

Customer Vulnerability Review
Summary Report
March 2023

Contents

1. Introduction and background.....	3
2. Executive Summary	3
2.1. Key Findings.....	4
3. Detailed report	6
3.1 Governance, controls, and oversight	6
3.2 Identification of vulnerable customers	11
3.3 Support for vulnerable customers	13
4. Conclusion and Next Steps.....	19
Appendix 1	21

1. Introduction and background

Against a backdrop of the continuing effects of the pandemic, rising inflation, the impact of cost-of-living increases and more widely, global economic and political volatility, we anticipate a further evolution and increasing scale of customer vulnerabilities.

A key deliverable for the Lending Standards Board (LSB) in 2022/23 was to undertake a significant project across the Standards of Lending Practice for personal and business customers (the Standards) and the Contingent Reimbursement Model Code for Authorised Push Payment Scams (CRM Code), focused on the identification and treatment of vulnerable customers and how the level and nature of vulnerability has evolved over recent times. We also considered the impacts of recent developments which have raised new challenges for registered firms in delivering fair customer outcomes, particularly to those customers who are, or may be, in a vulnerable situation.

The detailed scope, objectives, methodology and approach can be found in Appendix 1 to this report.

2. Executive Summary

The LSB Compliance team recently completed a thematic review which assessed whether vulnerable customers are receiving fair outcomes, in line with the personal and business Standards, across a sample of registered firms. We also drew upon insights obtained from our 2022 review of adherence to the CRM Code, where these relate to vulnerability.

It should be noted that the CRM Code does not contain as detailed information with regards to vulnerability as that which is defined within the Standards, as the Code is more nuanced towards the customer being vulnerable to the scam which occurred. However, it is good practice to also consider the other points raised within this report from a wider vulnerability perspective for customers who are victims of scams. Due to the nature of these insidious crimes, there is a high possibility that customers may be more vulnerable afterwards, not just financially but also from an emotional perspective. Firms should consider utilising vulnerability support teams, where these exist, or having the ability for customers to be supported more widely than just dealing with the scam reimbursement. Therefore, where practical, all points raised within this report should be applied in relation to all customers whether they are protected by the Standards of Lending Practice or the CRM Code.

In general terms, the majority of firms have considered vulnerable customers within their overall strategies for achieving good customer outcomes, with these being designed to comply with the requirements of the Standards and the Code. However, we did find that there were varying levels

of progress and achievement in delivering and operationalising these strategies to ensure full adherence to both sets of Standards and the CRM Code.

The frameworks that have been implemented should allow firms to oversee the impact of identifying and supporting vulnerable customers, as well as being underpinned by training and support for staff.

We were encouraged that firms are placing a clear focus on support for, and treatment of vulnerable customers, with engagement from Executive level and throughout organisations to ensure this cohort of customers are identified and treated appropriately to ensure good customer outcomes.

However, we believe that more work is required to be fully compliant, to ensure intentions are translated into actions, and for firms to consistently achieve good customer outcomes.

Our findings from this review are summarised below.

2.1. Key Findings

A number of themes emerged from our reviews across the Standards of Lending Practice for personal customers, business customers and in relation to the CRM Code.

Overall, it is clear firms are committed to meeting the relevant requirements of the Standards and the CRM Code. Given the current macro-economic environment, firms need to ensure the governance, strategies and processes they have in place are able to work effectively for known vulnerable customers as well as those yet to be identified as needing more support.

The key areas highlighted below are expanded upon within the remainder of the report together with specific comment on areas to improve, and also highlighting areas of good practice.

Governance, controls and oversight

- **Management Information (MI)** – more pertinent information needs to be produced to allow vulnerability strategies to be evaluated. In some cases, MI did not provide a holistic view of the effectiveness of vulnerable customer identification, the number of cases, the level of support offered and achievement of good customer outcomes.
- **Quality Assurance (QA)** - was often narrowly focussed on the processes for identification of vulnerability with little consideration of the softer skills needed to engender effective probing and questioning. This could result in opportunities to raise weaknesses in the identification, probing and supporting of vulnerability being missed.

- **Training** - the inconsistencies in identifying and investigating potential vulnerability triggers and examples of declared vulnerability being missed indicates that more needs to be done to embed training. Training should be focussed to the area or function within which staff are operating.
- **Record-keeping** – often vulnerability information was either inaccurately captured or not recorded. Where it was captured, it was not always easily visible where there were considerable notes across multiple systems.

Identification

- **Digital channels** - firms' arrangements for identifying vulnerability were limited within digital channels.
- **Embedding training** - overall the quality of conversations across all channels was inconsistent, with instances of rigid scripting and potential vulnerability triggers being missed or not probed and/or not recorded.

