Customer vulnerability and current accounts – a review of UK practice

A report by the Fairbanking Foundation

March 2017

fairbanking
Banking made fairer for your financial well-being

Contents

About The Fairbanking Foundation:

The Fairbanking Foundation is a charity dedicated to encouraging and helping banking institutions to improve the financial well-being of their customers and thereby the UK public as a whole. Our work is designed to provide well-researched, independent and insightful new input to assist in producing financial products that benefit customers. In 2011 the first Fairbanking Marks were granted for products that have features which help customers alter their financial behaviour. In 2013, the Fairbanking Foundation became the first certification body in the UK for financial products to be accredited by the UK Accreditation Service for meeting international standards.

More information about Fairbanking can be found at **www.fairbanking.org.uk**
and enquiries can be sent to **info@fairbanking.org.uk**.

Written by Antony Elliott OBE, FCIB, Chief Executive, The Fairbanking Foundation
and Melanie Worthy, policy consultant
Published by The Fairbanking Foundation, March 2017

Acknowledgements
The Fairbanking Foundation was assisted by a small panel of experts who provided invaluable advice on the shaping of the survey and research. It is enormously grateful to:
- Chris Fitch, Research Fellow, Personal Finance Research Centre, Bristol University;
- Leonora Miles, Senior Policy Adviser (Financial Services), Macmillan Cancer Support;
- David Steele, Policy Manager, Financial Services, Age UK.

Professor Michael Mainelli and his colleagues at Z/Yen Group managed the survey process.
Melanie Worthy, policy consultant, assisted with the shaping of the survey and co-authored the report.

This report is also a reflection of other contributions from people both within and outside the financial services sector who helped shape the necessarily more nuanced approach with regard to this important subject. The Fairbanking Foundation is most appreciative of the support and encouragement received.

The Fairbanking Foundation® is a company limited by guarantee registered in England under number 06625040 and registered as a charity in England and Wales under number 1125769.
Registered office: 20–22 Wenlock Road, London N1 7GU..

Executive Summary

What we did

We identified areas where customers in vulnerable circumstances with a Mental Capacity Limitation (MCL) and/or a Long Term Condition (LTC)[1] would benefit from specialist services in relation to their current account. A survey was conducted of financial institutions to identify the customer service practices that are being adopted. We were encouraged to receive responses from six major providers in the market.

There appears to be little measurement, or monitoring, of the numbers of customers in vulnerable circumstances, or heed of population forecasts

Why we did this

This is the first survey by the Fairbanking Foundation of how financial institutions treat current account customers in vulnerable circumstances with MCLs or LTCs. The purpose of the report is to:

- highlight current market practice, gauge the market's response to recent regulatory focus and gain an understanding of how the experience of customers in this situation may improve in coming years; and

- identify whether practices are sufficiently defined to extend the Fairbanking Foundation's certification programme to measure consistency of service in this important area.

The survey focused on financial institutions' current account (with overdraft facility) product services for customers in vulnerable circumstances.

Service gap

The Fairbanking Foundation finds that there are significant gaps in the services provided by financial institutions for customers in vulnerable circumstances. As a result the outcomes of these customers' experiences dealing with financial institutions falls short. Financial institutions recognise that they need to do much more to improve the experience of these customers. They are engaged in improving processes and services but this is against a backdrop of a complex working environment and constraints on resources. The required changes are not likely to happen quickly without stronger commitment and intervention by senior management.

1. Mental Capacity is a person's ability to make an informed decision at a specific point in time. It is determined by a person's ability to: understand information; remember information; weigh-up information; and make/communicate an informed decision. Consequently, mental incapacity, or a mental capacity limitation, is a person's inability to make an informed decision at a specific point in time due to an "impairment or disturbance in the functioning of the mind or brain". This can, for example, include: some forms of mental illness; dementia; significant learning disabilities; the long-term effects of brain damage; physical or medical conditions that cause confusion, drowsiness, loss of consciousness; delirium; concussion following a head injury; and the symptoms of alcohol or drug use. Law and regulatory guidance expect lenders to presume that all borrowers have the mental capacity to make an informed decision about a loan (to prevent discrimination against people with certain conditions), unless the lender also knows, or reasonably suspects, that a mental capacity limitation exists.

A long-term condition (LTC) is a physical or mental illness that usually lasts a year or longer, and which may require ongoing care, support and treatment. Examples of LTCs can include physical conditions such as cancer, heart disease, diabetes, chronic obstructive pulmonary disease (COPD), musculoskeletal disorders and complications following a stroke. LTCs also include mental illnesses such as anxiety, depression, dementia, schizophrenia and bipolar disorder. Some people have more than one LTC at the same time. Many people with a physical health problem, for example, will experience mental illnesses such as anxiety or depression at the same time. Around half of all people with cancer experience levels of anxiety and depression severe enough to affect adversely their quality of life. Fairbanking has included in its scope LTCs that cause mental capacity limitations.

Need for early intervention

A key finding is that financial institutions are missing the opportunity to identify vulnerable customers and offer appropriate services, support or intervention, at a sufficiently early stage. This is a major failing. In general, the identification of vulnerability due to a health condition does not emerge until a customer has 'landed' in the collections and debt recovery department. At this point, the chance to provide an optimal solution for all parties has often passed, and financial problems and emotional distress are often compounded.

While it is good that some financial institutions have established specialist customer support services within their debt recovery operations, there is a need to loopback and put this knowledge to use and integrate appropriate approaches earlier in the customer engagement process.

There appears to be little measurement, or monitoring, of the numbers of customers in vulnerable circumstances, or heed of population forecasts, which is worrying given the expected growth of this group predicted by all demographic indicators.

Current practice

The survey covered three areas fundamental to servicing customers in vulnerable circumstances: handling information and training; establishing and operating dependency[2] arrangements; and treatment of fraud and scams. The findings are:

Handling information and training

- Financial institutions are improving their processes for collecting information when vulnerability is evident, including the ways that they ' flag' or mark customer records with appropriate information, plus are using the information held for monitoring, and they are engaged in extensive technological improvements, which will enable the earlier identification and servicing of customers in vulnerable circumstances, but
  - they are yet to establish a standard approach to information handling and
  - appear confused in respect of their data privacy obligations.

- They are engaged in extensive technological improvements, which will enable the earlier identification and servicing of customers in vulnerable circumstances.

Dependency arrangements

- Financial institutions find this difficult terrain. There is no standard approach applied for establishing dependency arrangements but the institutions are starting to embed good protocols and support structures and practical measures to establish dependency arrangements, plus they are responsive in emergency situations.

- Independent evidence from the Office of the Public Guardian (OPG) points to difficulties for customers in vulnerable circumstances and their representatives because of uneven industry practice, inconsistent services, and an awareness, training and skills gap among staff.

> *Financial institutions are failing to grapple with fraud on behalf of customers in vulnerable circumstances and need to adopt a more nuanced service here.*

- Although there is no standard approach, there is sufficient good practice here to establish a set of criteria that could be tested. Fairbanking believes it would be possible to devise a framework for the measurement of dependency arrangements set up for customers in vulnerable circumstances.

Treatment of fraud and scams

- Financial institutions do recognise the need to grapple with fraud on behalf of customers,

2 Dependency is defined as where a customer's account is handled by a third party.

including those in vulnerable circumstances. But they need to adopt a more nuanced service here. Vulnerable customers suffer more distress, may not realise immediately that they have been victims of fraud, and need differentiated treatment.

- There are encouraging examples of intervention on behalf of customers where a scam activity is suspected, including the ability to "pause" and interrupt payments while the customer reconsiders the transaction. Financial institutions nevertheless have further scope to improve and apply consistent practices on scam prevention for customers in vulnerable circumstances. However, good initiatives designed to prevent scams are starting to emerge.

Service exemplars

There are encouraging signs. We did observe many instances of good practice, including liaison partnerships with charities and external organisations, particularly with training of staff.

