MONEY AND MENTAL HEALTH
POLICY INSTITUTE

DATA PROTECTING

Using financial data to support customers

Katie Alpin and Merlyn Holkar

Contents

Publication

The Money and Mental Health Policy Institute, October 2019

22 Kingsway, London, WC2B 6LE

Acknowledgements

The Money and Mental Health Team would like to express our gratitude and admiration to members of our Research Community who gave up their time and shared their experiences.

Thank you also to all the financial services firms who took part in workshops and interviews to support this project.

Special thanks to Barclays for supporting this work, and in particular to Chris Quince, Hannah Cane and Matt Robinson for their thoughtful input.

We also wish to express our thanks to colleagues at the FCA including Gordon Chapple, Henrike Mueller, Rebecca Alexander and, most of all, Shelley Cross.

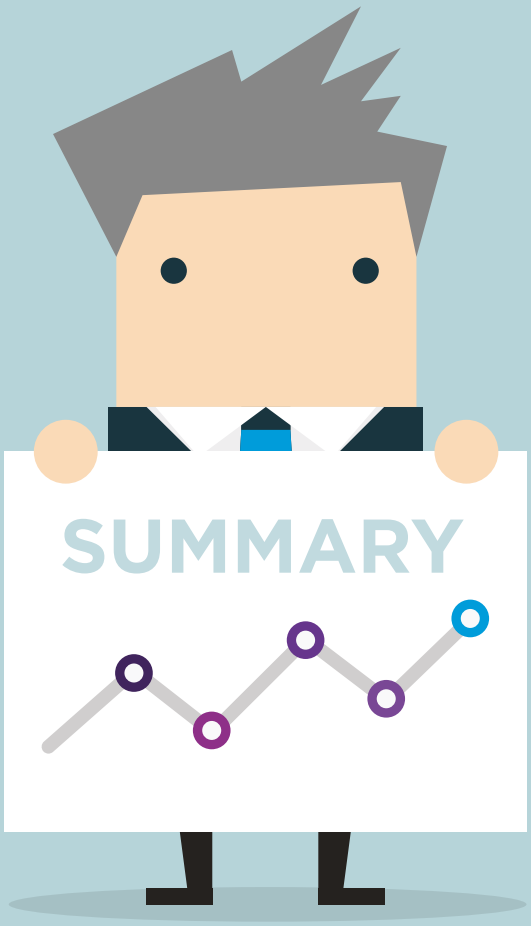
Thanks to the rest of the team at Money and Mental Health, in particular to Helen Undy and Brian Semple for editorial support, and Tasneem Clarke for support with data analysis.

About the authors

Katie Alpin is Head of Research and Policy at Money and Mental Health. She previously worked as an economist and holds degrees from the University of Oxford and the London School of Economics.

Merlyn Holkar is a Senior Research Officer at Money and Mental Health. Merlyn holds a BA in Philosophy, Politics and Economics from the University of Warwick. Before joining Money and Mental Health, Merlyn worked in the Policy and Campaigns department at Contact a Family.

Kindly sponsored by Barclays. This report represents the research and views solely of the authors and of the Money and Mental Health Policy Institute and does not represent the views or experiences of Barclays.


SUMMARY

Executive summary

Banks and building societies may be able to spot indications of vulnerability, such as a reduction in income, changes in spending behaviour or missed bill payments, in data generated when we use financial services.

Timely support from financial services providers, offered in the right way, could help people get the support they need, improving both financial wellbeing and mental health.

The case for using data

- Half of adults (50%) think their bank or building society should use their financial data to identify problems and offer support, with just one in ten (12%) disagreeing.
- A majority think it would be useful for financial service providers to help spot financial problems as they develop (68%), offer proactive support when things go wrong (66%), and help with day to day financial management (61%).
- People with mental health problems are particularly enthusiastic about the prospect of proactive support with their finances. Not only are they more likely to experience financial difficulty, but symptoms of mental health problems can make it harder to spot issues and to ask for help.

Consumer concerns

- Half of people (51%) agree that the benefits of their bank or building society looking through their financial data to try and spot problems outweigh the risks, while only one in ten (11%) disagree.
- Public concerns fall into three broad categories:
  - **Privacy concerns** Half of people (52%) are worried about the privacy implications of their bank or building society analysing their financial data for signs of potential difficulties
  - **Practical concerns** Nearly half of people (44%) worry that their bank or building society would treat them differently if they carried out this kind of analysis, for example denying them access to credit or undermining their financial autonomy
  - **Emotional concerns** One in three (30%) people think that their bank or building society telling them about a financial problem would make them feel worse about it. Participants with mental health problems felt receiving these messages could cause anxiety and shame, which could worsen their mental health.
- These risks must be weighed against the risks of not using financial data to identify vulnerability, including missing the opportunity to offer timely support and reduce financial and psychological distress.

Firm concerns

- Firms are unclear about how data protection rules apply in the context of analysing financial data to offer proactive support.
- Many providers only have a fragmented view of customers' finances, limiting their ability to identify potential issues.
- Well-meaning offers of support could be received badly by customers.
- Where customers don't respond to interventions, or where customers identified as potentially vulnerable go on to apply for credit or other products, firms may face additional liability and regulatory risks.

Best practice for designing interventions

- To protect privacy, firms should provide customers with choice and control over whether and how their data is analysed to identify potential vulnerability. This should include the option to opt out, and allowing customers to choose what types of potential vulnerability they are comfortable with their bank or building society looking for.
- When designing and delivering interventions as a result of something spotted in data, firms should:
  - » Be mindful that different issues require different interventions, and consider letting customers choose what should happen in specific scenarios
  - » Allow people to choose which communication channels are used to send them messages
  - » Ensure the tone of messages is friendly and the content is focused on offering support
  - » Consider the benefits of account aggregation to overcome data limitations
  - » Be open with consumers about the possibility of inaccurate results.
- Testing and co-producing interventions with customers would help firms to develop interventions that reach a balance between being effective and unintrusive.