Support

- **Solutions** - we did not always see solutions being set up to support vulnerable customers. There was conflation between financial difficulties and wider vulnerability, resulting in the focus on addressing financial difficulty rather than supporting from a vulnerability perspective. Some solutions, such as breathing space or holds on account, were instigated without explanation or opportunity for review with customers to ensure this was helpful.
- **Ongoing reviews** - once vulnerability was identified, we did not always see regular proactive reviews to understand if the customer's circumstances had changed and if the support provided required adjustment.
- **Communications** – verbal and written communications need to be clearer in explaining the implications of missing payments and more positive to encourage engagement. Signposting was often generic to debt advice bodies and would benefit from being more tailored to support for customers with vulnerabilities.
- **Debt outsourcing and sale** - while customers categorised as having an ongoing mental or critical illness were excluded from outsourcing and debt sale, we did see that other vulnerabilities, which could have associated mental health impacts due to trauma, were included.

Whilst the key findings above are focussed on areas for improvement we also identified a number of good practices across firms.

These included:

Governance and controls:

- Setting strategy – firms would often engage external expertise to ensure strategies were appropriate and considered all types of vulnerability.
- Product design - strategies were clearly reflected in the product design and review frameworks which considered the impact on vulnerable customers.

Identification:

- Well embedded training helped staff in conversing with customers to be able to ascertain the nature of vulnerability and agree the most appropriate support for that customer.
- Customer driven initiatives which allow proactive request for support, whether due to a vulnerability or not, helps with targeting of support. A secondary benefit was the ability to review and refresh the support available as situations evolve.

Support:

- Promoting the benefits of more targeted third-party support was helpful for customers with specific vulnerabilities, such as gambling or being a victim of domestic abuse.
- Internal systems designed to support staff with guidance or understanding of how to assist a vulnerable customer ensures the most appropriate solution is provided.
- Flexibility in how customers are contacted by considering the impact of the specific vulnerability helps to continue engagement.

3. Detailed report

3.1 Governance, controls, and oversight

We considered whether firms had appropriate governance, controls and oversight structures in place to ensure the requirements of the Standards and Code were being met, whilst providing assurance of how this is being achieved.

Governance

Strategies are in place and visible to executives and senior management. It was pleasing to note that there are structures in place to ensure there is both upward and downward flow of information related to vulnerable customers. All firms understood the importance of having a clear approach to identification of, and support for, vulnerable customers.

Whilst we found that firms had vulnerability strategies designed to meet the requirements of the Standards, these were at various stages of maturity, with some requiring more development than others to ensure the effective identification and treatment of vulnerability.

Management Information and data was often lacking in detail to allow those with accountability to understand the qualitative nature of how the strategies are being achieved. Where MI was more mature, it included the more detailed metrics supported by QA outputs, vulnerable customer related complaints root cause analysis, vulnerable customer feedback and breach reporting. The overall impact was a holistic view of the effectiveness of the performance of the vulnerability strategy.

Overall, most firms had clear strategies in place, but these did not always translate into operational effectiveness. Further detail on the issues in this space are contained below.

Good Practice:

- Strategies are designed to encompass all products, channels and activities whilst considering the differing types, duration and severity of vulnerabilities.
- To understand the nature of vulnerability within the customer base and inform the strategy, some firms used external sources such as market researchers and expertise from technical working groups or trade bodies. In addition, we found examples of firms utilising the insights of charities and third-party organisations to inform them about the impacts and needs of different types of vulnerability.

Areas for Improvement:

- MI requires development to ensure that senior management have clear visibility of the effectiveness of vulnerability strategies in adhering to the Standards and the CRM Code and how these are providing good customer outcomes.
- Where strategy improvements are needed, this had been identified by the impacted firms and action plans developed. However, some of these plans were at a very early stage and there is a need for defined actions to be progressed to ensure there is the ability for vulnerability to be identified and supported at the earliest opportunity.

Controls

From a controls perspective, we considered various areas that would enable firms to ensure high level strategies are reflected in policies and operational procedures and processes. The majority of firms reviewed had a defined customer vulnerability policy in place which reflected elements of the overarching strategy. This was then reflected further in detailed processes such as product design and review, standard operating procedures and training programmes.

Training

Firms had a range of training in place to support staff in identifying triggers of potential vulnerability which was mainly aimed at those who would be interacting with customers. In some instances, the training was extended to cover other functions where there may not have been direct customer contact but given the important nature of the subject, all staff would complete some element of training on this topic.