The examples are highlighted throughout the report, with the proviso that no independent evidence was obtained to verify the effectiveness of financial institutions' service to customers in vulnerable circumstances.

Positive initiatives are continuing and will be further aided by technology innovations. These will improve data recording and staff/colleague and customer communications. They will also enable more prompt intervention and hopefully close the gap in treatment earlier.

We are pleased to highlight these as examples of positive practice:

- **Barclays:** early adoption of flags and care markers in operational processes; Community Driving Licence (CDL) to support staff.

- **RBS:** good monitoring and modelling of customer behaviour patterns, enabling earlier identification of vulnerability, plus its widespread adoption of the Dementia Friendly Financial Services Charter.

- **Santander:** helpful advice, budgetary tools and product solutions for customers identified with a potential vulnerability, an explicit business focus on good customer outcomes; operation of a centre of excellence for assisting in the registration and operation of dependency arrangements by attorneys and deputies.

- **Lloyds:** plans to extend further the TEXAS protocol to all retail operations across the banking group.

- **Clydesdale:** operates vulnerable procedures within its fraud department to ensure appropriate safeguards are put in place; investigation of mass scams, e.g. multiple cheque writing.

Prospects for future measurement?

The Fairbanking Foundation concludes that it cannot yet devise a comprehensive or meaningful framework for the measurement and certification of standards of financial institutions' services to customers in vulnerable circumstances with MCL or LTC regarding current accounts.

Encouragingly, financial institutions are starting to grapple with this significant challenge and the Fairbanking Foundation is confident that it will be possible for measurement in due course. But, for the time being, this must remain, for the large part, aspirational. However, the Foundation intends to consult further on the possibility of specific certification regarding two discrete aspects of the service offer to vulnerable customers: dependency arrangements and scam-prevention activities.

The Fairbanking Foundation is pleased to share these findings, which it hopes will expedite the adoption of good practice, and looks forward to further dialogue with stakeholders.

1. Introduction and approach

Industry context

In response to the challenge, laid down by the FCA, following its publication of Occasional Paper *Consumer Vulnerability*[3], there has been much stakeholder and industry activity. The FCA paper highlighted the sheer scale of customer vulnerability in the UK with:

- 6.5m people having significant caring responsibilities for others. This is expected to rise to 9m by 2037 (Carers UK);

Vulnerability has many forms and is inherently difficult to define. This survey has restricted its focus to customers in vulnerable circumstances, due to mental capacity limitation, which may also be due to a LTC

- 800,000 people living with various degrees of dementia. This is expected to double over the next 40 years (Carers UK);

- in any given year, one in four adults experiencing at least one mental disorder (NHS statistics); and

- people with mental health issues being three times more likely to have problems with debt (Office for National Statistic quoted in MALG 2009 Good Practice Awareness Guidelines).

The British Bankers Association (BBA) established a Vulnerability Taskforce and published a set of recommendations and principles in 2016.

Simultaneously, Fairbanking developed a series of questions on vulnerability, which formed the basis of this survey and research.

Fairbanking's survey was conducted between June and August, 2016 and reviewed six of the nine themes under which the Vulnerability Taskforce grouped its set of *principles and recommendations*, albeit in the context of current accounts:

- sensitive flexible response;
- effective access to support;
- one-stop notice;
- specialist help available;
- easy for friends and family to support; and
- scam protection.

Approach and scope

This survey was designed to establish possible areas for evidencing the service standards in financial institutions for customers in vulnerable circumstances and gauging market readiness. It has focused on current account (with overdraft) services for customers in vulnerable circumstances due to mental capacity issues (some of which may arise from long-term health conditions). This is a natural extension from Fairbanking's existing suite of certification.

Six financial institutions (**Barclays, Clydesdale, M&S, Lloyds, RBS** and **Santander**[4]) took part in the survey, representing approximately 75%[5] of the current account market in the UK.

Vulnerability has many forms and is inherently difficult to define. This survey has restricted its focus to customers in vulnerable circumstances, due to mental capacity limitation as defined below[5]. Mental capacity can be verified with more certainty as a potential indicator of customer vulnerability. It is, therefore, deemed a more reliable measurement.

3 FCA: Occasional Paper no 8, *Consumer Vulnerability*, February 2015

4 HSBC did not complete for logistical reasons, but would want to take part in any future survey.

5 Source: CMA statistics, 2016.

Furthermore, financial institutions already must comply with related legislation and regulation (such as the Equality Act, Mental Capacity Act and CONC), so we would expect to find this reflected in their operating protocols.

The survey focused on the services received by customers in vulnerable circumstances, due to a mental capacity limitation, in relation to a "current account with overdraft". It examined four key areas to determine service standards, support offered and the impact on financial wellbeing. These were:

- information handling;
- dependency arrangements;
- treatment of fraud; and
- treatment of scams.

Please note the findings below in relation to "one", "some", "number of", "most" or "all" financial institutions relate only to the six financial institutions surveyed here.

2. Use of customer information

2.1 Introduction

This section of the survey looked at how financial institutions handled information about customers who might be vulnerable, which would lead to appropriate treatment and services. It also examined what financial institutions were doing to identify and apply indicators of vulnerability; the role of specialist customer units; the approach to data-sharing across a financial institution; and training provision, plus signposting customers in vulnerable circumstances to help from external organisations.

2.2 Current and best practice

For the financial institutions we surveyed we found:

Identifying customers

- All financial institutions had established customer vulnerability operational frameworks to identify and support customers, But there is no sign, at this stage, that they are identifying significant numbers of customers in vulnerable circumstances, or projecting future expected growth.

- It is clear that financial institutions do not usually identify customer vulnerability, until the customer has 'landed' in the collections and credit recovery departments which communicate with and act towards customers in more personalised or bespoke ways than other departments.

- Most are following established industry protocols such as:

  - TEXAS Thank, Explain, Explicit Consent, Ask, Signpost (customer protocol) in relation to customers in vulnerable circumstances and

  - IDEA (Impact, Duration, Experience, Assistance).

- All share data about customer vulnerability within the financial institution to some degree. Some financial institutions apply 'flags' to customer records on their systems, but there is evident nervousness and uncertainty among some about how to do this. This largely stems from lack of confidence and clarity about the provisions of the Data Protection Act and other legislation, culminating in an over-cautious approach to compliance.

- All enable staff to capture and record, with the customer's permission, details of any accessibility support needs the customer may have.

- Most are developing technology to provide for appropriate flags to be placed on customer accounts and alert customer advisers to identify, and record, information about a customer who might need extra support.

- Some are monitoring the success of the assistance provided to customers in vulnerable circumstances.

Barclays: *"Frontline colleagues can use care markers on a customer's records, which can be used where a customer has a condition or need that they either want colleagues to be aware of, or where it requires us to respond differently (for example to say they are deaf so our colleagues can be alerted to this when a customer with this marker contacts us). Alongside these care markers, we are looking at other mechanisms by which we can record where a customer is in vulnerable circumstances. Within our collections team, where a customer gives us permission to log their circumstances, we will make detailed notes and put a flag on the account that differentiates the severity of the vulnerability. However, this flag doesn't drive a different solution, rather it prepares colleagues to know how severe this customer's situation is. Where a customer does not give express consent to record vulnerability, or details of it, we make generic notes and follow our usual business processes."*

Lloyds: *"We are extending the TEXAS framework to the whole of the bank's retail team."*

Barclays: *"The Group's Customer Vulnerability Framework includes a Recording and Sharing workstream that provides subject matter expertise and supports the business regarding data privacy and information collection* *activities. The workstream has updated all relevant bank policies to reflect extraordinary situations, such as cases whereby a customer is especially susceptible to detriment as a result of vulnerabilities. "*

Santander: *"Information is only shared across departments that deal with financial difficulty. We keep notes in accordance with requirements under DPA when sharing this information across departments and if we ask for consent first."*