Policy Recommendations

While best practice can help firms resolve some questions about using financial data to identify and respond to indications of customer vulnerability, some broader questions require input from policymakers and regulators.

- The Financial Conduct Authority (FCA) and Information Commissioner's Office (ICO) should:
  - Issue joint guidance to help financial service providers understand how regulatory principles could apply in the specific case of using financial data to identify customers who are struggling and offer proactive support
  - Seek out and support providers who want to test using financial data to proactively support customers.
- The government should:
  - Ensure the ICO has sufficient funding to enable them to engage with firms and other regulators as issues emerge
  - Create a repository or 'data trust' of anonymised financial data to allow researchers to identify more patterns which could indicate potential vulnerability.
- The FCA should:
  - Provide further guidance to firms or create a space to share best practice around the difficult ethical issues which could be raised when data is used both to identify possible vulnerability and assess credit-worthiness.

Introduction

Each year in England alone, 100,000 people attempt suicide while in problem debt.[1] Many people in problem debt report feeling isolated and trapped.

But there is always someone who knows about the debt, and who could reach out to offer support: the creditor.

Many other signs of distress might also be visible in the data generated when we use financial services. Banks and building societies may be able to see when redundancy or illness reduce income, or when a change in circumstances suddenly increases spending. As we use cards more and cash less, and the amount of information available to banks and building societies grows, do firms have an ethical obligation to step in and offer support if they can see issues arising?

This question is particularly pressing for many people living with mental health problems. Often people experiencing mental health problems find that their income falls due to time off work or the need to reduce hours, at exactly the same time that costs increase as people can't face public transport or have to pay for prescriptions. Mental health problems can also make keeping track of spending, sticking to a budget or remembering bills much harder, through symptoms like increased impulsivity, worsened memory, reduced energy and motivation, and poorer planning and problem-solving.[2] As a result of these challenges, people with mental health problems are three and a half times more likely to be in problem debt.[3]

Financial difficulties can cause serious shame and embarrassment. Sadly, these feelings can make it harder to find help. People with mental health problems can find it even more difficult to seek support. More than half (54%) of people who have experienced a mental health problem struggle to use the telephone and four in ten exhibit significant levels of anxiety when dealing with essential services providers, like sweating, a racing heart or difficulties breathing.[4]

Although reaching out for help can be incredibly difficult, financial problems can usually be resolved. Too often, however, people don't find the support available. Nobody tells you when you become eligible for benefits. Money management tools are hidden in bank apps, where only the most engaged customers find them. Signposting to debt advice languishes unread at the end of threatening letters.

Timely support from financial services providers, offered in the right way, could make all the difference in getting people the help and support they need. However it also brings risks, particularly to our privacy. To find a way forwards, we must balance these risks against that of missing the opportunity to improve the nation's financial wellbeing and mental health.

This report

This report examines how financial services providers could offer customers timely support based on signs of potential vulnerability identified in financial data. Figure 1 offers some examples of what this might mean in practice.

1. Bond N and Holkar M. Silent Killer. Money and Mental Health Policy Institute. 2018.
2. Holkar M. Seeing through the fog. Money and Mental Health Policy Institute. 2017.
3. Holkar M. Mental health and debt: A statistical update. Money and Mental Health Policy Institute. 2019.
4. Holkar M, Evans K and Langston K. Access essentials. Money and Mental Health Policy Institute. 2018.

Figure 1: Examples of ways that financial data might be used to identify and offer support to customers

Example 1

If a bank sees evidence that a customer's income has fallen, they could offer budgeting advice or signpost to information about benefits. Many people are unaware that they may be eligible for welfare benefits, and feelings of shame can make it very difficult to reach out for help.

Example 2

Persistent use of an unauthorised overdraft may indicate that a customer is in financial difficulties. Their bank could offer an appointment for a chat in branch or signposting to debt advice. With many people in problem debt waiting upwards of 12 months to seek advice,[5] this could help people get help sooner and drastically reduce anxiety and stress.

Example 3

Some mental health conditions can make it harder to keep track of spending, and people can end up in financial difficulties as a result. A simple message from the bank alerting a customer when they are spending more than usual for them, with information about budgeting tools, could help the person notice a change in their behaviour and take steps to avoid more serious problems.

We are not suggesting that financial services firms should attempt to identify or diagnose mental health problems. While mental health problems may make financial difficulties more likely, and can make it harder to ask for help, banks and building societies should focus on identifying financial behaviour or circumstances which could indicate potential vulnerability. By identifying possible signs of vulnerability and offering help or signposting to support, banks and building societies can help resolve financial problems, which is likely to improve mental health, without needing any specific mental health expertise or to ask questions about customers' health.

