support for vulnerable customers.
- Targets don't just drive revenue, they promote support for vulnerable customers.
- Discussions examine what support to provide to vulnerable customers, when to provide it and which budgets to apply.
- Internal awards recognise outstanding staff behaviour towards vulnerable customers.
- Stories (positive and negative) are used internally to give examples of how vulnerable customers were treated.
- Using data to prove that better support for vulnerable customers reduces complaints, prevents claims abandonment, improves retention and lowers operational costs.

5.2 Effective data management and systems

Effective customer vulnerability management, as emphasised by the FCA, requires suitable systems to store, manage and analyse customer data. This section outlines considerations for building a robust data framework. Refer to Appendix 2 for a customer vulnerability data framework checklist.

5.2.1 UK GDPR compliance

All management of customer vulnerability data must comply with UK GDPR. While the fear of non-compliance and fines can be a barrier, UK GDPR does not prevent the storage of customers' vulnerability data. It does require that this data is managed appropriately, under a lawful basis (for example, 'explicit consent'), with robust security and clear governance; and with respect for the data subject's rights. The key is to build or procure compliant systems, not to avoid collecting necessary data. The CII and FCA are respectively working on further guidance on this topic.

5.2.2 Data quality and accuracy

It may sound obvious, but if a consumer's basic contact information is not correct then it is unlikely that any vulnerability data will be. Contact data specialists LexisNexis say that such data decays at around 10%-15% a year because of normal circumstances such as people moving, deaths, divorce, separation etc. Maintaining up-to-date contact information is a basic step in ensuring data integrity.

5.2.3 Objectivity and classification

To be useful across an organisation, customer vulnerability data should be consistent and objective. Subjective, free-text assessments and records may solve an immediate issue for one member of staff, but can create other issues:

- likely to be difficult to aggregate for Consumer Duty reporting.
- likely to be in an unsuitable format to communicate to a third party.
- may be difficult for others to understand.
- may include subjective opinions.
- may not meet the UK GDPR's data accuracy requirements.

GOOD PRACTICE

Firms should adopt objective vulnerability assessment methods and record data consistently, excluding subjective opinions that could breach UK GDPR data accuracy requirements or create inconsistency.

This is best achieved through adopting a standardised classification system or taxonomy to describe the customer's vulnerability circumstances and their severity, ensure consistency, enable analysis, facilitate communication with others (including across the value chain) and meet UK GDPR data accuracy requirements.

Most data should be structured (enabling aggregation, reporting and automated triggers) and should be supplemented by free-text fields for elements that don't fit predefined categories.

5 Enabling elements

5.2.4 Data structures

When designing or buying IT systems, firms should ensure that they can both capture and manage a rich dataset of customer circumstances. The following data elements provide a comprehensive model:

Component	Description	Example
Primary circumstance	An objectively assessed characteristic or circumstance of a consumer, including health, financial and life events.	Recently made redundant due to poor health.
Secondary circumstance	More detail on the circumstances, including customer ability to engage and understand, as well as their resilience and capacity.	Has a poor understanding of financial matters; does not have a source of financial advice.
Severity of circumstance	The severity of the above circumstances should be measured from 'extremely vulnerable' to 'not vulnerable'.	Combination of job loss and health issues creates a high level of vulnerability.
Demographics and preferences	Factual information about customer demographics, situation and preferences, for example, marital status and employment status.	Single, prefers online communication.
Current coping mechanism/need	How customers overcome their vulnerabilities; their need or preference.	Turn off the heating, uses credit card.
Firm activity	The interaction between the firm and consumer.	Advising on, selling or servicing a financial product.
Potential harm	The potential harms that may occur from the combination of the consumer's characteristics and their circumstances.	Consumers making rushed uninformed decisions may turn to money lenders or high-cost credit.
Support pathway	The support, signposting that could be provided.	Guidance for payment holidays, finding benefit entitlements.
Support triggers	The combination of factors: the characteristics, severity, circumstances and demographics which trigger a support pathway.	Change in life events, loss of income, lack of professional advice.
Support pathway result	If the support pathway was recommended and if it was taken up by the consumer.	Payment holiday taken up, benefits realised.
Outcome	If the customer received a good or poor outcome.	Immediate cash flow issues overcome; feels more in control and able to plan for a new job.

5 Enabling elements

5.2.5 Overcoming the data minimisation requirements

Firms may perceive a conflict between Consumer Duty reporting obligations and the UK GDPR data minimisation principle. This can be resolved using a tiered system for recording and sharing vulnerability information, similar to how credit scoring provides an actionable rating without disclosing the underlying financial detail.

Such a model can operate within the firm and between firms, as explained here:

- **Within firm role-based access**: a high-level indicator (for example, a flag, colour code or simple rating) can be shared widely within the firm. This allows all relevant staff to know that a customer may require special consideration, without any access to sensitive personal data. Any specific, detailed information is reserved for specialist teams who require it to provide tailored support, operating on a strict 'need-to-know' basis.
- **Inter-firm data sharing**: this tiered system enables firms to share the high-level indicator with third parties in their distribution chain. This ensures that a customer's vulnerabilities are recognised and managed throughout their entire journey. This fulfils the FCA's requirement for comprehensive lifecycle management whilst respecting data privacy.