Barclays: *"Within our branch and telephony network, information on customers would be recorded on a notepad. We are currently reviewing how we can improve processes for customers in vulnerable circumstances to ensure that colleagues are clear what information to save, how and when."*

RBS*: "We are monitoring effective ways in which we can use the data on customer behavioural patterns and any changes that occur that signify that the customer may benefit from an account review. Behavioural and usage patterns e.g. increase in cash line transactions, cheque book ordering, replacement debit card/PIN, increase in branch visits or late bill payments."*

RBS: *"We incorporate customer impact measures, which include customers in vulnerable circumstances, within our monthly product monitoring. These measures focus on customer detriment and desired outcomes. For each product area, specific MI and thresholds have been identified that are the best indicators for that product of potential customer detriment. In addition, we undertake regular customer research and mystery shopping as well as post implementation reviews after any changes have been made to ensure the required changes are happening as expected and highlight any customer impact/learnings from the changes."*

Lloyds: *"We monitor cheque, debit card and international payments in place, with referrals to an account manager where concerns are identified about transaction activity among customers in vulnerable circumstances."*

Clydesdale: *"We continue to monitor customers in vulnerable circumstances we have identified and assisted, e.g. through transaction analysis to ensure that the steps taken are appropriate to provide adequate support to them."*

Customer communication and awareness

- All financial institutions provide a range of multichannel communication mediums for customers to get in touch to discuss or advise on a vulnerability, or potentially vulnerable situation.

- All have tools to assist customers in vulnerable circumstances communicate with the financial institution and transact business at different stages of the customer product lifecycle.

- All have a range of communications materials, particularly via websites, alerting customers to where they can get help and assistance in the financial institution for a vulnerability or special need.

- One proactively communicates with customers when certain trigger events have taken place on the account, either by outbound calling, letter or text, advising that assistance is available and to offer help with budgeting.

- All signpost additional sources of help from external authorities and have contact with charities, e.g. Dementia Support.

- One monitors complaints handling among customers in vulnerable circumstances in particular.

Clydesdale*: "To ensure that additional support is given to customers facing difficult circumstances, there is also a prompt within the online application process to contact us if the customer feels additional support is required."*

Clydesdale*: "We offer a customer with disabilities a variety of tools to assist their communication. These include but are not* *limited to ease of access, text-to-speech functionality on our ATMs, chip and signature debit cards, Internet and telephone banking services for the blind or visually impaired and Minicom facilities. Our website provides links to guidance on accessibility options for popular operating systems and browsers. We also provide statements, documents or information packs in braille, large print and audio formats."*

***RBS**: "We use contactless and fingerprint recognition technology in mobile banking, which removes the need for a customer to have more than one PIN. This benefits customers in vulnerable circumstances."*

Role of the Collections department

- When identified, customer vulnerability is usually only determined when the customer arrives in the collections department/team.
- Some financial institutions reported they make credit decisions intended to support customers to ease any short and long-term financial difficulties; this is a general practice that they should be following anyway. Some make credit decisions to support customers to ease short and long-term financial difficulties.
- A number of financial institutions said they specifically take mental capacity limitations and long-term conditions into consideration when determining appropriate approaches to collecting debt from vulnerable customers.
- One uses quality assurance by an independent governed team to monitor customers' outcomes.
- Typically, the specialist customer unit, operating within the collections department, identifies appropriate liaison with external organisations, including charities.
- All partner/liaise with charities on programmes to support customers in vulnerable circumstances. Some also receive training for their staff.
- All provide written communications giving information and highlighting where to get free independent advice from debt charities.

***Santander:** "When identified, we refer customers (in collections, or who need financial support) with mental capacity issues or longterm conditions (in addition to other vulnerable situations) to specialist support teams, where their case is managed. The team provides support by completing a budget planner, giving the customer options and solutions to consider (one solution might be to move to a basic account). They will consider all solutions to help the customer."*

***Barclays:** "Where the agent [working in collections] picks up there is vulnerability they will complete the TEXAS model and then immediately hand off to the vulnerable team. The process of identifying customers in our frontline collections is based around specific triggers that might indicate there is a customer in vulnerable circumstances. The vulnerable team will then case manage this customer's journey with us and has the ability to write off debt up to a limit or perform a medical write-off, or set up an appropriate repayment vehicle. This differentiates them from front line collections colleagues. Our approach to vulnerability is to consider the impact of long-term conditions and mental capacity issues on a customer and also their financial position. Where a vulnerable circumstance is a driver of financial difficulty or where, because of their circumstances, they may otherwise struggle, we will provide additional support. "*

***Barclays:** "Within our collections department, our vulnerable team is specially trained both internally and by the Samaritans to handle these cases. Front line staff have undergone bespoke vulnerability training to identify and empathise with customers in vulnerable circumstances. Where one of our customers is suicidal, or where we have agreed a write-off of debt, our current account collections team will share these details with colleagues in Barclaycard and also with our secured collections team."*

Staff training and awareness

- All financial institutions are raising staff awareness and improving culture to support customers in vulnerable circumstance. Treatment of customers in vulnerable circumstances modules is incorporated in their annual training programmes.

- All provide a variety of staff training and communication programmes, using various mediums to help staff assist customers in vulnerable circumstances. Typical content includes likely/possible vulnerable scenarios, or "moments", often supported by a scripted conversation framework. In addition, all provide referral, or access, to wider specialist support available in the financial institution.

- Some specifically cite using the experience of staff to inform the design and delivery of services to customers in vulnerable circumstances.

__Barclays:__ "Within our frontline environment, we deliver raised awareness and improve colleague understanding through a 'Community Driving Licence' (CDL) qualification tool. This equips colleagues to understand better and respond to customers in vulnerable circumstances. The embedding activities within the CDL encourage colleagues to do more in their communities and deepen their understanding, such as through joining Alzheimer's Society's Dementia Friends programme. Alongside this, colleagues have access to Toolbox, an online "gamified" platform, which helps guide colleagues and customers through interactions. We use a conversation framework to ensure discussion guided by customers in vulnerable circumstances and a number of "moments", such as paying for care."

__RBS:__ "We have an internal Dementia Hub: we use Life Event films to promote the awareness of such conditions; and a comprehensive training programme and material to help identify, understand and raise awareness of situations and adjustments that can be made. We actively promote Dementia Friendly Bank status within our brands using the Dementia Friendly Financial Services Charter and promote Dementia Friends initiatives, with many colleagues undertaking enhanced dementia training. We are also working with Macmillan Cancer Support to continue to ensure that we meet its nine-point recommendation charter for banks."

2.3 Conclusion

From the financial institutions surveyed, Fairbanking concludes that for information handling among customers in vulnerable circumstances, there is:

- not a clear picture of whether customer vulnerability is routinely identified;

- still some way to go to improve operational information handling processes and systems, e.g. around appropriate application of flags; and

- no consensus about operating standards for the sector.

Fairbanking notes the progress that financial institutions are making towards creating bespoke solutions, often involving planned technological improvements. There is a significant gap in that it is not clear what will be effective solutions for the customers concerned. At present, in our view, it is too difficult to develop and apply a standard for good practice for information handling. It will require a few more years of development, even from those that purport to be the best in the field.

Fintech should be an enabler not a barrier. Financial institutions, including challenger banks, should design processes for the most vulnerable customers, including taking into account third party access on behalf of those customers. Financial institutions often say that their back office and embedded or legacy systems are a key barrier to them being able to offer an appropriate service to vulnerable customers . Challenger banks have the opportunity to develop appropriate systems when setting up.

3. Dependency Arrangements

3.1 Introduction

The survey examined how financial institutions gauge the need for special arrangements for customers in vulnerable circumstances who are becoming dependent on others and the arrangements that are put in place. It considered how assurance is verified that representatives are in a position to manage the customer's money on their behalf, while maintaining as much continuing independence for the vulnerable customer as possible. It also examined how arrangements and safeguards typically apply for Power of Attorneys, Deputies and provision for emergency situations.