5. StepChange Debt Charity. Statistics Yearbook: Personal Debt. StepChange Debt Charity. 2013.

This work comes alongside public conversations about how data can be used for good, and the safeguards that should be put in place to protect privacy and avoid discrimination. 2018 saw the establishment of the Centre for Data Ethics and Innovation (CDEI). The Centre's first two projects, around online targeting and bias in algorithmic decision-making, could both have implications for the types of analysis discussed in this report. The government also continues to explore how data portability could boost competition and improve service across essential services markets like energy and telecoms.[6] Separately, the government has set up the Office for Artificial Intelligence, responsible for overseeing a grand challenge encouraging industry, charities and academia to work together using data, AI and innovation to transform the prevention, early diagnosis and treatment of chronic diseases by 2030. There is a significant tension between the promise of this programme and concerns over high-profile data leaks, including from credit referencing firm Equifax in 2018, and the ethical use of data, for example, in the Royal Free Hospital's deal with Google's DeepMind.[7]

In financial services, questions about whether and how firms should use data to identify customers who are potentially vulnerable have been pushed up the agenda by the Financial Conduct Authority's draft guidance on the fair treatment of vulnerable customers. The guidance encourages firms to take a proactive approach to understanding the nature and scale of vulnerability among their customer base.[8] With half of UK adults experiencing at least one type of potential vulnerability (a health problem, recent life event, low financial resilience or low financial capability),[9] this is a sizeable challenge and a significant departure from approaches based on offering customers extra support when they disclose a vulnerability. The guidance suggests that using financial data to identify signs of financial stress and offering targeted help could be good practice.

For Money and Mental Health, this work follows a TechSprint (hackathon) we held in partnership with the FCA in 2017, which aimed to develop new tech tools to help people living with mental health problems to avoid financial difficulties. Many of the brilliant suggestions built on the idea of using data to identify potential problems and offer prompts or support to help people stay in control. However, relatively few of the ideas generated made it into customers' hands. When we asked firms why they had not proceeded with the work, they identified two big unanswered questions holding them back:

1. **Should firms analyse financial data to identify potential vulnerability?**

   While acknowledging that proactive intervention could help customers, firms were concerned about the potential privacy implications, how this work would fit with data protection legislation, and the ethical consequences.

2. **If firms should carry out this analysis, how do they ensure it is safe, fair and in line with the customer's best interests and wishes?**

   Firms wanted to know more about how customers would want them to react if they identified potential problems in financial data, to ensure this work would be effective in getting customers the support they need.

6. Department for Business, Energy and Industrial Strategy and Department for Digital, Culture, Media and Sport. Smart data: putting consumers in control of their data and enabling innovation. HM Government. 2019.
7. Information Commissioner's Office. Royal Free – Google DeepMind trial failed to comply with data protection law. 2017. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/
8. Financial Conduct Authority. Guidance consultation: Guidance for firms on the fair treatment of vulnerable customers. 2019.
9. Financial Conduct Authority. Understanding the financial lives of UK adults. Findings from the FCA's Financial Lives Survey 2017. 2017.

In this report, we attempt to answer these questions. To do so, we draw on work with the Money and Mental Health Research Community, a group of 5,000 people with lived experience of mental health problems, or of caring for someone with a mental health problem, who are at the heart of everything we do. We carried out:

- A survey of 540 people with lived experience of mental health problems
- An online focus group with six people with lived experience of mental health problems, to explore the issues in greater depth.

In addition, we commissioned a nationally representative poll of 2,103 people to understand the appetite across the population for banks and building societies to proactively identify vulnerability, and public concerns with this approach.

We also draw on extensive conversations with firms about the possibility of using data to identify vulnerability, and the challenges involved. These included a half-day conference and two private roundtable discussions held jointly with the Financial Conduct Authority (FCA) and depth interviews with a small number of financial services firms and regulators.

Further details on methodology are provided in Annex A.

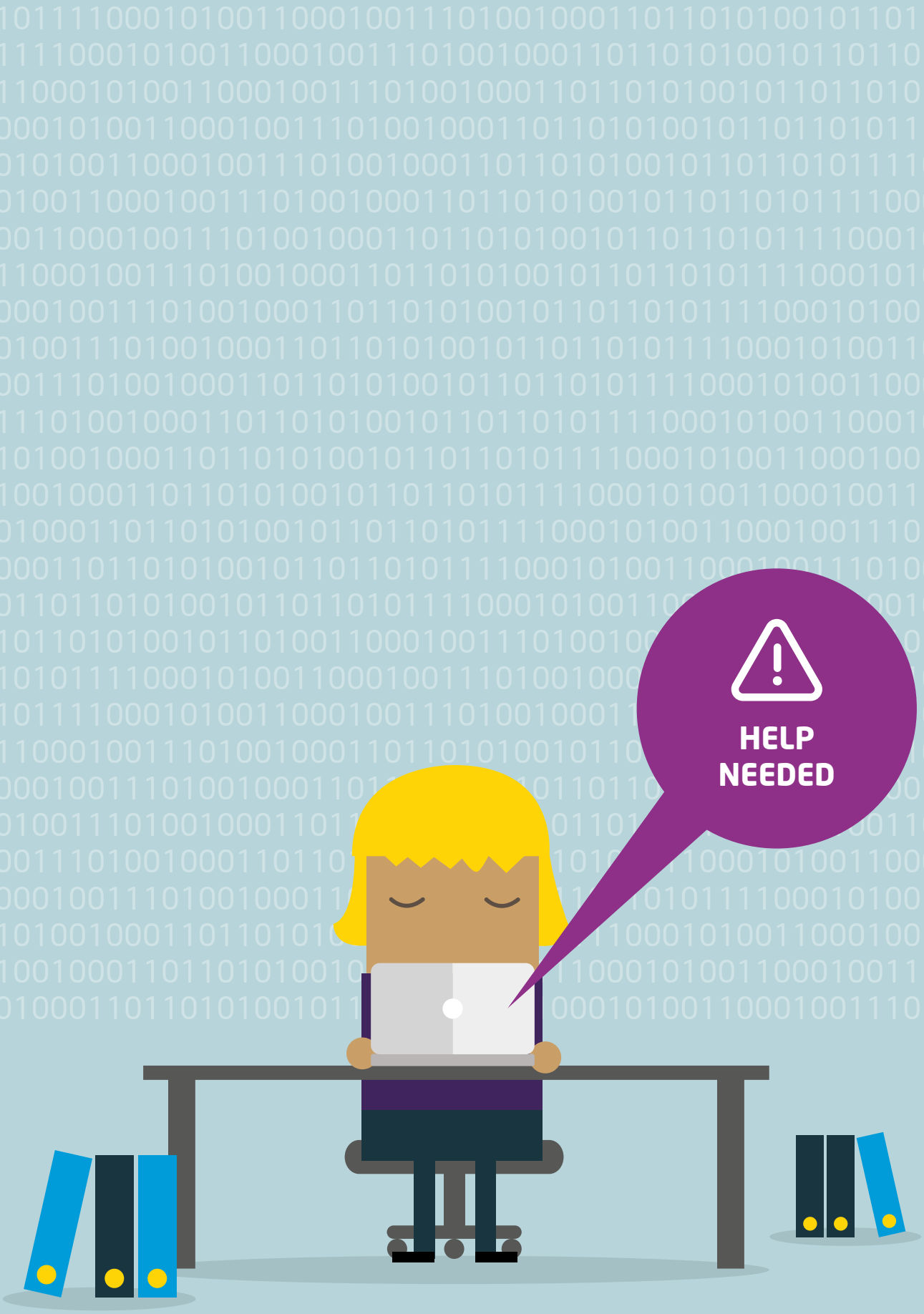
The first part of this report sets out the opportunity and the challenges associated with it, offering some answers to the first of our questions about whether this type of analysis should be undertaken.