This table below shows a practical example of implementing this multi-tiered system:

Level	Level of detail	Example	Who might access this data
1	Vulnerable or not.	Yes/no.	All staff; no limits.
2	Need.	Ensure a family member or carer is present.	Anyone who may encounter the consumer.
3	Vulnerability scale, for example, very vulnerable.	Very vulnerable.	Most staff who encounter, or influence, customers.
4	Topic level, for example, health, financial, life events.	Health.	Staff who encounter the customer but don't have any say on actions to be taken.
5	More detail on the characteristic and its severity.	Severe mental health.	Staff who prescribe actions to be taken for the client.
6	Full detail, including severity and how it affects the consumer; and any mitigating strategies, if known.	Severe bipolar. On medication.	Only those staff involved in prescribing a service for the individual.

Smaller firms (for example, small financial planning or broking firms) may not need as many levels of granularity for their own purposes. However, this may be required when sharing data with outsourced partners such as para-planning firms. In addition, there may be a need to share data with networks and manufacturers.

5.2.6 What data to store: customer circumstances or support needs

A common debate is whether to store the underlying circumstance (for example, the customer is visually impaired) or only the required support need (for example, provide documents in Braille). While only storing the need may seem to reduce UK GDPR risks, this is usually a false economy because:

- The need often implies the circumstance, meaning it is 'special category data' (for example, example, medical data) around which there are stricter UK GDPR rules.
- A support need for one product or service may not apply to another.
- Customer circumstances may change over time.
- The products recommended or provided may change over time.
- The support needs which a firm (or others in the value chain) provides may change over time.

GOOD PRACTICE

Storing both 'circumstances' and 'needs' allows firms to more easily adapt their support as new risks or solutions emerge.

5.2.7 Managing individual vulnerabilities in family groups

Financial decisions are often made at the household level (for example, mortgages, pensions and loans), so systems that link individuals as a household unit and capture relationship dynamics (for example, caring responsibilities, single-income dependencies and power imbalances) enable a more holistic vulnerability management.

Deciding whether to group household members will depend on the dynamics of the group. For example, a group of students living together will probably not be appropriate to combine, even if they share the contents insurance for a premise. However, a family with an adult with Downs syndrome (whom they look after) may well benefit from being linked together, even if they live separately. Understanding a family group may also help to understand dynamics of coercive behaviour and abuse that may go unnoticed if data is only stored on individuals.

5 Enabling elements

5.2.8 Interactions between circumstances of vulnerability

The circumstances vulnerable customers may experience are often complex and overlapping. For example, a life event such as bereavement or relationship breakdown may trigger mental ill-health or low financial resilience, compounded further if the customer has low capability to manage finances or engage with financial services.

The FCA identified three main models of how a customer's vulnerabilities interact and compound harm:

1. **Parallel paths**: different vulnerabilities coexist independently, each creating separate challenges but without exacerbating one another directly. Effective firm practices can manage these vulnerabilities individually, preventing escalation.

2. **Root driver**: one primary customer vulnerability significantly drives or intensifies others. Addressing the root cause in the most effective way can mitigate risks arising from downstream vulnerabilities.

3. **Vicious circle**: customer's vulnerabilities interact in a cyclical manner, continuously worsening their situation over time. Whilst there may be a root cause that triggered the process, the lived experience continues in a cycle. Early intervention from firms is crucial to break or prevent this cycle and additional care is required to address derivative vulnerabilities once the cycle is in motion.

GOOD PRACTICE

It is not necessary to identify or record which model of interaction is occurring, but we do recommend that firms' systems and processes can cope with multiple circumstances and multiple support needs.

Firms should identify and prioritise interconnected vulnerabilities within their management systems. By recognising these compounding factors organisations can prioritise support and reduce the risk of cumulative harm

Firms should customise their customer vulnerability management systems to align with their specific product offerings and service models, ensuring that interventions effectively prevent harmful interactions between different vulnerable circumstances. Even small adjustments, such as personalised communications channels and responsive support teams, can substantially improve outcomes, while building deeper customer trust and loyalty.

5 Enabling elements

5.3 Training and capability building

Effective support for vulnerable customers requires a whole-organisation approach. Training cannot be limited to customer-facing teams or be a one-off compliance exercise.

Firms should measure and record employee competence and understanding to ensure training is not just implemented, or completed, but has measurable outcomes.

5.3.1 Scope of training

Training should be role-specific and extend across all levels, from entry-level employees to senior leadership. Training will be different for frontline and non-front-line staff.

- **Frontline staff**: for example, customer service, sales and claims handlers. The team should identify, understand and respond to vulnerability effectively, ask sensitive questions and provide appropriate support and signposting.
- **Non-frontline staff**: for example, product development, marketing, IT, AI governance, compliance and senior management. The team should embed customer vulnerability considerations in product design, communication strategies, system development and the overall firm strategy and culture.