This is complex territory for financial institutions on the front line. Fairbanking's survey and wider stakeholder discussion identified a number of failings and service inadequacies.

> *With an ageing population, it is going to be more important for financial institutions to have a coherent approach to dependency arrangements going forward.*

While most financial institutions adopt safeguards and protocols to protect customers who become identified as needing dependency arrangements, there is no standard approach. Independent OPG documented cases (see Appendix 1) illustrate the difficulties caused to customers in vulnerable circumstances and the need for higher and more consistently applied service standards, staff awareness, training and support.

With an ageing population, it is going to be more important for financial institutions to have a coherent approach to dependency arrangements going forward. It makes business sense for financial institutions to adopt a coherent approach towards third parties who are able to assist customers in vulnerable circumstances to manage their affairs.

3.2 Current and best practice

Identifying dependency requirements

- There is good evidence of financial institutions identifying the need for dependency arrangements in individual cases. Sometimes, this process is assisted by the application of flags on customer's account records.
- However, there is little evidence that dependency needs are identified sufficiently early, or pro-actively anticipated, for example by monitoring the people likely to be affected.
- Some financial institutions do report they analyse transaction activity to alert them to an emerging need for dependency support.

Customer communication and awareness

- All financial institutions identify the need for dependency arrangements among customers in vulnerable circumstances primarily through their interactions with customers.
- There is little evidence of customers in vulnerable circumstances being effectively signposted or referred to get help quickly if they need to make arrangements for others to manage their accounts for them.

Dependency assessment

- All financial institutions have measures in place to identify the need for full dependency and processes that are triggered when required.
- All provide, or are addressing, arrangements to support the need for special or temporary emergency arrangements, anticipating where possible.
- By their nature, often emergency situations cannot be anticipated. When such circumstances arise, financial institutions will appraise how best to support the vulnerable customer on a case-by-

case basis, and there is encouraging evidence of responsive support.

Santander: *"The need for dependency support is done via colleagues in face-to-face interaction in branches and telephony. They are trained to identify cognitive decline, etc, plus encourage discussion on Attorney/Deputyship to support them. Staff are trained to handle enquiries with regards to Attorney/Deputyship Registrations. We are able to support their appointment. We have a Centre of Excellence that processes all registrations for Attorneys and Deputyships on accounts. We also have a dedicated helpline to answer questions.*

"We identify triggers that might signal the need for dependency arrangements. For instance, if card and PIN numbers were being ordered frequently, unusual activity on the account, informed by a third party (e.g. care home, etc.). All staff are trained as Dementia Friends and able to recognise cognitive decline."

Barclays: *"We can support customers needing to establish emergency temporary arrangements by organising home or hospital visits by branch colleagues. In some exceptional circumstances, written instructions to set up access can be accepted."*

Lloyds: *"We accept a letter of authority as a one-off agreement for emergency situations, which must be authorised by a senior manager. This type of transaction is only permitted in exceptional circumstances where the need is clearly established."*

Delegated controls/safeguards

- All financial institutions have established processes for dependency arrangements and will communicate with representatives about the specific safeguards in place for that customer.

- Typically, restrictions are imposed on third party authorities, including on internet or telephone banking, adding a party to an account, applying for lending facilities, accessing safe custody and change of name or address. This is to protect the vulnerable customer and the restrictions are extended to specific product features and facilities, e.g. representatives are not permitted to open a credit card, or be a secondary card holder to a credit account, nor generally become a joint account holder on the account.

- Some have incorporated bespoke facilities to assist in the establishment of dependency arrangements for customers in vulnerable circumstances.

Financial institutions do not operate a standard approach for representatives in relation to what they can do on a current account. As noted above, the OPG has highlighted how this can compound the difficulties that customers in vulnerable circumstances and their representatives experience in establishing dependency arrangements for current accounts.

Clydesdale: *"We apply safeguards sensitively and can tailor payment instruments provided to the customer if additional safeguards are needed. This can involve cancelling an existing chequebook, or replacing the debit card with one that will only transact online and allow a lower cash withdrawal amount, or one that only requires a signature other than a PIN if memory problems are experienced. In addition, where third party access is put in place, the order/mandate/power can have restrictions on access included. Access to telephone and Internet banking can also be restricted by allowing a nominated user rather than full access for certain orders."*

Santander: *"Accounts have an indicator set on them to indicate an Attorney or a Deputy has been appointed. If a Court of Protection has been registered, all donor access ceases, i.e. account access and cards are stopped."*

Specialist customer unit

- A specialist customer unit is typically used to support the establishment and operation of dependency arrangements for customers in vulnerable circumstances.

- The specialist customer support teams provide training and support, including provision for cross-referral, for staff establishing dependency arrangements.

- Specialist units often have responsibilities for advising and supporting staff assessing the need for dependency arrangements

Staff training and awareness

- Typically, training for staff on dependency arrangements is a modular part of the overall training programme. Independent OPG evidence points to the need for improved staff awareness, training and effective staff access to wider available internal support[6].

Although there is no standard approach, there is sufficient practice to be able to establish a set of criteria that could be tested.

- one institution operates a specific dedicated delegated access/Power of Attorney team that has responsibility for training for dependency arrangements over and above the training provided as part of the general staff training programme.

Financial abuse

- Some financial institutions are reporting suspected abuse by representatives to the OPG, and most are improving and now operating regular liaison with external authorities. There is increasingly appreciation of the benefits of OPG dialogue and advice.

6 OPG has produced e-learning for frontline banking staff to help them understand the customer journey and recognise valid examples of Lasting Powers of Attorney, Enduring Powers of Attorney and Court Orders.

- One carries out extensive investigation of suspicious activity.

> ***Santander***: *"Any financial abuse identified or suspected is raised internally to our SARs unit (Suspicious Activity Reporting) or our fraud department for investigation. Colleagues are alert to suspicious activity on the account or in relation to other transaction concerns."*

3.3 Conclusion

From the financial institutions surveyed, Fairbanking concludes that it would be possible to devise a framework for measurement of dependency arrangements established for customers in vulnerable circumstances. Although there is no standard approach, there is sufficient practice to be able to establish a set of criteria that could be tested.

The Fairbanking Foundation will consider further whether this should be pursued and will obtain the views of interested parties as to whether a certification in this area would be supported.

4. Treatment of fraud and scams

4.1 Introduction

This section of the survey examines how customers in vulnerable circumstances due to mental capacity limitations may identify themselves as being vulnerable to, or being the victim of, a fraud or scam. They require appropriate arrangements to be put in place that mitigate the risk of fraud and provide reassurance and extra support that might be needed.

It also examined how these customers might be identified as being particularly susceptible to scams and, therefore, needing extra checks and arrangements in place. As with fraud, when a scam occurs, a customer may need extra reassurance and support, especially since financial liability is normally placed on a customer.

- A fraud is where money is stolen from a customer's account without the knowledge or involvement of the customer (i.e. unauthorised transactions in the pure sense).

- A scam is a fraud perpetuated against the customer that involves luring the customer into authorising a transaction that they would not authorise if they knew it was a fraud.

Financial institutions do not seem to identify a need to provide an extra level of care for customers in vulnerable circumstances due to mental capacity limitations who are subject to frauds. This appears to be because the institutions assume liability for fraud. However, this ignores the additional distress that might be suffered by a vulnerable customer who is the victim of fraud. Vulnerable customers also may not realise that they have been a victim of fraud, or may discover this later than other customers.

From independent analysis, and recent FOS cases[7], we know that complaints about how financial institutions handle scams are being upheld on the basis that customers' concerns should have been picked up on and investigated earlier and resolved better. Also noted, is the detriment and poor service suffered, particularly among customers in vulnerable circumstances, because of inadequate staff empathy.

4.2 Current and best practice

From the financial institutions surveyed:

4.2.1 Fraud

Identification of fraud/operational intervention

- All financial institutions have arrangements in place to deal with fraud across their entire customer base. All operate a dedicated fraud contact centre/team or department.