- **Section One** sets out consumer demand for banks and building societies to use financial data to spot potential vulnerabilities and intervene.
- **Section Two** explores consumer concerns about data being used in this way.
- **Section Three** sets out some of the challenges firms could face if they try to identify potential vulnerability using financial data and offer customers targeted support.

The second part of this report seeks to find a way through some of these challenges and to make practical recommendations to firms, regulators and government. In doing so, it offers answers to our second big question, about how this analysis can be conducted safely, fairly and in line with customer wishes.

- **Section Four** sets out new evidence on consumer preferences and presents best practice for firms seeking to identify potential vulnerability in financial data.
- **Section Five** presents a series of recommendations for regulators and government which would help reduce uncertainty about using data to identify potential vulnerability, and unlock possible benefits.

Part One


HELP
NEEDED

Section One: The case for using data to identify vulnerability

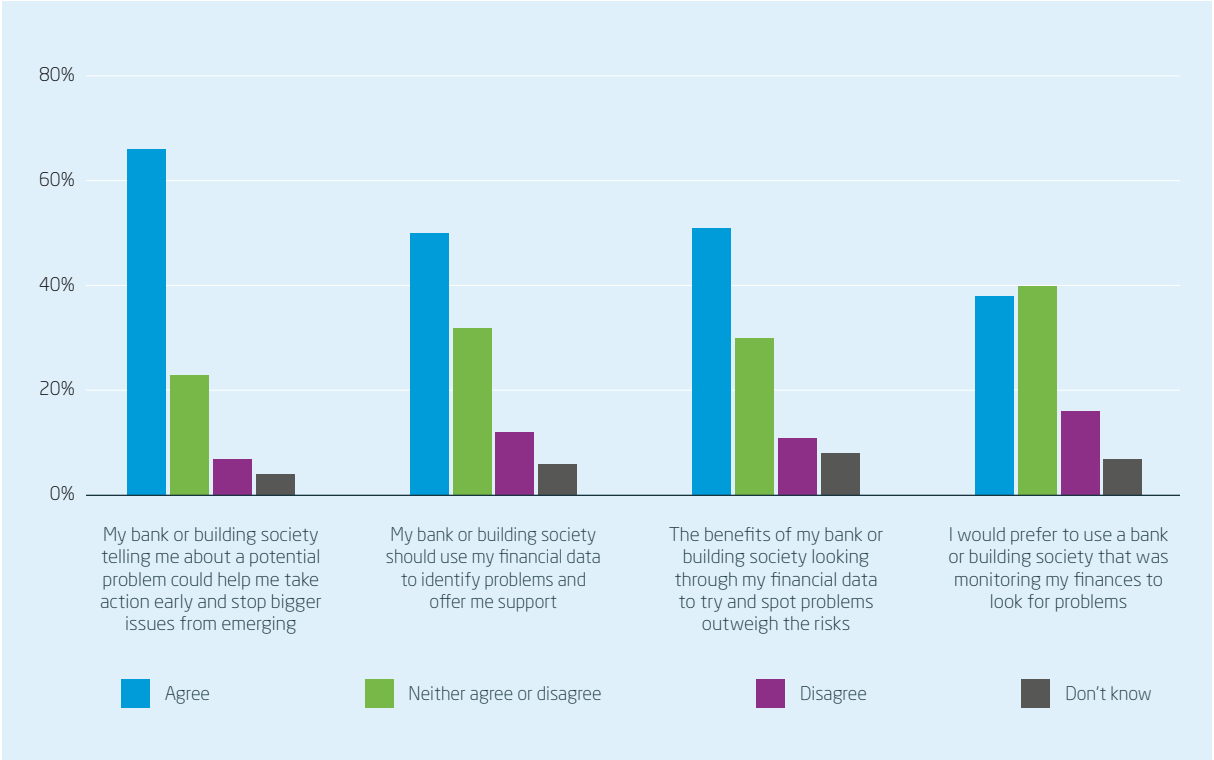
This section explores consumer demand for financial services providers to proactively support customers who are struggling with their finances. We examine attitudes across the population, and specifically among people who have experienced mental health problems, using national polling data and input from our Research Community.