Training typically consisted of a combination of face to face and computer-based sessions, with focus being both at induction and on a refresher basis, usually undertaken at least annually. Staff would also be expected to undertake further training where weaknesses had been identified during assurance reviews.

From the information we reviewed, the design and content of training appeared to cover the expected key areas, however, as is noted later within this report, our review found examples of interactions with customers which demonstrated that this training had not been embedded amongst all customer facing employees.

Our view is that this points to a need for further embedding of training as well as a clear focus within quality assurance processes to identify where weaknesses are appearing, to ensure further coaching or remedial training can be undertaken.

Areas for Improvement:

- Firms should ensure that training is sufficiently embedded to support staff in their ability to identify and respond to potential triggers of vulnerability and specific disclosures in a consistent manner. Role-specific training, using practical examples aligned to the different types of situations staff may come across day to day, can assist with embedding knowledge provided during training sessions.

Policies and procedural controls

Moving on to the more detailed elements of policy and procedures, all firms reviewed were able to evidence a number of documents which included details on how vulnerability was considered, driven by the overarching strategies and supported by detailed procedural documents.

The policies and procedures in place were designed to cover all aspects of the customer journey. From a Standards perspective this included product design, followed by sales process, servicing and monitoring of accounts through to financial difficulties support. Whereas in relation to CRM Code, the relevant policies and procedures were focussed towards identifying customers vulnerable to scams and how this is considered at the key points within the payment journey.

By covering the whole customer journey, this provides firms with a greater opportunity to identify and support their vulnerable customers to ensure good outcomes are achieved. However, similar to the point raised above in relation to training, we found that the required outcome of these policies and processes were not always reflected in front line employees' interactions with customers. Further comment is contained within the Identification and Support sections of this report.

From a digital perspective we found that firms faced challenges in the ability to identify vulnerable customers during the customer journey. Digital journeys are designed to facilitate a speedy and efficient way for customers to apply for credit or make payments. Therefore, there is a need to consider how appropriate friction can be added which allows customers with any vulnerability to be identified and supported, without adding complexity or unnecessary barriers for those without additional needs.

Good Practice:

- Typically, firms had product design and review frameworks in place which considered an assessment of vulnerable customer impacts. This provided firms with the opportunity to ensure that when launching and/or reviewing existing products, there is a defined process to include in-depth assessments of the potential impacts on vulnerable customers.

Record-keeping

Across all channels, where vulnerability was identified and recorded, we found that customer records did not always capture the vulnerability impacts, support needs and solutions considered. This was mainly due to the inconsistency of approach by staff within the firms reviewed. From the cases assessed during our review, we often identified that records were either inaccurate, did not reflect conversations held or support being provided or indeed, on occasion, there appeared to be no records maintained at all, albeit a 'vulnerability flag' may have been recorded.

Some firms have centralised systems for recording vulnerability and others require notes to be recorded across multiple systems. This can hinder the firm's ability to maintain accurate records and also means that customers often have to repeat their situation each time they engage with the firm.

Areas for improvement:

- Firms should ensure that vulnerability information is appropriately recorded on internal systems regardless of channel, at the point of identification or disclosure, in line with a 'tell us once' approach. This will ensure vulnerable customers are supported throughout the lifecycle of their account.

- Firms should ensure that vulnerability is consistently recorded, with all necessary consents, so that vulnerable customers can be easily identified and supported throughout the customer journey, regardless of the way in which the relationship is managed.

Third Parties

Where applicable, third-party supplier management policies were in place. These included appropriate initial and ongoing due diligence which considered the effectiveness of the third parties' vulnerability related policies and processes and the wider potential for customer harm. We observed regular business reviews with third parties and additional due diligence conducted where the third parties' activities could have a greater risk for vulnerable customers.

Oversight

The majority of firms had a defined three lines of defence framework in place which captured vulnerability within the related activities. In respect of first line quality assurance (QA), this typically included process driven 'point-in-time' and end-to-end customer outcome tests, however the outcome tests occurred less frequently.

The manner in which QA was undertaken was often narrow in focus with attention being placed purely on procedural competence, rather than any element of soft skills being included. This type of focus has the potential risk of not identifying when staff miss triggers of vulnerability, show empathy or evidence questioning and probing skills to ensure they have a full understanding of a customer's situation and whether they need any additional support.

Depending on the size and structure of the firm, second and third line assurance activity included various methods to garner assurance including, for example, 'check the checker' assessments, thematic reviews with a focus on vulnerability or end-to-end customer journey reviews. Whilst the outputs of these various reviews would be escalated through internal governance, as mentioned previously, this was not always at a detailed level to provide assurance of strategies being followed or ensuring visibility of how vulnerable customers are being supported.