GOOD PRACTICE

Firms should ensure that vulnerability training is firm-wide and role-appropriate. For example, frontline training should cover recognising disclosure cues and handling conversations empathetically, while product teams should learn how to design frictionless customer journeys that anticipate vulnerability.

5.3.2 Training content

Training should include:

- **Understanding customer vulnerability**: the FCA's definition of customer vulnerability; the different types of vulnerabilities; and how vulnerabilities can impact customer interactions, decision-making and outcomes.
- I**dentifying customer vulnerabilities**: recognising potential indicators of vulnerability, understanding disclosure barriers, and asking both sensitive and appropriate questions.
- **Responding to customer vulnerabilities**: knowing firm's policies and procedures for supporting vulnerable customers, providing tailored support, signposting to specialist services and escalating complex cases.
- **Customer vulnerability data management**: knowing which vulnerability data can be recorded and processed responsibly and ethically and in line with data protection regulations.
- **Inclusive communication and accessibility**: principles of clear communication and accessible service delivery.
- **Monitoring outcomes**: understanding how data should unearth insights, drive improvements and report on outcomes.

GOOD PRACTICE

While comprehensive training is essential, firms should measure its effectiveness to prove it is delivering better outcomes and driving change, rather than being a compliance exercise. The real question is not: "was the training completed?" but rather, "did the training improve customer outcomes?"

Firms can measure this, using both leading and lagging indicators, for example:

Leading indicators (measure behaviour change):

- An increase in Quality Assurance scores for empathy and patience during calls with vulnerable customers.
- A measurable increase in the proactive identification and correct logging of a customer's vulnerability characteristics by front-line colleagues.
- A reduction in call escalations from front-line agents to specialist support teams.

Lagging indicators (measure customer outcomes):

- A decrease in complaints related to colleague misunderstanding of vulnerable customer cohorts.
- An increase in post-interaction survey scores from customers who received support.
- A reduction in the number of times a vulnerable customer must disclose their circumstances within the value chain.

If the leading indicators improve, but the lagging indicators do not, it is a clear signal that the training content or another part of the process is failing. Simply repeating the same (or similar) training is not a solution. There should be clear evidence that firms continue to learn, adapt and improve.

5 Enabling elements

5.4 Vulnerability disclosure: creating a positive environment

Creating a positive disclosure environment is crucial for positive customer engagement. This involves actions, messages and instructions that encourage customers to share their circumstances. Several reasons might deter customers from disclosing information:

- Fear of stigma and judgment: customers worry about negative perceptions resulting from disclosing conditions like mental illness.
- Fear of discrimination: customers fear unfair treatment, such as being denied coverage or receiving higher premiums.
- Emotional discomfort and complexity: disclosure can be distressing, especially when filling in complex forms.
- Mistrust: scepticism about the firm's motives can deter honest disclosure.
- Past experiences: Negative past interactions can make customers reluctant to disclose.

A good model is that of a value exchange. Consumers are more likely to share data if they think there is value for them or their peer group. It is important to communicate and demonstrate this value for customers to encourage them to disclose their circumstances and needs.

GOOD PRACTICE

To encourage trust and disclosure, organisations should:

- **Serve customers**: firms should use customer vulnerability data primarily for the purposes of protecting the consumer. Any organisational protection should be strictly secondary, justified and handled with exceptional care.
- **Educate customers**: firms should weave clear and concise explanations of why vulnerability information is requested should be woven into every touchpoint. Periodically remind customers how disclosure benefits them.
- **Provide reassurance**: firms should reassure customers that disclosures will be received constructively and respected ; and acted upon with genuine concern for their circumstances.
- **Design proactive digital prompts**: online journeys should include prompts that encourage vulnerability disclosure at appropriate touchpoints, not just as checkboxes within terms and conditions.
- **Ensure transparency**: in plain language, firms should inform customers why they collect vulnerability data, what they use it for, their lawful basis under UK GDPR (for example, consent, legitimate interests) and who they will share it with. This information should be accessible and not buried in fine print.
- **Empower customer control**: ideally firms should have systems which enable customers to control their own data. Consumers should be able to choose and later change who can access their data, set and revise retention periods, dictate how much detail is shared, decide when to review it (whether on a schedule or as needed) and easily confirm 'no changes' or update the record whenever they wish.

6 Implementation

6.1 Cross-functional ownership and accountability

Implementing vulnerable customer management involves multiple disciplines across different departments. These include:

- **Operations**: operations manage those staff members who engage with customers and are involved in the identification and mitigation of customer vulnerabilities.
- **New business**: new business manages the sales and onboarding processes where an initial customer vulnerability assessment should usually take place.
- **Compliance**: compliance oversees the vulnerable customer policy along with implementing Consumer Duty.
- **Information Technology**: IT manages customer-focused data in software systems.
- **Marketing**: marketing manages or influences communications and engagements with customers.
- **Learning and Development**: L&D manages staff training and integrates training into onboarding processes.
- **Human Resources**: HR will need to be aware of, and put in place, support for staff who may have to deal with sensitive customer circumstances, for example, divorce, suicide, bereavement etc.
- **Senior management**: senior management needs to access and respond to reporting metrics and management information as part of Consumer Duty reporting and the FCA's Senior Managers and Certificate Regime (SM&CR).