> *when a scam occurs, a customer may need extra reassurance and support, especially since financial liability is normally placed on a customer*

- All treat cases of fraud on a case-by-case basis and do not adopt a different approach to assisting customers in vulnerable circumstances, or mitigate the risk of fraud for this group differently.

- All monitor customer activity and proactively discuss with a customer any abnormalities or irregularities on their account, which might be

7 Ombudsman news, fighting fraud Issue 135, August 2016. In particular pp 6-7 case study 135/3 where the victim Mrs N, correctly suspecting a telephone scam from someone masquerading as a broadband company, had not been given accurate information and sufficient advice from the financial institution, plus had not been treated with sufficient sympathy by the financial adviser. There had not been a proper investigation with the financial institution's fraud department, which also had not been properly briefed. In this instance, it would have revealed the scam. FOS found that much more should have been done on the first phone call, which would have been likely to reveal the fraud, and not confuse the customer, who was not sure if she had been scammed or not. (Subsequently, the financial institution fully compensated the customer).

fraud. This is part of the normal Know Your Customer (KYC) processes.

- Most do not specifically identify customer characteristics that may increase susceptibility to fraud, but they do look at behaviour on the account.

__Lloyds:__ "We offer tools to support customer independence, including: use of audio statements; braille statements; hearing loss interpreters; large print; service call; signature stamp; talking ATM; and text relay and sign video relay calls, to counter the risk, and identify an instance, of fraud."

__Lloyds:__ "We have a range of general customer base initiatives, including: internet banking anti-fraud messages; electronic authentication process; telephone banking IVR anti-fraud messages; and social engineering scripts are read when discussing unusual/high value payments. Enhancements to digital processes and the issue of anti-fraud leaflets are scheduled for next quarter implementation."

__Clydesdale:__ "Vulnerability procedures are in place within our fraud departments to ensure the customer receives the right support, dependent on their individual circumstances. This work will be ongoing to ensure relevant safeguards are made known to the customer (Power of Attorney, Third Party Mandates / Agent to Operate agreements) and all appropriate options are considered."

Specialist customer unit

- The specialist customer units and anti-fraud staff liaise and coordinate activities in all institutions, although organisational structures vary.

- Often the specialist customer unit provides specific support for customers in vulnerable circumstances who have been the victim of fraud.

Customer communication and awareness:

- All financial institutions run fraud awareness campaigns in branches and via social media and with telephone and website information services. Some proactively provide referral services to Cifas.

- One has run a successful TV campaign.

- Most do not pro-actively offer to restrict marketing communications for customers in vulnerable circumstances. However, they will restrict marketing, if requested by the customer. One institution does explore this in exceptional situations.

__Clydesdale:__ "We treat all customers as potentially vulnerable to fraud. As such, various initiatives and campaigns are being run to raise customer awareness. This includes messages via social media, secure messages to internet banking customers including warnings on log-in, inviting fraud experts to speak to customers in our branch network and telephone waiting messages, which provide the customer with information, while waiting to speak to an adviser. We also run a 'We Will Never' campaign, which tells customers what to expect when receiving a genuine communication from the bank, as well as providing information and leaflets from other members of Financial Fraud Action UK (FFA UK). In addition, our website has a Fraud Prevention and Security Centre section that provides detailed information and a UK-based freephone contact number for those who have been affected by fraud."

__Barclays:__ "We launched a TV advertising campaign around fraud and scams, looking to raise awareness of the risk of scams. Following the advert, we saw a 700% increase in traffic to our www.barclays.co.uk/fraudsmart page."

__Lloyds:__ "We can restrict marketing depending on the specific circumstances of the vulnerable customer and, where warranted, remove internet banking facilities to protect consumers from fraud."

Staff training and awareness

- All financial institutions have training in place for staff in relation to the risk of fraud on any customer. They provide in-depth and extensive training and raise awareness for staff on the avoidance, mitigation and remedies for fraud on customers. However, we did not find evidence of the training and awareness activities making distinctions between the risks for those customers in vulnerable circumstances and other customers.

Liaison with external organisations

- Most do not routinely report known or suspected fraud abuse by representatives/PoAs to the OPG; this is despite the OPG encouraging financial institutions to do so.

- All operate customer signposting processes to other agencies, especially Cifas.

- All are involved with other agencies and projects. These include Think Jessica, Get Safe online, Joint Declaration. Home Office Joint Fraud Task Force, Take 5 Campaign and Havering protocol run by local Trading Standards. All are members of FFA UK. All these organisations have developed or are piloting coordinated programmes to combat fraud and scams, which financial institutions support.

- Victim Support and Trading Standards is leading the Victims and Vulnerability work strand within the Joint Fraud Taskforce and addressing many of the issues highlighted in this report. Government and industry (via Cifas and trade associations) are engaged in this work and have signed the Home Office pledge.

- Every high-street bank is a member of Cifas and therefore is a partner in Cifas's Protecting the Vulnerable scheme. This links the financial services sector (and beyond) with efforts by local authorities to safeguard vulnerable people under their care and protection

> ***Lloyds:*** *"We are a sponsor of Think Jessica. We make use of external organisation literature to promote education and awareness to prevent fraud and participate in anti-fraud schemes, e.g. Havering protocol, run by local Trading Standards. We are actively working with FFA UK and the Met Police on the Banking protocol in the Greater London area and support the Joint Declaration. Home Office task force (Take 5).*

4.2.2 Scams

Identification of scams/operational intervention

- Most financial institutions treat scams on customers on a case-by-case basis and do not adopt a different approach to assisting customers in vulnerable circumstances, or for mitigating the risk of a scam in this group.

- The organisational structure for assisting with scams varies from one financial institution to another. Some deal with scams in the fraud department. Others rely on specialist customer support units to provide active support for identifying particular scams in circulation, where customers in vulnerable circumstances may be especially susceptible.

- One takes specialist counsel on vulnerability into consideration to ensure appropriate customer outcomes.

- One institution is able to interrupt payments in the event of a suspected scam. It can deploy scripts/messages at the point of the transaction and scam detection can interrupt a payment and delay sending it until it has been discussed and confirmed with the customer.

- All institutions say they will restrict marketing where this is requested by a customer.

- One proactivity discusses with the vulnerable customer the option of applying marketing restrictions, where it is thought there is greater susceptibility to the risk of being scammed.

> ***Santander:*** *"We will interrupt payments where suspicious activity is suspected on an account pending discussion with the customer."*

__RBS:__ "We provide additional support to customers in vulnerable circumstances if required."

Remedies for scams

- Most financial institutions apply the same level of liability whether or not there is customer vulnerability. With scams, financial liability is normally placed on a customer.

- Some financial institutions, however, will take a customer's vulnerability into account and offer additional support.

- One uses "best endeavours" to recover customers' money lost to scams and to provide strong support, plus in extreme circumstances if warranted, to make a referral to adult social services.

__Barclays:__ "We make 'best endeavours' to recover monies for customers lost to scams and provide strong support, plus in extreme circumstances if warranted, make a referral to adult social services."

__Santander:__ "We will take a customer's vulnerability into account in determining whether liability will be assumed and the customer compensated. "

__RBS:__ "All scam cases are individually reviewed to ensure an appropriate outcome for the customer. Questions we ask and processes reviewed are: Type of scam? Have we seen this before? What could we have done to prevent this? Could we have done more? What is the individual customer situation?"

Customer awareness and advice/support

- All financial institutions run scam awareness customer campaigns in branches and via social media, and with telephone and website information services.

- All have wider customer initiatives, not specific to those deemed vulnerable, that include anti-scam messages on internet banking, telephone banking IVR anti-scam messages, and use of "social engineering" scripts for unusual or high transaction value payments.