Areas for Improvement:

- Firms need to ensure that QA processes are effective in their assessment of the identification and treatment of vulnerability in a consistent manner, across the Standards and the CRM Code.
- Firms should ensure there is sufficient focus within assurance frameworks of both procedural and soft skills such as empathy and questioning/probing to ensure that customer facing employees have the necessary skills to identify vulnerable customers and ensure that such customers are supported appropriately.

- The outputs of assurance programmes should be included within reporting to senior management and Executive level as confirmation of the effectiveness of vulnerable customer strategies and the achievement of good customer outcomes.

3.2 Identification of vulnerable customers

Across the full customer journey, firms have taken steps to implement methods which allow staff to proactively identify vulnerability or for customers to self-declare a need for additional support.

The design of sales processes allows for opportunities to explore potential signs of vulnerability, impact and support needs when conducted face to face or via telephone for both personal and business customers. Of the cases assessed during this review, there was evidence of probing and questioning to understand the needs of the customer. However, we found that there were inconsistencies in approach both within firms and across the review population as a whole. We also identified cases where there was a lack of record keeping, which meant that had any vulnerability been declared or support need identified, there was a risk that this was not considered during any future engagement with the customer. This appeared particularly prevalent within the Relationship Managed account area for business lending.

The identification or declaration of a vulnerability should be supported with a 'tell us once' approach to recording of information to ensure any support needs are recognisable by all staff, regardless of when they interact with the customer. This also allows for regular review and update of a customer's situation to ensure the right support is provided when required. Vulnerabilities can be both transient or permanent and it is important that the identification methods used by firms take account of this.

In the payments space, the proactive identification of customers vulnerable to scams has improved since inception of the CRM Code. However, again there is still a level of inconsistency across firms, with staff not using or demonstrating the necessary skills to probe potential triggers of vulnerability. There is also a similar read across for the recording of a customer's vulnerability or understanding of how the scam has impacted them and whether there are further support needs.

For these customers it is important that whilst reimbursement is forthcoming where they are vulnerable to the scam, firms should also look to identify if there is any wider vulnerability, either as a result of the scam or in spite of the scam. Where a wider vulnerability is identified, then it is incumbent on firms to ensure this is managed as it should be, had it been identified at a different point in the customer journey.

For the latter part of a customer journey, specifically those customers facing financial difficulties, we found that this is often the point at which vulnerabilities become more visible to firms. Staff are trained to identify any vulnerability when assisting customers in difficulty but again there were inconsistencies and is an area where we believe there is more work needed to fully embed training. A key area of focus for training should be on the softer skills needed to be empathetic whilst being able to draw out information from customers through sensitive questioning and probing. Again, this should be underpinned by well-designed and executed QA and oversight.

Within digital channels we found less opportunities to identify vulnerability due to systems not currently being developed to allow this to occur easily. It is acknowledged that customers may use a digital channel rather than interact directly with frontline staff, either because of the misconception their vulnerability may impact their ability to obtain credit, make affordable repayments or because it is a more suitable channel for their needs. Nevertheless, the challenge for firms seems to be in enabling identification or self-declaration of vulnerability and additional support needs, without adding too much friction into the process.

Consequently, we found that the level of vulnerability disclosure was low in digital channels, and given the rise in digitisation and customers' usage of this channel, firms need to develop ways to improve vulnerability disclosure as a priority.

It is expected that wherever a customer is within their journey, they are presented with an opportunity to either raise a need for further support to help with their vulnerability or situation. Or indeed the firm has suitably trained and skilled staff to establish this through appropriate probing and questioning.

Good Practice:

- Where training had embedded, we saw examples of clear and focussed conversations with customers, which helped staff to identify support needs. Often where the focus of the conversation was on the support rather than just trying to 'box off' a vulnerability, better outcomes were achieved.
- Initiatives to allow customers to pro-actively request support or other measures to assist them in managing their accounts, helped firms to identify where focus needed to be within their vulnerable customer strategy. Through these sorts of insights firms have the ability to continually review and refresh the support offered to vulnerable customers, as well as those customers without a specific vulnerability.

Areas for improvement:

- Firms should ensure that processes and systems allow for the identification or disclosure of vulnerability at all key points in the customer journey, irrespective of channel.

- Firms should ensure that staff have the appropriate skills and support to empathetically engage with vulnerable customers and explore their circumstances, with a view to identifying and supporting their needs.
- With the customer's consent, firms should ensure that any vulnerability or related support needs are clearly recorded for future reference. This should be supported with a 'tell us once' approach.
- Firms should ensure that processes allow for review of the customer's circumstances to understand how any identified vulnerability is still having an impact and whether there are ongoing or further support needs.
- Improvements to identification of vulnerability within digital journeys should also link into accurate record keeping, which would allow support to be provided regardless of which channels customers engage through in future.