1.1 Attitudes towards financial services providers using data to offer support

Half of UK adults (50%) think their bank or building society should use financial data to identify problems and offer support, with just one in ten (12%) disagreeing. As Figure 2 shows, this leaves a considerable proportion of the population uncertain about whether they would like their financial services provider to do this work. One in three adults (32%) neither agree nor disagree that their provider should offer this support, and 6% don't know.

Two thirds of adults (66%) recognise that being alerted about a potential problem by a financial services provider could help them take action early, and prevent harm. Offering this service could even offer firms a competitive advantage; four in ten people (38%) would prefer to use a bank or building society that monitored their finances to look for problems.

Figure 2. Attitudes towards financial services providers using customer data to provide support



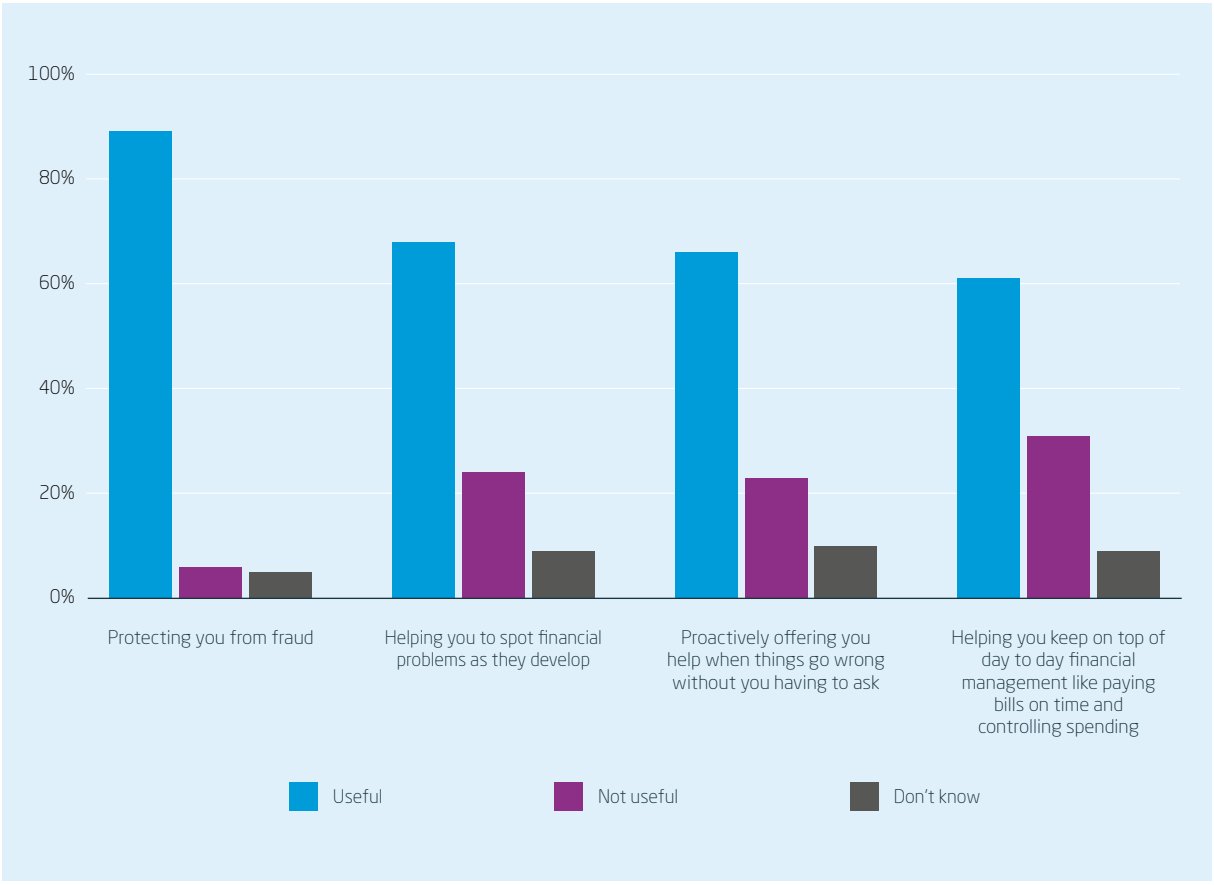
Source: Online survey of 2,103 people, carried out by Populus 21-22 August 2019. Data is weighted to be nationally representative.

People who have experienced mental health problems are consistently more enthusiastic about their financial data being used in this way. Seven in ten (71%) people who have experienced mental health problems feel that being alerted about a potential problem could help them to act early and avoid bigger issues, compared to 64% of people who have never experienced a mental health problem.

1.2 Attitudes towards particular use cases

As Figure 3 shows, almost everyone (89%) supports financial services providers using data to prevent fraud. Fraud prevention is a useful control case, as financial services providers are currently required to use customer data for this purpose, and many people are aware that their data is used in this way or will have experienced a fraud prevention intervention first hand.

Figure 3: Attitudes towards particular use cases of financial services providers using customer data to provide support



Source: Online survey of 2,103 people, carried out by Populus 21-22 August 2019. Data is weighted to be nationally representative.