__Age UK research__ (independent to Fairbanking Survey): Age Friendly Banking[8], cites the case of Mr Johnson a customer of Coventry Building Society, where the advice given by the Financial Crime Team on a particular type of scam in circulation, provided detailed information as to what the scammers might say to convince him that they were genuine callers, what they might ask him to do, plus would happen once he had done this. They advised him to reflect further. This prompted Mr Johnson to call back on a phone number – he was advised to search for on the institution's internet – he realised he had been duped by fraudsters and the scam was prevented.

__Lloyds:__ "Scammed customers may be referred to Lloyds Disability Services Support Team, where specific advice is given. Scam case details involving duped customers are referred to a dedicated panel of subject matter experts to determine actions. The level of customer vulnerability is a key factor of consideration. Options may include enhanced training and awareness of customer vulnerability, amendments to transaction thresholds, additional account monitoring and referral to Victim Support.

__Lloyds:__ "Education and awareness is a key factor in the approach to preventing customers from being the victims of scams. This is provided through the online channels in the form of advice and guidance, via automated scripting on IVR systems and through colleague to customer interaction through our community banking branches and our telephone banking services. To support this, our automated transaction monitoring tools attempt to identify cases that are more likely to be social engineering, at which points efforts are made to warn the customer and identify

8 Age UK: *Age Friendly Banking, What it is and how you do it,* April 2016

such cases, securing their accounts before funds are released."

Specialist customer unit

- Most financial institutions involve, as for fraud, the specialist customer unit and scam operation in remedies for scams. This is provided for all customers.

Staff training and awareness

- All financial institutions provide staff training on the risk of scams generally, plus training and communication scripts and pointers on the dangers and likelihood of customers in vulnerable circumstances being specifically susceptible and targeted.

- As noted above (see footnote 7), FOS provides independent evidence suggesting that financial institutions still have further to go in regard to having appropriate knowledge, skill and empathy for a customer in vulnerable circumstances who may have been scammed, and in improving the outcome for such customers. The detriment caused is particularly marked for customers in vulnerable circumstances, who will be much more susceptible to scams and are often less able to identify, or articulate, any concerns as early as other customers.

Liaison with external organisations

- All financial institutions are involved with other agencies and projects. These include Think Jessica, Get Safe online, Joint Declaration. Home Office task force (Take 5) and Havering protocol run by local Trading Standards. All are members of FFA UK. All these organisations have developed or are piloting coordinated programmes to combat fraud and scams, which financial institutions support.

Monitoring of scam activity

- Several financial institutions are conducting specific scrutiny of worrying activity on customer accounts. Two are currently looking at high volumes of cheque writing, indicating a group of customers who have fallen victim to mass marketing scams.

  Clydesdale: *"We are conducting investigations of, and monitoring, high volumes of cheque writing, which is suggestive of a mass scam currently in circulation."*

4.3 Conclusion

From the financial institutions surveyed, Fairbanking has identified activities suitable for measurement in relation to fraud on customers in vulnerable circumstances, but does not observe much sign of emerging good practice, or understanding of the extra importance of grappling with fraud on these customers. Therefore, at this stage, Fairbanking does not propose to attempt to introduce a certification for this area of activity.

> *Fairbanking does not observe much sign of emerging good practice, or understanding of the extra importance of grappling with fraud on these customers.*

In relation to scams, due to a lack of evidence of consistent good practice, or sufficiently widespread focus on the particular risks for customers in vulnerable circumstances, Fairbanking concludes that it cannot progress to comprehensive standards.

Scams are an area that causes significant suffering and financial loss. Financial institutions appear to have a commitment to invest here and existing initiatives, such as around payment interruption, are commendable. If further improvements can be achieved over the next few years, Fairbanking could look to incorporate the treatment of scams into a new standard.

Appendix 1: Office of the Public Guardian: evidence on dependency arrangements

In 2013, OPG co-authored the third party authorisation framework, along with others, including the BBA, BSA, SFE and the Law Society. This provided guidelines for customers and branch staff for third party account management. Although banks are not obliged to offer services, many have since taken positive steps to improve customer service. The picture remains inconsistent. The OPG team continues to assess strategic steps it can take to improve customer experience, working across all financial areas and increasing the level of engagement with financial institutions.

The industry, regulator and law enforcement agencies should work together to find additional identification options for vulnerable people

OPG statistical data:
As of 31 October, 2016, there were 2,223,777 instruments on the register. These are broken down as:

- LPA (property and finance): 1,448,704
- LPA (Health and Welfare): 631,664
- Total LPA: 2,080,368.
- EPA: 143,403.

Receipts of all types of Powers of Attorney are averaging roughly 50,000 per month, of which just over 1,000 are EPA, with the remainder comprising LPA (H&W and P&F), with approximately 30,000 per month being P&F. OPG currently supervises 57,000 Deputyship orders.

Post-Registration Behaviour and Satisfaction Survey Quantitative Report 2016

For the past couple of years, the OPG has commissioned research into behaviour and satisfaction of customers using their registered Powers of Attorney and/or Deputyships. An annual survey has now been created. These examples are taken from recent surveys.

Survey findings
54% of OPG's customers have more than one type of power in place and, out of those, 80% are satisfied when using LPAs, EPAs and Deputyships, although this had in fact dropped by 2% since the previous year.

A common obstacle perceived by attorneys and deputies is with banks performing security measures, including requests for various forms of ID and sometimes asking to see donors and clients in person.

Financial institutions across the board use the full range of acceptable evidence for ID verification, including having an exception process in place for customers who do not possess "standard" identification documents. The industry, regulator and law enforcement agencies should work together to find additional identification options for vulnerable people.[9]

What does this mean?
The OPG welcomes the work that financial institutions are doing to safeguard their customers with ID checks.

It also observes that the customer satisfaction rate is as high as 80%.

Its findings suggest that staff in financial institutions know about LPAs, but less so about Deputyships and EPAs.

9 This is taken from principle 8 on industry alignment in the BBA report "Improving outcomes for customers in vulnerable circumstances". See Bibliography.

Data sources: Financial sector key themes – (Source: OPG data, 2016)

Practicalities of lodging a deed

Typical problems occur with the lack of standardisation of registration formats, lost paperwork in banks, and banks insisting unnecessarily on the original deed (when an office copy or certified copy is produced). Banks expect the donor to travel to the branch with the attorney, so they can be identified. This can happen even when the donor has lost capacity.

Recent cases:

- A client was advised by a bank that he could not open a bank account as there was a Deputyship in place. The client felt this impacted on his independence.

> *Banks expect the donor to travel to the branch with the attorney, so they can be identified. This can happen even when the donor has lost capacity*

- Catalogue of errors/poor service. A joint deputy reported that she has had a "shocking, dreadful, stressful" time with a bank. She was treated badly, with no customer care. It took the bank six weeks to set up a Deputyship account and it advised her that she could only set the account up without the other deputies, despite the court order stating "joint and several" deputies. The bank advised that if the deputy wanted internet access or telephone banking for the client, the other deputies could not register. The bank kept sending information re internet and telephone banking to the wrong place. It then closed the account down, stating fraud.

- A bank refused to accept the registered LPA to manage online accounts unless proof of the donor's mental capacity was provided (donor lacks capacity). The LPA had been activated for other accounts. The head office has also reiterated this information.

- A bank refused to accept the Court of Protection (COP) order as the stamp was in black ink instead of blue ink. They also advised that the COP date should be stamped on each page.

- A bank was not accepting an interim order from the deputy allowing her to access the client's funds.

- A bank refused to accept the EPA as it contained a clause stating that the donor must give written authority for the attorneys to act when donor has capacity. The caller had such a letter, but the bank stated that donor had to attend in person. The donor had suffered a stroke and was physically disabled.

Awareness of arrangements for deputies/attorneys

Typically, bank staff are not aware of the MCA or the roles of deputies and attorneys, do not recognise a legal deed, or understand the types of Power of Attorney. Banks also insist on an LPA when an EPA is presented and will suffice. Banks often refuse or restrict attorney access to internet and telephone banking, cashpoint cards and cheque books.