3.3 Support for vulnerable customers

Once a customer has either been identified as vulnerable or proactively raised a vulnerability, the next step is to ensure the correct support is provided to achieve a good customer outcome.

Support for vulnerable customers needs to be available throughout the customer journey, whether this is applying for credit, running their account or making payments. Once the support need has been agreed, this should not be the end of the story. Firms need to ensure there is a regular review of the customer's circumstances, in line with customer needs and agreement, to ensure the support remains appropriate and useful.

The following section of the report sets out a number of areas where there needs to be consideration of customers' support needs and how this can feature in the actions firms take.

Communication

We considered the extent to which firms' communications support vulnerable customers in understanding and making informed decisions about products, as well as to manage their accounts from application, through servicing and if they fall into financial difficulties.

Lending

It was clear from the information received that firms have considered the language used within product sale and welcome documentation packs. This also included consideration of customers with accessibility needs. It is important to maintain focus on the content of documentation to ensure this is easily understandable for all customers, but particularly those with a vulnerability, especially if this is linked to mental capacity.

Beyond product sale communications, it was not always evident what support solutions had been considered to assist customers through the application process and with the ongoing management of the account. We also observed a lack of flexibility within processes to support vulnerable customers who may have difficulty in understanding information. For example, not allowing a third party or appointed power of attorney to assist the customer and relay product sale or application information.

It was confirmed by all firms that where a customer has any vulnerability or accessibility needs which may result in a different format being required for documentation, this can normally be accommodated. This is sometimes harder to achieve in a digital channel, however we are aware that some firms are working towards adjustments to enable this specific cohort of customers to easily access information.

Customer facing material was also available both in hard copy and online, to assist customers. Some firms' customer facing material focussed on money help and guidance for customers in financial difficulties. Others had taken a broader approach, covering topics such as mental health conditions, long term illnesses, financial abuse and sudden life events, along with signposting to independent third-party charities/organisations that can provide support. As customer support needs evolve, it is important that firms consider the type and impact of signposting opportunities to ensure these remain relevant and timely.

Payments

Within the payments space, particularly when customers had been the victim of an APP scam, we found that verbal communications were more appropriately tailored where a vulnerability had been identified or was known. This was mainly related to support for customers who had been identified as being vulnerable to the scam rather than wider vulnerability, as mentioned previously. However, this was not always reflected within the letters issued following the completion of the assessment of the customer's case. Across the industry, outcome letters still require adjustment to make it clear the rationale for the reimbursement decision and how firms have arrived at such a decision. In addition, firms should consider whether they need to take into account any known vulnerability, either to the scam itself or a wider vulnerability, and how this will be supported.

Financial difficulty

From a financial difficulties perspective, we identified some good examples of clear customer communications within our testing of both the personal and business Standards. It is noted however, that communication within the personal lending space appears to be more mature

than within the business lending. The best examples were more verbal than written albeit there was a level of inconsistency both within, and across, firms.

In situations where a customer was identified as being vulnerable, staff were able to adjust the tone and focus of their conversation when providing support to these customers. This included gaining an understanding of the situation and then ensuring the support being offered was appropriate to the circumstances. Some of the positive elements covered areas such as signposting to appropriate charities or organisations with a focus within the area of vulnerability. Or the ways in which the firm could interact with the customer taking into consideration what worked best for their circumstances.

We found that inconsistency tended to arise when discussing the accounts and the options for management thereof with the customer and staff would conflate financial vulnerability with wider indicators of vulnerability. We are conscious that within the financial difficulties arena, one can in fact trigger the other, but it is our view that some conversations could have been clearer. Areas such as explaining the implications of missed payments or the purpose of breathing space were not always clear. We also saw examples of automatically putting accounts on hold when a vulnerability was identified but without an explanation of for how long, the benefit of this or whether there was anything needed from the customer.

Being clearer about these actions and any related implications could assist vulnerable customers in making more informed choices and ensuring their situation was not exacerbated due to misinformation, or indeed, a lack of information.

We found that the subsequent written communications were not generally reflective of conversations that may have been held. At times, these were quite severe in tone with a very structured focus on securing repayment of arrears, rather than offering support for customers. This, in turn, is unlikely to encourage engagement, particularly from customers who may already have elevated stress and anxiety levels due to their vulnerability. We also found that written communications did not include details of the support that could be provided despite a vulnerability being identified. Signposting was often minimal, generic in nature and positioned towards the end of written communications, therefore limiting the impact.