It is important to engage with all these stakeholders as part of implementing Consumer Duty, incorporating their needs into planning and management processes.

GOOD PRACTICE

Firms should establish clear accountability for vulnerability management. A RACI (Responsible, Accountable, Consulted, Informed) framework may be helpful.

- Who is **Responsible** for executing specific vulnerability management tasks, for example, conducting assessments, updating systems and providing support.
- Who is **Accountable** for overall outcomes and has decision-making authority; typically a named Senior Manager under SM&CR.
- Who must be **Consulted** before decisions or changes are made, for example, Compliance, Data Protection Officer etc.
- Who should be **Informed** of progress, issues and outcomes, for example, Board, relevant committees etc.

This framework ensures all stakeholders understand their role; prevents accountability gaps; facilitates cross-departmental collaboration; and provides clear escalation pathways when issues arise.

Leveraging customer journeys as the common thread that unites stakeholders ensures that everyone works toward the shared goal of achieving good outcomes for all customers.

6 Implementation

6.2 Phasing approaches

Firms can choose between a phased roll-out of customer vulnerability management (for example, staggered department or team rollout) or a 'big bang' implementation with all departments, staff and services operating concurrently. For all but the smallest firms, a phased approach is recommended, allowing customer journeys to be tested and refined before full deployment across all areas. There are several dimensions to consider when phasing implementation:

The stages of customer vulnerability management:

- Identification
- Classification
- Monitoring
- Mitigation or support
- Reporting

IT integration:

- Manual processes (the recommended starting point)
- Integrated IT systems (following validation)

Distribution channels:

- Direct
- Indirect

The coverage across processes and departments:

- Sales, point of sale
- Operations and service delivery
- Claims
- Complaints

Organisational scope:

- Pilot offices or teams
- Business units or subsidiaries
- Geographic regions
- Full enterprise rollout

The coverage of products:

- New business processes
  - Priority products with highest vulnerability risk
  - Lower-risk products
- Existing customer base
  - Recent customers
  - Legacy portfolios

GOOD PRACTICE

There is no universal blueprint. Each firm should tailor their phasing strategy based on their organisational structure, customer base, risk profile, and resources. Here are some recommendations:

- **Start small and manual**: before investing in systems development or integration, begin with a limited subset of customers, using manual processes to test and refine approaches.
- **Direct channels first**: where firms operate both across direct and intermediated distribution channels, prioritising in-house channels allows for better control over process development and the building of staff expertise.
- **High-impact areas**: focus initially on customer touchpoints and products where customer vulnerability identification and support will have the greatest positive impact.
- **Build expertise before scaling**: develop internal competency and proven processes before expanding to external partners or automated systems.
- **Iterative refinement**: use each phase to validate approaches, gather feedback and make necessary adjustments before a broader rollout.

6 Implementation

6.3 Selecting systems

Principles-based regulation allows firms to implement vulnerability management in ways suitable and proportionate to their business. This guide does not prescribe specific solutions but highlights the considerations required when selecting systems.

6.3.1 Moving beyond manual-only approaches

Many firms have begun training front-line staff to identify vulnerability through manual assessment and data entry. While this has demonstrated progress in identifying vulnerable customers and preventing harm, manual-only approaches have limitations, including:

- **Reactive coverage**: this only reaches the small proportion of customers who contact the firm and self-disclose.
- **Inconsistent data**: subjective assessments may vary between staff members.
- **Unstructured records**: free-text notes in Customer Relationship Management (CRM) systems are:
  - Difficult to aggregate for outcome reporting.
  - Insufficient for longitudinal monitoring.
  - May not meet UK GDPR data accuracy requirements.
- **Limited evidence**: difficult to demonstrate identification, monitoring and support provision over time.
- **Outcome comparison**: different data formats prevent systematic comparison of vulnerable versus non-vulnerable customer outcomes.

Storing vulnerability data in spreadsheets or unstructured CRM text fields creates operational inefficiencies and may not meet UK GDPR requirements for any firm with more than a handful of customers.

6.3.2 System options

Larger firms may choose to build custom solutions integrated with their existing infrastructure.

Smaller firms are more likely to adopt the following approaches:

- **Purpose-built digital vulnerability management systems**: standalone platforms designed specifically for vulnerability data capture, monitoring and reporting.
- **Enhanced CRM systems**: either native functionality or integration with specialist vulnerability platforms.
- **Voice analytics**: useful for identifying vulnerability during direct customer interactions (for example, calls and chats) but these should be supplemented with systems covering customers not regularly contacted.

6.3.3 System requirements

Given the long-term nature of vulnerability data management and Consumer Duty monitoring obligations, most firms will require IT systems capable of the following:

- Structured data capture using consistent taxonomies.
- Secure storage meeting UK GDPR requirements.
- Longitudinal tracking of customer circumstances.
- Aggregated reporting by vulnerability cohort.
- Integration with existing customer management systems.

Firms should evaluate options based on their specific needs, customer base size and existing technology infrastructure. See system selection checklist in Appendix 3.