Recent cases:

- A deputy requested copies of statements on a client's account. After being kept on hold for over an hour and providing the same details repeatedly to various call agents, she was advised that she could not have them.

- An attorney registered the LPA with the bank, which accepted the authority given to the named attorneys for the majority of the accounts held by the donor. The bank had, however, excluded a Premier Investment Management Service account and advised that it needs an extension of the powers to permit operation of this investment by the attorneys.

- A deputy had an existing account with the bank in her own name as appointee. She then opened a Deputyship account but the bank refused to transfer over the funds from the appointee account to the Deputyship account because the deputy had no form of ID that it would accept. (She did not drive and had an out of date passport). The bank then transferred some of the money from the appointee account to the Deputyship account, but not the full amount. Some months later, it transferred the balance to the deputy's husband's own personal account for some unknown reason, which was then transferred to the Deputyship account. It took around six months for all funds to be transferred to the Deputyship account.

Appendix 2: Fairbanking Ratings 2016 – Current Account with Overdraft Questionnaire Part 2 Customers in vulnerable circumstances

The following questions were the key areas relating to customer vulnerability that Fairbanking surveyed amongst the financial institutions that participated.

Section 1: Customers in vulnerable circumstances due to a mental capacity limitation, or a long-term condition[9], or their representatives may pass information to do with the vulnerability to a financial institution with the intention that this would lead to appropriate treatment.

This section is about how banks/financial institutions gather and use this information about customers in vulnerable circumstances in relation to current accounts. In the context of this questionnaire, customers in vulnerable circumstances are defined as only those with a mental capacity limitation or a long-term condition.

Questions on using and handling information

1.1.1 When identified, how are customers in vulnerable circumstances using this product serviced differently?

1.2 Have indicators of customers in vulnerable circumstances been identified for this product?

1.3 Does the product/service enable a customer to self-identify a vulnerability?

Questions on protocols/procedures, training and outcomes

1.4.1 What training is given to staff to support the processes described above?

1.5.1 How does this unit provide support in relation to information collection/handling for customers in vulnerable circumstances?

1.5.2 Have outcomes been identified that should be achieved with the information gathered about a customer in vulnerable circumstances?

Questions on information collection/gathering

1.6 Through what channels is such information collected: SMS, Email, Post, Internet, Telephone, Video calls, In branch, Advocate?

1.7 Do you check with the customer in vulnerable circumstances, or their carer/representative or a 'notified trusted other', that the information collected is accurate, its use has been explained and that the customer is willing for it to be shared across the financial institution?

1.7.1 How does the product/service ensure that the information collected on the customer in vulnerable circumstances remains up to date?

1.8 Are there specific challenges for customers in vulnerable circumstances, in identifying and recording information (e.g. IT system

9 Mental Capacity is a person's ability to make an informed decision at a specific point in time. It is determined by a person's ability to: understand information; remember information; weigh-up information; make/communicate an informed decision. Consequently, mental incapacity or a mental capacity limitation is a person's inability to make an informed decision at a specific point in time due to an 'impairment or disturbance in the functioning of the mind or brain'. This can, for example, include: some forms of mental illness; dementia; significant learning disabilities; the long-term effects of brain damage; physical or medical conditions which cause confusion, drowsiness, loss of consciousness; delirium; concussion following a head injury; the symptoms of alcohol or drug use. Law and regulatory guidance expect lenders to presume that all borrowers have the mental capacity to make an informed decision about a loan (to prevent discrimination against people with certain conditions), unless the lender also knows or reasonably suspects that a mental capacity limitation exists.

A long-term condition (LTC) is a physical or mental illness that usually lasts a year or longer, and which may require ongoing care, support, and treatment. Examples of LTCs can include physical conditions such as cancer, heart disease, diabetes, chronic obstructive pulmonary disease (COPD), musculoskeletal disorders and complications following a stroke. LTCs also include mental illnesses such as anxiety, depression, dementia, schizophrenia and bipolar disorder. Some people have more than one LTC at the same time. A large number of people with a physical health problem, for example, will experience mental illnesses such as anxiety or depression at the same time. Around half of all people with cancer experience levels of anxiety and depression severe enough to adversely affect their quality of life constraints, technical language/terminology, data privacy legislation, etc.)?

Questions on consumer awareness of support for vulnerability

1.9 Does the product/service include features to raise awareness among potentially customers in vulnerable circumstances that it can provide additional service support if required? How (i.e., by what channel?) is the communication with the customer delivered.

Questions on data/information handling

1.10 How is the information collected for the product/ service used for the benefit of the customer in vulnerable circumstances? E.g. to help ameliorate financial difficulty/distress.

Questions on customer service and effectiveness

1.11 Is evidence collected in relation to the effectiveness of the features described above in providing help to customers in vulnerable circumstances? (i.e. in producing good outcomes)

1.11.1 How is evidence obtained? E.g. investigation/ programmes, customer/carer surveys, transaction analysis. What information does the product/service collect to verify its effectiveness?

Questions on third party liaison/arrangements

1.12 Does the product/service provide support in identifying and signposting external organisations (e.g. council support services) that might offer further support to a customer in vulnerable circumstances?

Section 2: Questions on Dependency

Customers in vulnerable circumstances due to a mental capacity limitation or a long-term condition, who are becoming or have become dependent on others, need to be assured that representatives, or 'notified trusted others' are in a position to manage their money, while maintaining as much independence as possible for the customer. The following questions apply to these representatives, including any appointed Deputies and Attorneys.

Questions on identifying dependency requirements and protocols

2.1 Does the product/service encourage customers, or groups of customers, to consider putting in place arrangements to protect or assist them in the future? E.g. Power of Attorney (PoA) or 'notified trusted other' in anticipation of cognitive decline or unexpected vulnerability.

2.2 Does the product/service identify that a customer is becoming dependent or requiring the support of another (carer/representative)?

2.2.1 What are the triggers/signals that identify this need, e.g. customer behaviour, operation of the current account, etc?

2.3 Does the product/service identify where there is a need for full dependency arrangements to be put in place?

2.5 Does the product/service apply particular processes in establishing dependency arrangements with representatives/representatives, or a 'notified trusted other'?

Questions on delegated controls/authority

2.6 Does the product/service determine and apply safeguards to the account of a customer in vulnerable circumstances needing dependency arrangements? (For example, delegated access controls/transaction limits and notifications that customers understand)

2.7 Does the product/service have processes in place to identify when a carer/representative or a 'trusted notified other' acting for the customer may be abusing that arrangement?

2.8 Does the product/service have arrangements to refer/report any suspicious activities of deputies or PoA to the Office of the Public Guardian (OPG)?

Questions on operational arrangements

2.9 Does the product/service have processes to establish emergency and temporary arrangements when a customer finds themselves suddenly in vulnerable circumstances (e.g. in hospital, cannot physically travel into the branch etc)?

Questions on monitoring

2.10 Does the product/service monitor the effectiveness of arrangements established with representatives/ representatives or a 'trusted notified other'?

2.11 Do you know what proportion or the number of customers for this product/service who would benefit from an arrangement to support representatives/representatives or a 'trusted notified other'?

Section 3: Questions on Fraud

Customers in vulnerable circumstances due to a mental capacity limitation or a long-term condition, or their representatives/relatives, may be vulnerable to fraud and need additional/appropriate arrangements put in place that provide reassurance and extra protection.

Questions on awareness of fraud

3.1 Does the product/service make a customer in vulnerable circumstances aware of actions they could take to reduce their risk of fraud?

3.1.1 What processes does the product/service put in place or recommend to the customer in vulnerable circumstances?

3.1.2 What does the product/service do to increase awareness of the risk of fraud among customers in vulnerable circumstances?

3.1.3 Does the product/service raise awareness and provide training to staff on the risk of fraud on customers in vulnerable circumstances?