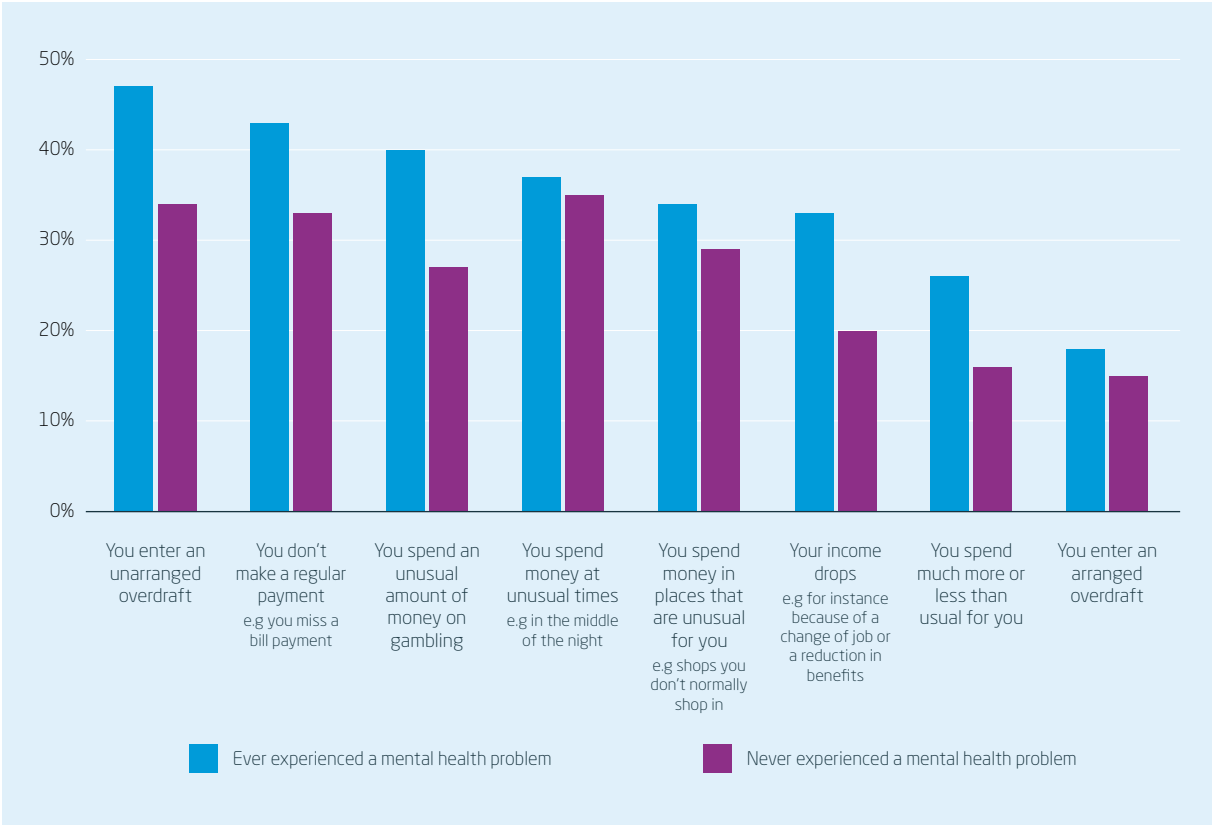
"I had a bank stop my credit card because it was being used frequently at locations over 100 miles from my home. I had neglected to inform them that I was on holiday in that location... It was useful to know that they were on the lookout for fraud."

Expert by experience

Nearly eight in ten people would also find it useful for their bank or building society to help them spot financial problems as they develop (68%) or to proactively offer help when things go wrong (66%). Three quarters of people (61%) think it would be useful for financial services providers to use data to help them keep on top of day to day money management.

Three in four people (75%) would like their bank or building society to proactively offer help in at least one of the specific circumstances listed in Figure 4.

Figure 4: Circumstances in which people would like their bank or building society to offer help or support



Source: Online survey of 2,103 people, carried out by Populus 21-22 August 2019. Data is weighted to be nationally representative.

People who have experienced mental health problems are consistently more likely to want help, especially if they spend much more or less than usual, or their income drops. Many Research Community members believed that, if designed appropriately, proactive support could help them to avoid both financial difficulty, and the additional strain this can place on their mental health.

> "I feel they could really help by flagging things as they happen as it may prevent things escalating."
>
> *Expert by experience*

Research participants with mental health problems suggested two main benefits: helping to spot problems, and supporting financial independence.

Helping to spot problems

Common symptoms of mental health problems, like increased impulsivity and difficulties concentrating, can make it harder to control spending and stick to a budget, increasing the likelihood of money troubles. At the same time, people often disengage from their finances. Avoidance is a common psychological coping mechanism among people experiencing anxiety.

> "A contact letter [would help] as when my mental health is flared up I bury my head in the sand and stop looking at anything stressful. However I do always open my mail."
>
> *Expert by experience*

If a financial services provider could gently alert a customer with mental health problems to early indications of money troubles, this could help them seek help before problems escalate, reducing financial and psychological distress.

Supporting financial independence

Other Research Community members felt that this kind of support could help them to stay in control of their finances by helping them to understand and change their behaviour.

> "In an ideal world, if they could help me to understand what areas of spend indicate that I am heading for an episode of depression. I think that there may be a pattern that I follow but can't always see it."
>
> *Expert by experience*

Section One summary

- There is broad support for proactive use of financial data to identify possible problems. Half of adults (50%) think their bank or building society should offer this support, with just one in ten (12%) disagreeing.
- A clear majority think that financial services providers helping to spot financial problems as they develop (68%), offering proactive support when things go wrong (66%), and helping with day to day financial management (61%), would each be a useful service.
- People with mental health problems are particularly enthusiastic about the prospect of proactive support. Not only are they more likely to experience financial difficulty, but symptoms of mental health problems can make it harder to spot issues and to ask for help.