7 References

Edmonds, James, *Are 50% of your customers really vulnerable?* (MorganAsh, 2025)

Financial Conduct Authority, *Delivering good outcomes for customers in vulnerable circumstances – good practice and areas for improvement* (FCA, 2025)

Financial Conduct Authority, FG21/1, *Guidance for firms on the fair treatment of vulnerable customers* (2021)

Financial Conduct Authority, FG22/5, *Final non-Handbook Guidance for firms on the Consumer Duty* (FCA, 2022)

Financial Conduct Authority, PS229, *A new Consumer Duty: Feedback to CP21/36 and final rules* (FCA, 2022)

Financial Conduct Authority, *Financial Lives survey* (FCA, multiple years)

Fitch, Chris et al., *A once in 25 years opportunity – ten principles for designing vulnerable consumer data sharing programmes* (Money Advice Trust and What We Need, 2024)

Fitch, Chris, Dan Holloway and Conor D'Arcy, *Making it easier for consumers to disclose a mental health problem* (Money and Mental Health Policy Institute and Money Advice Trust, 2022)

Fitch, Chris et al., *What support can firms give disabled consumers and people in vulnerable situations* (Money Advice Trust and What We Need, 2025)

Fitch, Chris et al., *Vulnerability, GDPR, and disclosure, a practical guide for creditors and advisers* (Money Advice Liaison Group and Money Advice Trust, 2020)

Gething, Andrew, *Data-sharing isn't just good for customers – it's what they expect* (MorganAsh, 2025)

Gething, Andrew, *How to identify vulnerable customers* (MorganAsh, 2002)

Gething, Andrew, *Mind the gap: FCA highlights why firms ae falling short on Consumer Duty* (2025)

Gething, Andrew, *Top 10 myths of implementing customer vulnerability management* (MorganAsh, 2025)

Gething, Andrew, *Top 10 pitfalls made by firms when implementing customer vulnerability* (Morgan Ash, 2025)

Gething, Andrew, *Understanding the vulnerability gap* (MorganAsh, 2025)

Gething, Andrew, *Why sharing individual customer date is the practical solution to meeting Consumer Duty* (MorganAsh, 2022)

Harvey, Adrian, *Customer vulnerability: your questions answered* (MorganAsh, Elephants Don't Forget and FWD Consulting, 2024)

Money and Mental Health Policy Institute, *A best practice guide for insurers: supporting customers with mental health problems* (Money and Mental Health Policy Institute, 2023)

Money Advice Trust, *Inclusive design in essential services: a guide for regulators* (Money Advice Trust and Fair by Design, 2021)

Surviving Economic Abuse, *Checklist for insurers* (Surviving Economic Abuse and Cooley, 2023)

Surviving economic abuse, *Good practice guide for financial services* (2025)

Turner, Phil, *Bereavement processes in insurance and financial services – not "dead good"* (The Journal, Chartered Insurance Institute, 2025)

8 Appendices

Appendix 1: Customer vulnerability management checklist

Every firm is on a unique journey with its customer vulnerability management strategy, which translates into different levels of operational maturity. This checklist should quickly pinpoint areas for enhancement and support the assessment of current capabilities against good practice.

Strategy, governance and culture

- ❑ **Target market analysis**: clearly defined and quantified characteristics and scale of vulnerabilities – and their impact or consequences (for example, the potential harms) that the customer base and target market face.
- ❑ **Policy**: a policy which defines the data needed, where it is stored, how it is kept both accurate and consistent, and when it is to be deleted (all in accordance with UK GDPR).
- ❑ **Product design**: product design, approval and review processes consider the needs of vulnerable customers in order to prevent foreseeable harms and ensure fair value.
- ❑ **Systems and processes**: systems and processes manage the data required for customer vulnerability management.
- ❑ **Staff training**: training ensures that all relevant staff (from front-line teams to product teams and senior leadership) are trained, empowered, competent and confident to understand the needs of, and support of, customers in vulnerable circumstances.
- ❑ **Culture**: led by senior management and the board, firms can evidence an organisation-wide culture which prioritises delivering good outcomes for vulnerable customers.

Identification and recording

- ❑ **Proactive identification**: proactive processes identify customer vulnerabilities across the entire customer journey, rather than rely solely on customer disclosure at any single point (for example, claims or complaints stages).
- ❑ **Holistic assessment**: assessments cover the full range of vulnerability drivers (e.g. health, life events, low resilience, low capability etc.) and their potential to intersect with other vulnerabilities (not just financial vulnerabilities).
- ❑ **Consistent recording**: a taxonomy to consistently record all vulnerability related data and its potential impact.
- ❑ **Protected characteristics**: systems that allow firms to monitor outcomes for customers with protected characteristics, in line with the Equality Act 2010.

Action and support

- ❑ **Tailored support**: firms can demonstrate how they use customer vulnerability data to provide tailored support and inform product design.
- ❑ **Consumer understanding**: firms should test and adapt customer journeys to ensure that those customers with diverse needs can easily navigate them.
- ❑ **Accessible journeys**: firms have review and remove unnecessary friction ('sludge') in customer processes that create barriers or harm for vulnerable customers.