Questions on remedies for, and to limit, financial loss from fraud

3.2 How does the product/service assist a customer in vulnerable circumstances when fraud occurs?

3.3 Does the product/service have a customer service unit providing specialist support to assist customers in vulnerable circumstances at risk of being a victim of fraud? What special arrangements does it put in place?

3.4 Does the product/service enable customers in vulnerable circumstances to establish special communication arrangements, such as restricted marketing to reduce the risk of fraud?

3.5 Are there circumstances under which you would suggest to a customer in vulnerable circumstances at risk of fraud, that they consider making additional arrangements for voluntary restrictive protection e.g. Cifas Protective Verification? (In this Cifas members are required to make additional verification checks to ascertain that applications genuine.)

3.6 Are there special arrangements with external organisations to reduce the risk of fraud on customers in vulnerable circumstances?

Section 4 Questions on Scams

Customers in vulnerable circumstances due to a mental capacity limitation or a long-term condition, or their representatives, relatives, or 'trusted notified other' may be vulnerable to scams and need additional arrangements put in place that reduce this risk and mitigate loss.

Questions on awareness of scams

4.1 Does the product/service make a customer in vulnerable circumstances aware of actions they could take to reduce their risk to scams?

4.1.1 What processes does the product/service follow or recommend to a customer in vulnerable circumstances to reduce the risk of being scammed?

4.1.2 What does the product/service do to increase awareness of the risk of scams among customers in vulnerable circumstances?

4.2 Does the product/service raise awareness with and provide training to staff on the risk of scams on customers in vulnerable circumstances?

4.3 Does the product contain features to alert customers in vulnerable circumstances to scams (e.g. multiple cheque writing)?

Questions on remedies for, and to limit, financial loss arising from scams

4.4 Does the product/service assist a customer in vulnerable circumstances when a scam occurs?

4.5 Does the product/service proactively identify the risk, and implement procedures to intercept, prevent, or at least reduce the likelihood, of a scam succeeding on a customer in vulnerable circumstances? How does it do this?

4.6 Does the product/service assume liability for customers in vulnerable circumstances who have been scammed, even where the customer is deemed to have caused, or contributed to the breach?

4.7 Does the product/service fully compensate the financial loss arising from a scam for a customer in vulnerable circumstances?

4.8 Does the product/service have a customer service unit providing specialist support to assist customers in vulnerable circumstances at risk of, or a victim of scams? What does it do?

4.9 Does the product/service enable customers in vulnerable circumstances to establish special communication arrangements, such as restricted marketing to reduce the risk of scams through the telephone channel?

4.10 Are there special arrangements with external organisations, including authorities to reduce the risk of scams on customers in vulnerable circumstances?

Section 5 Additional Information

Please note that any additional information provided in this section may contribute towards a higher rating for the customer vulnerability (due to a mental capacity limitation, or long-term condition) certification.

5.1 Does your treatment of customers in vulnerable circumstances have any additional features that could qualify as Fairbanking features that improve the experience and financial well-being of such customers?

5.2 Do you have any research or evidence to substantiate the benefit to your customers who may be in vulnerable circumstances of any of your product features (e.g. academic, customer feedback, behaviour change measures)?

5.3 Do you have any plans to improve the product in this context for customers in vulnerable circumstances over the next 2 years? (These could be at high level although they should be specific).

Glossary

BBA
British Bankers Association

BSA
Building Society Association

CIFAS
Credit Industry Fraud Association System, a UK-based fraud prevention service

CMA
Competition and Markets Authority

CONC
FCA Consumer Credit (CONC) Sourcebook of rules and guidance.

DPA
Data Protection Authority

Deputy
To act for someone if they 'lack mental capacity' and authorised by the Court of Protection to make decisions on their behalf.

Mental Capacity
Mental Capacity is a person's ability to make an informed decision at a specific point in time. It is determined by a person's ability to: understand information; remember information; weigh-up information; make/communicate an informed decision. Consequently, mental incapacity or a mental capacity limitation is a person's inability to make an informed decision at a specific point in time due to an 'impairment or disturbance in the functioning of the mind or brain'. This can, for example, include: some forms of mental illness; dementia; significant learning disabilities; the long-term effects of brain damage; physical or medical conditions which cause confusion, drowsiness, loss of consciousness; delirium; concussion following a head injury; the symptoms of alcohol or drug use. Law and regulatory guidance expect lenders to presume that all borrowers have the mental capacity to make an informed decision about a loan (to prevent discrimination against people with certain conditions), unless the lender also knows or reasonably suspects that a mental capacity limitation exists.

A long-term condition (LTC) is a physical or mental illness that usually lasts a year or longer, and which may require ongoing care, support, and treatment. Examples of LTCs can include physical conditions such as cancer, heart disease, diabetes, chronic obstructive pulmonary disease (COPD), musculoskeletal disorders and complications following a stroke. LTCs also include mental illnesses such as anxiety, depression, dementia, schizophrenia and bipolar disorder. Some people have more than one LTC at the same time. A large number of people with a physical health problem, for example, will experience mental illnesses such as anxiety or depression at the same time. Around half of all people with cancer experience levels of anxiety and depression severe enough to adversely affect their quality of life

EPA
Enduring Power of Attorney. This has been replaced by Lasting Power of Attorney, but EPA agreements signed before 1 October 2007 are still valid.

FCA
Financial Conduct Authority

FFA UK
Financial Fraud Action UK

IDEA
Impact, Duration, Experience, Assistance (customer protocol)

IVR
Interactive Voice Response

KYC
Know Your Customer compliance protocol

LPA
Lasting Power of Attorney

Long-Term Condition (LTC)
A physical or mental illness that usually lasts a year or longer, and which may require ongoing care, support, and treatment. Examples of LTCs can include physical conditions such as cancer, heart disease, diabetes, chronic obstructive pulmonary disease (COPD), musculoskeletal disorders and complications following a stroke. LTCs also include

mental illnesses such as anxiety, depression, dementia, schizophrenia and bipolar disorder. Some people have more than one LTC at the same time. A large number of people with a physical health problem, for example, will experience mental illnesses such as anxiety or depression at the same time. Around half of all people with cancer experience levels of anxiety and depression severe enough to adversely affect their quality of life.

OPG
Office of the Public Guardian

TEXAS
Thank, Explain, Explicit Consent, Ask, Signpost (customer protocol)

Think Jessica
A charity whose remit is to protect elderly and vulnerable people from scams which come through the postal system and criminals who contact them by telephone.

Bibliography

Age UK: *Policy Position Paper, Consumer Vulnerability* April 2016

Age UK: *Age Friendly Banking, What it is and how you do it* April 2016

Alzheimer's Society: *Dementia-Friendly financial services: A charter for improving the customer experience of people living with dementia when dealing with financial services organisations* 2013

BBA: *Improving outcomes for customers in vulnerable circumstances* February 2016

Guidance for people wanting to manage a bank account for someone else. BBA/BSA/OPG. December 2015

BBA/BSA/Alzheimer's Society: *A framework for authorising people wanting to operate a bank account for someone else* February 2013

The Fairbanking Foundation: Fairbanking Ratings: *Reaching for the Stars* November 2013

FCA: *Occasional Paper no 8, Consumer Vulnerability* February 2015

ICO *Guide to data protection*

Office of the Public Guardian: *Financial Sector Key Themes* (see Appendix 1)

FOS: *ombudsman news, fighting fraud*. Issue 135 August 2016

Macmillan: *Counting on your support: How the banking industry can improve the service it provides to customers living with cancer* May 2014

Payments Council: *Pay my Way Managing Payments, Safe ways to allow others to pay on your behalf* 2013

Royal College of Psychiatrists/Money Advice Trust: *Lending, debt collection and mental health: 12 steps for treating potentially customers in vulnerable circumstances fairly* November 2014

The Fairbanking Foundation
20–22 Wenlock Road,
London N1 7GU
Phone: 020 7617 7957
info@fairbanking.org.uk
www.fairbanking.org.uk