USERNAME
PASSWORD

Section Two: Challenges from consumers

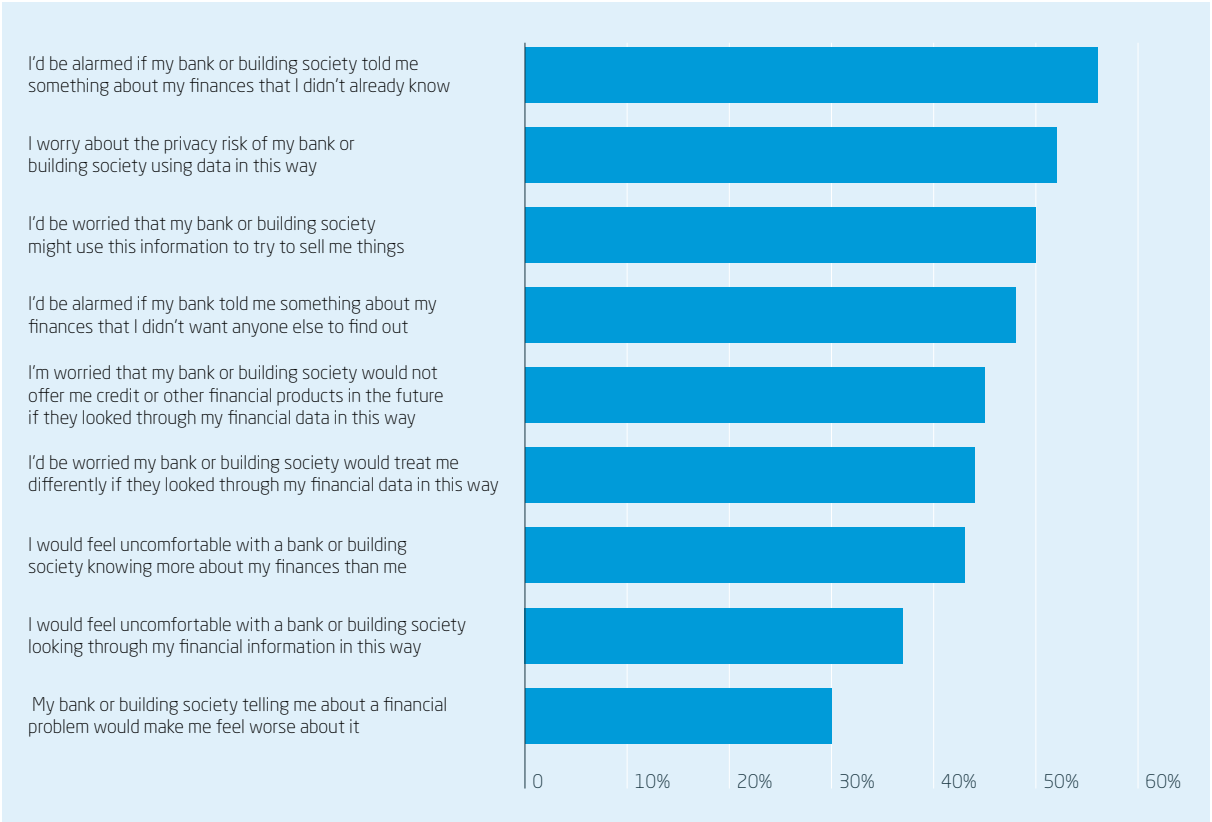
Half of people (51%) agree that the benefits of their bank or building society looking through their financial data to try and spot problems outweigh the risks, while only one in ten (11%) disagree. As with many new, complex ideas, there is substantial public uncertainty: one in three people (30%) neither agree nor disagree that benefits outweigh risks, and 8% say that they don't know.[10]

Figure 5 illustrates the prevalence of common concerns about banks and building societies undertaking this sort of analysis.

These concerns, and those expressed by participants with mental health problems in our qualitative research, fit into three interrelated categories:

1. **Privacy concerns** about how data will be used and shared
2. **Practical concerns** about what financial services providers would do if they spotted a problem
3. **Emotional concerns** about how it would feel to receive a message from your bank or building society suggesting there may be a problem.

Figure 5: Prevalence of concerns about banks and building societies analysing financial data to identify potential vulnerability (% agreeing with each statement)



Source: Online survey of 2,103 people, carried out by Populus 21-22 August 2019. Data is weighted to be nationally representative.

10. Online survey of 2,103 people, carried out by Populus 21-22 August 2019. Data is weighted to be nationally representative.

2.1 Privacy concerns

Many participants assume that banks and building societies are already analysing customers' financial data for marketing or other purposes.

> "They already monitor their customers, I am sure, to see whether they can sell them anything more, but don't use the same information to see if the customer needs help."
>
> *Expert by experience*

However, half of people (52%) are still worried about the privacy implications of their bank or building society analysing their financial data for signs of potential difficulties.[11] Over a third of people (37%) report that they would feel uncomfortable with their bank or building society looking through their financial data in this way.[12] These fears crystallised in specific worries about the information being hacked, leaked or shared with other banks, external organisations or government.

> "I would be concerned that the bank would share this information with other organisations such as insurance companies. I would also be concerned that banks do not have adequate measures in place to prevent this sort of sensitive information being stolen by external organisations."
>
> *Expert by experience*

Participants with mental health problems worried that feeling their privacy had been invaded would make them feel judged, and worsen their mental health.