Monitoring, reporting and assurance

- ❑ **Quality data and evidence**: a data architecture that delivers consistent data and allows firms to evidence the steps taken, and the outcomes achieved, to accommodate each customer over the lifetime of products and services.
- ❑ **Outcomes monitoring**: firms can report on the outcomes experienced by vulnerable customers compared to non-vulnerable ones in Consumer Duty Board reports – and can compare outcomes between different cohorts of vulnerable customers (for example, those experiencing a specific negative life event, who have a type of low resilience) and between a specific cohort of vulnerable customers and non-vulnerable ones.
- ❑ **Assurance and testing**: a regular assurance programme (for example, call monitoring, case file reviews or mystery shopping) can test whether vulnerability policies are followed in practice.
- ❑ **Distribution chain oversight**: monitoring and governance extends across the entire distribution chain to evidence good outcomes across it (this requires data sharing).

8 Appendices

Appendix 2: Customer vulnerability data framework checklist

Use the following checklist to assess or build a vulnerability data framework.

Foundations

- ❑ **Data quality**: is there a process to maintain the accuracy of core customer contact information over time?
- ❑ **Classification**: is there a firm-wide, objective taxonomy for classifying customer vulnerability characteristics and severity?

Data model and systems

- ❑ **System capability**: can the IT systems store, link and analyse key data components (for example, circumstances, severities, potential harms, support pathway and outcomes)?
- ❑ **Household view**: can systems link individuals to form a family or household unit or view?
- ❑ **Combination of circumstances**: do our systems show when multiple circumstances of vulnerability are compounding, to make customers' situations worse?

Governance and policy

- ❑ **Data policy**: is there a clear policy on storing underlying circumstances, severities, and support needs, as well as when support needs were implemented?
- ❑ **UK GDPR compliance**: is the lawful basis for processing customer vulnerability data documented? Are security and governance measures robust and compliant with UK GDPR?

8 Appendices

Appendix 3: System selection checklist

When considering what technology to adopt, the following checklist should help assess whether systems meet the requirements for effective customer vulnerability management.

Identification and classification

- ❑ Are there proactive and reactive methods to assess and identify the customer's vulnerability characteristics?
- ❑ Is there a classification system or taxonomy that records vulnerabilities in an objective way (not just a binary yes/no) so that data is consistent and excludes the recording of subjective opinions.
- ❑ Are the correct data elements (as per Section 5.2.4 Data structures) in place, including circumstances, severity, coping mechanisms, support needs, the support implemented and the resulting outcomes?
- ❑ Can the system document the impact of multiple and overlapping vulnerability circumstances?
- ❑ Is the system designed to capture and manage customer vulnerability across groups (mostly family groups)?

Data protection requirements

- ❑ Can it store data securely with appropriate encryption and access controls?
- ❑ Can it record the rationale for processing the data (for example, consent, legitimate interests)?
- ❑ Can it modify, update and delete individuals' data in line with data subject rights?
- ❑ Can it provide information to the customer (from subject access requests) in accessible formats?
- ❑ Does it have mechanisms to keep data both accurate and up to date?
- ❑ Does it cater for only the appropriate personnel to access data, limiting access to those who need it?
- ❑ Does it support role-based access in a tiered way (e.g. front-line staff see basic flags; specialists see full details etc.)?

Lifecycle management

- ❑ Can it record data and changes in data over the lifetime of products and services, for example, whether circumstances have improved, worsened or remained the same?
- ❑ Does it support automated alerts when vulnerability circumstances change or require review?
- ❑ Can it prompt for scheduled reviews based on risk and product type?
- ❑ Can it integrate with customer communication systems to prevent inappropriate contact?
- ❑ Does it suggest next steps or support needs based on identified vulnerabilities?
- ❑ Can it record whether the customer adopted the recommended support or not?

Reporting

- ❑ Can it aggregate data by vulnerability cohort for outcome monitoring?
- ❑ Can it track trends over time (for example, identification rates, outcome gaps and intervention effectiveness)?

Audit trail

- ❑ Does it capture a complete history of all changes (i.e. who, what, when, why)?
- ❑ Can it demonstrate regulatory compliance through evidence trails?

8 Appendices

Appendix 4: Pros and cons of different approaches to customer vulnerability management

The following table highlights the main pros and cons of approaches to customer vulnerability management currently tried in the UK market.