Good practice:

- We saw examples of ‘warm’ transfer processes for customers who want to engage with a third-party debt advisor or specialist support service. This led to increased levels of uptake by customers which will help to achieve good customer outcomes.
- Where signposting was done well, staff would highlight the benefits of third-party support to the customer and link this back to how this could improve their situation. Conversations typically included details of how external bodies could assist with management of the customer’s creditors, maximising income and specialist organisations

who could assist customers with specific vulnerabilities, for example, gambling issues, addiction or domestic abuse victims.

Areas for Improvement:

- The tone and manner of communications needs to encourage engagement so vulnerable customers feel supported throughout their relationship with their firm. This should include access to clear information about the options available that consider their vulnerability needs.
- Firms need to ensure signposting is prominent and where possible, tailored to the customer's circumstances. This will enable customers to understand the benefits of accessing third-party assistance and make an informed decision on how to proceed.

Specialist support and escalation

The approach taken by firms to support vulnerable customers differed depending upon their size, structure and resources available. Some firms had established dedicated specialist support units used for referral of all vulnerable customers, regardless of where they sat within their account lifecycle. Whereas others had specialists embedded within teams or indeed had taken the approach of upskilling all staff to assist with identifying and supporting vulnerable customers.

It is worth noting that we feel there is no right or wrong approach but that the design of support should be such to ensure the customer is put at the heart. Within some firms we did identify there was not the ability for staff to escalate cases or seek guidance to assist with how to support a vulnerable customer. Escalation routes need to be available for staff regardless of the structure or format of the business but again designed to ensure support can be provided and the best customer outcomes are achieved.

Some firms have designed specific systems and information repositories which staff can access to help answer any queries which may arise when they are supporting customers. These are regularly reviewed to understand the nature of questions which are being raised so the information can be refreshed to ensure it remains appropriately focussed.

Firms had a range of solutions available to assist and support vulnerable customers determined by their individual needs. This included such initiatives as spending blocks, enabling third-party representatives to support customers (once lending has been agreed and provided) or providing information in braille or 'speech to text'. For those customers also experiencing financial difficulties, there was flexibility which enabled customers with particularly acute vulnerabilities to be taken out of the outbound contact strategy, preventing calls being made to them.

As mentioned, there were occasions where there was conflation between financial difficulty and vulnerability. In these instances, the focus was very much on addressing the customer's financial

difficulty rather than identifying and supporting the vulnerability, which may in turn have automatically helped with their financial situation.

Firms have a range of forbearance options in place that can be utilised for vulnerable customers, including short term holds and breathing space, reduced payment plans, re-age of debt and write off. Breathing space was mainly used for vulnerable customers however, it was not always clear that the customers vulnerability had been considered to establish if that was appropriate given their circumstances.

Where firms invite customers to engage with them digitally to set up repayment plans, consideration should be given to the appropriateness of this channel for different vulnerability types. For example, where behavioural characteristics such as a lack of concentration or difficulty memorising information may impact the customers' ability to provide accurate and up to date information. Where firms determine a digital portal provides yet further choice for customers, particularly those who may not wish to engage directly, there should be consideration of how this aligns with face to face or telephony interactions to ensure the requisite controls and identification of vulnerability are established to provide the correct support needed.

Our review found that once a customer is identified as having a vulnerability and potentially needing additional support, there is very little ongoing proactive review of their circumstances and needs, with reliance sometimes being placed on customers proactively providing updates. We also found that staff did not always actively seek updates to vulnerable circumstances when they contacted customers to discuss next steps following the end of forbearance or other temporary support measures.

External Recovery

Within some firms, the later part of a recovery strategy is to either outsource collection of the debt to a third party or to onward sell the debt. For those customers with business accounts, this may also involve the services of an Insolvency Practitioner should the financial position of the business require this approach.

For the purposes of this review, we focussed our attention on the strategies of firms and their use of debt collection and debt purchase firms. Our assessment did not include a review of the actual third parties being used but rather attention was placed on the controls and governance within firms in ensuring the Standards continued to be met.

As part of the due diligence process when onboarding either a Debt Collection Agency (DCA) or Debt Purchase Firm (DPF), we found that the assessments included a check on the appropriateness of arrangements for servicing vulnerable customer debt. This included reviews of vulnerability policies and procedures, onsite visits, reviews of regulatory permissions, regular

vulnerable customer call observations, reviews of MI and oversight of QA processes. On an ongoing basis, firms' focus tended to be through review of cases and on MI produced by the third party.