Approach	Pros	Cons
Advisers and brokers handle directly as they always have done, and record notes in a CRM.	• Uses direct customer contact. • Uses experience of adviser/broker. • Little change for advisers or customers.	• May be uncomfortable asking personal questions. • When data is recorded as text within CRM it is difficult to report on. • Depends on conscientiousness of the adviser/broker. • Lack of scalability. • Over-reliance on an individual's memory and understanding of vulnerability. • Opinions and judgements may breach UK GDPR. • Minimal evidence for audit trail and reporting. • Experience is that the implementation of this is variable, with many vulnerabilities missed. • Typically, a significant under-recording of customer vulnerabilities. • Cognitive burden on front line staff.
As above, but with customer vulnerability questionnaires added to CRM.	• Adds thoroughness. • Enables customers to complete assessments in privacy.	• Vulnerability considered as binary. • Subjective, opinionated data. • Little understanding of severity. • No help on support needs. • Opinions and judgements may breach UK GDPR. • Difficult to separate data from embedded systems. • Completion rates may be low unless customers experience a value exchange. • Cognitive burden on front line staff.
Training front-live staff (typically for manufacturing and larger organisations).	• Easy to implement. • Solves vulnerability issues directly with customers.	• Reactive given it only covers those customers who are spoken with, or approach, the firm. • Delivers less consistent data for evidence and reporting. • Opinions and judgements may breach UK GDPR. • Cost of training is high and ongoing. • Training staff on all vulnerabilities and related support needs options is near impossible. • Very difficult to scale. • Almost impossible to capture data for reporting on outcomes.

8 Appendices

Appendix 4: Pros and cons of different approaches to customer vulnerability management (continued)

Approach	Pros	Cons
Voice analytics in call centre (typically product providers and larger organisations).	• Good for quality assurance in call centres to help train staff to identify vulnerabilities.	• Reactive given it only covers customers who approach the firm. • Detection based on voice pattern, but some vulnerabilities (e.g. blindness) are 'the norm' for the customer and do not affect vocal patterns. • May detect distress but lack contextual severity and customer preferences for mitigation. • Cost of training is high. • Training staff on all vulnerabilities and related support needs options is almost impossible. • No taxonomy of vulnerabilities for communicating outside of the system.
Digital vulnerability management systems.	• Thorough assessment of all customers. • Consistent digital data. • Accurate digital records with instant reporting. • Accommodates family groups, not just individuals. • Typically identifies around 50% of customers. • Records stored over time for monitoring and evidence. • Instant support recommendations, saving training overheads. • Meets and can exceed Consumer Duty regulations.	• Licence cost (although this far outweighs the costs of manual approaches). • Integration complexity in linked to existing systems to avoid double handling of data. • Vendor dependency.

8 Appendices

Appendix 5: Overcoming barriers – myth busting common fears

Here are a few of the common fears, which firms may experience or come across, when rolling out vulnerable customer management.

"We can't hold sensitive data because of UK GDPR."

This is incorrect. Firms can hold sensitive data, they simply need to comply with UK GDPR. This means they need to implement appropriate processes and systems, record the method of processing, store information accurately and securely, provide any information held to the customer upon request, and delete individual consumer's information when requested. If firms don't have, or procure, systems which enable them to do this, it is then they are likely to breach UK GDPR. The CII is working on a separate guidance on this specific topic.

"Treating vulnerable customers will add cost."

This fear typically comes from firms which have delayed starting the vulnerable customer journey. This is typically unjustified. There are several factors at play here:

- While 50% of customers may be identified as vulnerable, typically over half of identified vulnerabilities will be mild and will not require any action. However, they do need recording in case they are relevant in other circumstances or if they change over time.
- Most support needs (or 'next actions') have minimal costs.
- Those customers with severe vulnerabilities or disabilities typically already have mitigation strategies in place; that is how they manage their daily lives. Firms just need to know what these are, so they can work with them as opposed to against them.
- Understanding and adapting processes up front is typically cheaper than amending a process later down the line.
- Managing customer vulnerabilities up front should reduce claims and compensation fees.
- Some firms have implemented a purely manual approach, relying on front-line staff to identify vulnerable customers face-to-face and over the phone, without proper systems and support. This proves to be expensive. Others have yet to quantify the benefits of vulnerable customer management. Many of these benefits are in the future and difficult to measure, e.g. increased loyalty, repeat business or reduced claims. Some firms have already experienced increased revenues and made significant product alterations to take advantage of this personalised data.

"We only need to train front-line staff."

Training front-line staff is an important part of managing customer vulnerability but it is just one component. Investing in training (an ongoing requirement) without putting in place systems to support staff is expensive. Many larger firms have discovered that trying to train all staff to identify, signpost or treat all types of vulnerability, without systems support, is almost impossible. Firms should consider what systems can support their teams, in order to make their roles manageable as well as more efficient.

"The FCA has not said we must do this."

This is true. The FCA's Consumer Duty regulations are principle-based. They don't prescribe exactly how Consumer Duty and vulnerable customer management are to be implemented. While this approach is alien to many, it gives firms great and welcome latitude to implement processes which properly fit their business. The approach within this document is designed to meet Consumer Duty and vulnerable customer guidance principles.

"We don't need to assess everyone or be proactive."

Many firms only start identifying customer vulnerabilities when they are contacted, when customers volunteer issues, or at the claims or complaints stage. While there is nothing wrong with these methods, they are reactive and therefore limited; and firms usually discover that they can only identify a small single-percentage-figure of vulnerable customers. The FCA has upgraded its guidance to require firms to "actively encourage customers to share information." Firms should be proactive and engage with their customers.

"Asking additional personal questions will reduce sales."