This approach allowed firms to ensure the third parties, whilst perhaps not themselves a registered firm with the LSB, were maintaining the expectations set out in the Standards for both business and personal customers.

Once a firm made the decision to either outsource or sell a book of debt, systems and controls were designed to exclude vulnerable customers with ongoing mental health or critical illness issues. We also identified some firms had further controls in place to exclude cohorts of customer or even individual cases where transfer of ownership or service was not felt to be appropriate given the nature of the customer's vulnerability.

Where issues have been identified earlier in relation to record keeping, this can cause issues in ensuring the correct cases are included for onward collection or sale of debt. We saw examples of inconsistency in approach, with a lack of flexibility in categorising customer vulnerabilities, with the severity of vulnerability not always being considered when ringfencing accounts for external recovery. For example, customers who were victims of domestic abuse or serious crime could have associated mental health vulnerabilities due to the trauma of their experiences.

Good practice:

- Firms have begun using internal digital solutions designed to help support staff when talking to customers and managing vulnerable situations. Interactive information systems allow staff to request real time guidance to assist them in helping customers. Continuous monitoring and review of such systems will ensure information remains up to date and relevant.
- Where firms had the ability to make adjustments to contact strategies or the method of contact, this was helpful for customers with certain vulnerabilities, or those who are unable to converse via standard contact methods, such as telephony.
- When cases are outsourced for collection or as part of a debt sale, firms would include the ability for cases to be returned or bought back, should a vulnerability subsequently be identified where this would be a better outcome for the customer.

Areas for Improvement:

- Strategies must recognise the difference between financial difficulty and vulnerability so that collections processes and staff apply appropriate focus to identifying and supporting customer vulnerabilities, as well as to treating financial difficulty.
- Firms need to ensure that forbearance treatments fully account for the vulnerable customer's circumstances when deciding appropriate financial support solutions.

- Proactive regular reviews of vulnerable customers' circumstances and support needs should be completed so adjustments can be made where appropriate.
- Staff should have the ability to escalate queries or receive additional guidance which subsequently empowers them to explore vulnerability impacts and implement appropriate support, in consideration of the customers' needs and circumstances.
- Firms should ensure their processes and considerations in respect of excluding vulnerable customers from debt sale or transfer to a DCA are robust and consider all vulnerability impacts which may contribute to ongoing mental health issues or critical illness.
- Firms should ensure that improvements to record keeping should also consider future strategies for external recovery to ensure accounts are not transferred where this could have a poor outcome for customers, given the nature of their vulnerability.

4. Conclusion and Next Steps

Our thematic review of vulnerability was intended to assess the extent to which vulnerable customers are receiving fair outcomes from firms, in line with the personal and business Standards and the CRM Code, by considering the effectiveness of firm's vulnerability frameworks and key aspects of the customer journey.

We would like to thank all those involved in the review in enabling us to conduct our work.

Overall, firms have vulnerability strategies that are embedded and designed to comply with the expectations of the personal and business Standards and the Code in respect of vulnerability. We also identified that vulnerability strategies remain a continual focus for firms who have also sought internal and external insights to understand the appropriateness of their vulnerability strategy for their business model, customer base and external developments within the market.

There are clear frameworks for reporting and overseeing vulnerability strategies, as well as training and support for the identification and support of vulnerable customers. Furthermore, the need to consider vulnerability is captured within monitoring and assurance controls and processes for product design and review, product sales, collections and recoveries and debt sale for the Standards; and within the scams education and awareness strategies and claims assessment journeys in respect of the Code.

Nevertheless, we have found inconsistencies and deficiencies across all firms in the way that vulnerability is identified, assessed, treated, recorded, monitored and supported, with further development required to ensure adherence to both the personal and business Standards. Similarly, in our 2022 review of adherence to the CRM Code, we found that firms are inconsistent in their ability to identify and support customers who may be vulnerable to a scam. There is clearly more that firms need to do, overall, to develop and enhance their vulnerability strategies

to achieve both effective and consistent processes. Some firms within our review had self-identified a few of the areas highlighted as needing improvement in the report and were either considering next steps or have plans in place to address the needs.

It is especially important that improvements are progressed given that firms are identifying an increasing level of vulnerability incidence, due in part to the transition away from pandemic conditions and other factors, including the ensuing cost-of-living crisis. Firms are increasingly turning to customer-led digital solutions to manage volumes and drive disclosure. Whilst we encourage this activity, where firms engage with their customers via predominantly digital means, strategies should be designed with a recognition of the need to interact with customers to review their circumstances in depth and ensure that support solutions are appropriate and effective, through whichever channel the customer prefers to engage.