There has been a general drive to reduce friction in the onboarding journey, whether manual or digital, to reduce time. This has led some people feeling that gathering customers' vulnerability data will reduce sales – simply because it requires some additional steps. Evidence from firms suggests the opposite – having the extra information has led to improved engagement and even increased new business. It is useful to consider this as increasing personalisation and customer engagement, rather than just increasing friction. Indeed, the term friction isn't helpful in this context;

8 Appendices

Appendix 5: Overcoming barriers – myth busting common fears (continued)

done well, this doesn't rub the customer up the wrong way, it shows interest in their circumstances and a willingness to accommodate them.

"I already know my customers; I have known them for twenty years."

Many advisers do know a lot about their customers but that doesn't mean that there aren't still some issues that have not been uncovered (i.e. simply because they have not been asked about). For example, around 10%-20% of people are dyslexic, so at least ten customers out of a hundred have this characteristic of vulnerability. Vulnerabilities are not always apparent. Even where advisers believe they know all there is to know about their customers, this information is typically in their head and not recorded for communicating with others. Consumer Duty requires evidence and evidence requires consistent, structured, recorded data.

"Our customers won't like it. They won't answer personal questions."

This is one of many firms' biggest fears but is unjustified. When firms engage directly and empathetically, following regular engagement practices, customers are highly likely to participate. Of course, there is the need to explain to customers why they are being asked for this information and, importantly, why providing it will benefit them. Experience shows that it is best not to position this as "to meet regulations." Rather, firms should communicate that "the more they understand you, the better they can support you." Experience shows that most customers will disclose personal information. For example, research from MorganAsh's real assessment data shows that up to 95% of people will complete assessments if this is managed well. Paradoxically, financial services firms typically ask for lots of information on customer finances which, to many customers, is as personal or even more personal than their health issues. People will often more readily talk about their circumstances than their finances.

"People won't like being labelled as vulnerable."

The FCA's regulation wording has steered firms to categorise customers as 'vulnerable' or 'not' regardless of whether this terminology is helpful. We do not advocate that firms label people as vulnerable, nor use the term in discussions with them but rather to 'seek to understand customer circumstances and the severity or impact of the circumstances and how these affect the customer.' The purpose is to achieve the best outcome for the customer, and this kind of phraseology helps to position it in this way.

"People with addictions won't admit to it."

This is not true. Experience, to date, shows that a meaningful proportion of people with addictions (as with other characteristics) do provide the information, although it is of course unknown what proportion disclose. From a regulatory point of view, should an issue arise later, firms can evidence that they asked the consumer, thereby shielding themselves from vexatious claims.

9 Authors

Authors

- **Andrew Gething**, Managing Director, MorganAsh
- **Martin Grimwood**, Director, FWD Research
- **Vanessa Riboloni**, Head of Research and Insight, Chartered Insurance Institute

With special thanks to those who provided expert views and critical feedback to this publication:

- **Chris Adlard**, Director of Customer Experience and Compliance, Elephants Don't Forget
- **Christopher Brooks**, Head of Consulting, Lexden CX
- **Carla Brown**, CEO, Oakmere Wealth. President, Personal Finance Society Board
- **Vivine Cameron**, EDI Manager, CII
- **Matthew Connell**, Director of Policy and Public Affairs, CII
- **Tony Crane**, Founder, Crane Consulting
- **James Edmonds**, Managing Director, Duty CX. Managing Partner, Protect Association.
- **Faith Galiwango**, Business Transformation Lead, Direct Line Group
- **Eddie Grant**, Cabinet Office Disability and Access Ambassador. NED Personal Finance Society (PFS) and European Financial Planning Association (EFPA). Chair of the Finance in Society Research Institute (FISRI)
- **Adam Harper**, Executive Director, Strategy, Advocacy, Professional Standards, CII
- **Mandy Hunt**, Managing Director, Clear Group
- **Gem JianwaroPassant**, Customer Experience Consultant, Azoth Consulting Ltd
- **Lauren Long**, Ombudsman Leader – Cross-cutting Policy, Financial Ombudsman Service
- **Claire Massey**, Founder and CEO, Claim Guardians
- **Hannah Murphy**, Product Owner, Vulnerable Customer Strategy, Royal London
- **Ian Roberts**, Control and Contracts Manager, AXA UK
- **Chris Shadforth**, Communications and Engagement Director, CII
- **Ian Simons**, Content and Capabilities Director, CII
- **Johny Timpson OBE**, Chair of Absolute Military, MorganAsh and Building Resilient Households Group. Financial Inclusion Commissioner
- **Phil Turner,** Business Development Executive, CII
- **Leoni Trim**, Vulnerable Customer Operations Manager, Admiral
- **Kimberley Warwick**, Lead Manager, Vulnerable Customer, Admiral
- **Dr Alan Whittle**, Director, Unburdened Solutions
- **Emma Wride**, Senior Proposition Analyst, Vulnerable Customers, Royal London

The Chartered Insurance Institute
3rd Floor, 20 Fenchurch Street,
London EC3M 3BY

tel: +44 (0)20 8989 8464

customer.serv@cii.co.uk
cii.co.uk

Chartered Insurance Institute

@CIIGroup

COH_J4018 (11/25)