Next steps

All firms have now received their individual review reports, together with any associated actions raised by the LSB. We will continue to work with firms to ensure that all actions are remediated to drive consistency and resolve deficiencies. Additionally, we would encourage our entire registered firm base to compare our findings to their own approaches and consider if there are any learnings for them to apply to their own vulnerability strategies and activities across the full range of Standards and the CRM Code.

Our report will be used to inform the LSB's wider work focussing on the identification, treatment and support of vulnerable customers and how the level and nature of vulnerability has evolved. This will help inform whether updates to the Standards or Code, or the accompanying guidance documents, are required. This will also feed into our future Insight and thought leadership work which will be shared with registered firms to ensure that they are prioritising support for, and protection of, vulnerable customers.

Appendix 1

Scope and Objectives

The review aimed to provide assurance of how registered firms' adherence to the business and personal Standards in respect of the identification and treatment of customer vulnerability and to understand how arrangements are meeting evolving vulnerability circumstances and needs.¹

The review objectives were to assess the following:

- The effectiveness of firms' frameworks and reporting, in providing their senior management and board with a holistic view of performance in respect of vulnerable customers strategies throughout their interactions with the firm.
- The effectiveness of training and support for all staff to ensure they can identify and support vulnerable customers in accordance with firms' strategies, policies and processes.
- The effectiveness of monitoring and assurance controls in ensuring vulnerability policies, processes and controls are designed and operating effectively and delivering fair customer outcomes.
- The extent to which the product design and review processes consider vulnerability and ensures products are appropriately designed and targeted to mitigate against risk of harm and offer appropriate support throughout the lifecycle of the product.
- The extent to which firms' sales and credit assessment processes ensure vulnerable customers are identified and their needs appropriately supported.
- The effectiveness of firms' identification and treatment of vulnerable customers in financial difficulties, in providing appropriate support to help them deal with their debts in the most suitable way.
- The effectiveness of debt sale processes and controls in ensuring debts for customers with vulnerabilities that affect their ability to repay, such as ongoing mental health or critical illness, are not sold.
- Assessing the procedures firms have in place to identify customers vulnerable to APP scams, and how the relevant CRM Code provisions are applied across the customer journey.

The scope of the review covered vulnerability strategies, policies and processes in relation to:

- product and service design;
- credit application process;
- financial difficulty and forbearance treatments;
- debt collection and portfolio management;
- the monitoring and assurance framework; and

¹ Any references to customer or customers apply to business and personal customers unless otherwise stated.

- the extent to which firms adopt a ‘tell us once’ approach across all channels, processes and products.

All communication channels, including, telephony, face-to-face and digital platforms and all products in scope of the personal and business standards, were included.

The review was conducted across sample of five firms in in relation to the personal and business Standards, whereas the review work on the CRM Code covered all nine signatory firms.

Out of scope

In light of the LSB’s oversight work on Money Management, Credit Monitoring, and the Standards of Lending Practice for business customers in Asset Finance during Q3 and Q4 2021, these areas were excluded from this review.

The review was solely focussed on firms’ adherence to the Standards and CRM Code, in line with the LSB’s remit to provide independent oversight. Therefore, while it is recognised vulnerability has been an ongoing area of focus with the implementation of the FCA’s FG21/1 ‘Guidance for firms on the fair treatment of vulnerable customers’, this review did not include these requirements.

Methodology and Approach

The approach to this review as related to the personal and business Standards commenced with a Request For Information (RFI), which enabled a desk-based review of each firm’s policies, procedures, controls and governance as related to vulnerable customers.

This was followed by onsite visits to conduct call and file reviews, of 50 cases per firm split across credit assessment, collections and recoveries. This testing was designed to assess the extent to which firms’ vulnerability strategies and frameworks are aligned to the Standards and delivering fair outcomes for vulnerable customers.

This included reviewing how the identification and treatment of vulnerable customers at key points of the customer lifecycle, including product sale and credit assessment, collections and recoveries, is completed.

Following onsite testing, meetings with management and key personnel were held through virtual channels. These meetings provided an opportunity to clarify our understanding of the governance, controls and oversight arrangements in respect of the Standards across the whole customer journey and to validate these against the results of our testing. Once findings from the onsite testing and management meetings had been established a close out meeting was held to

discuss the initial findings of the review. An individual report, setting out the LSB's findings from the assessment has been issued to each firm, including any required actions which will be tracked through to completion.

A similar methodology and approach was conducted for the review of the CRM Code conducted earlier in 2022. This too included a focussed RFI, case file testing and meetings with Management to check our understanding.