> "Too much of what we do is monitored already. It's not healthy to be tracked like this. It would certainly make my mental health worse."
>
> *Expert by experience*

11. Ibid.
12. Ibid.
13. Ibid.

2.2 Practical concerns

Nearly half of people (44%) worry that their bank or building society would treat them differently if they looked for signs of vulnerability in their financial data. Slightly more people who have experienced a mental health problem fear this (47%) than those who have never experienced a mental health problem (42%).[13] Many participants were concerned about the embarrassment they would feel if they felt that staff were judging their decisions and behaviour.

> "If not done carefully, these kinds of schemes could easily lead to vulnerable people being judged and treated differently."
>
> *Expert by experience*

At the heart of many of these concerns were misgivings about why banks would want to identify potential vulnerability, with many participants expressing a scepticism about banks' motives.

Specific causes for concern included:

- Being refused credit or other financial products
- Targeted marketing of products
- Loss of financial control
- Efficacy of the intervention.

Being refused credit or other financial products

While a majority of people think it would be acceptable for banks to use customers' financial data to decide what financial products they are eligible for (55%), many still worry about the personal consequences. Nearly half (45%) of people worry that they would not be offered credit or other financial products in the future if

their banks used data in this way.[14] This fear is stronger among people with mental health problems, half of whom (52%) worry that their bank or building society wouldn't offer them credit or other products in the future if they used data in this way, compared to 41% of people who had never had a mental health problem.[15] While unaffordable credit can cause problems, for many people access to credit is important and losing the ability to borrow is a significant concern.

> "I'm worried the data will affect my chances of using borrowing etc to help improve my life in the times I'm well. I've used borrowing (responsibly) in the times I am well to really positive effect. Without that access to borrowing I would struggle to ever maintain any kind of good health – it's so linked with my financial wellbeing."
>
> *Expert by experience*

Targeted marketing of products

Half of people (50%) are concerned that their bank or building society would use this information to try to sell them things,[16] and 48% feel it is unacceptable for customers' financial information to be used to inform marketing.[17] Research Community members expressed concerns that banks may use insights about vulnerability to market products in a way that was not in the customer's best interests — for example, offering people in financial difficulty additional lines of credit which participants feared could lead to further difficulties.

> "Using this data could allow the banks to develop products that end up costing the customer and making the bank more money."
>
> *Expert by experience*

Loss of financial control and autonomy

Some participants in Money and Mental Health's research expressed a fear that banks and building societies may respond to potential vulnerability by seizing control of their accounts.

> "I fear they might try to dictate how I spend."
>
> *Expert by experience*

Efficacy of the intervention

Some respondents living with mental health problems were concerned that the ways banks could try to intervene after spotting possible problems in financial data simply might not be effective in preventing harm. If the notification arrives when a person is unwell, some respondents feared they would be unable to respond.

> "At my better times I might be open to help; but at other times any contact might make me push people further away because I'd feel even more like I'm not capable, coping nor in control."
>
> *Expert by experience*

14. Ibid.
15. Ibid.
16. Ibid.
17. Ibid.

2.3 Emotional consequences

One in three (30%) people think that their bank or building society telling them about a financial problem would make them feel worse about it.[18] Research Community members expressed fears that receiving these messages would leave them feeling ashamed. For a person experiencing a mental health problem, who may already be experiencing low self-worth, these feelings may be particularly difficult to cope with.

> "I'd feel shame. I'm struggling as it is and for an institution to know about my personal circumstances would be extremely humiliating. They may be acting necessarily and in my best interests but that wouldn't make me feel any better."
>
> *Expert by experience*

Others suggested that being informed of a potential financial problem could cause anxiety, particularly if they did not feel well enough to take action to address the issue. Some participants also thought receiving messages from their bank or building society while they were unwell could cause paranoia, which may further reduce their responsiveness to messages, and the efficacy of the intervention.

> "When suffering from poor mental health, the idea that your bank has been rummaging through your finances and judging that you are spending inappropriately is a difficult one to handle, especially if you are prone to paranoia. I can see the benefits, but also it could exacerbate the problem and further isolate someone."
>
> *Expert by experience*

However, if the message was sensitive and support effective, participants thought they may be willing to tolerate the emotional discomfort involved.

> "Although I might feel bad about the highlighted problem that isn't necessarily a bad thing if it prevents serious financial difficulty."
>
> *Expert by experience*

2.4 Balancing the risks

The risks of using transaction data to identify potential vulnerability and offer support must be balanced against the risks of not doing so, including the risk that people will not receive the help that they need and may experience further financial and psychological distress as a result.

Concerns may also loom larger when we discuss ideas in the abstract than when they become reality. Existing research shows that people become more open to the idea of banks analysing data in this way as they learn more about potential use cases.[19]

Many of these concerns can be addressed through the design of systems for analysing financial data, with some suggestions provided in the second part of this report.

18. Ibid.
19. GfK UK. Consumer attitudes to identifying vulnerability through the use of data. Barclays. 2018.

Section Two summary

- Half of people (51%) agree that the benefits of their bank or building society looking through their financial data to try and spot problems outweigh the risks, while only one in ten (11%) disagree.
- Public concerns fall into three broad categories:
  - **Privacy concerns** Half of people (52%) are worried about the privacy implications of their bank or building society analysing their financial data for signs of potential difficulties.
  - **Practical concerns** Nearly half of people (44%) worry that their bank or building society would treat them differently if they carried out this kind of financial analysis. Specific concerns include being denied access to credit and the loss of financial autonomy.
  - **Emotional concerns** One in three (30%) people think that their bank or building society telling them about a financial problem would make them feel worse about it. Participants with mental health problems felt receiving these messages could cause anxiety and shame which could worsen their mental health.
- These risks must be weighed against the risks of not using financial data to identify vulnerability, including missing the opportunity to offer timely support and reduce financial and psychological distress.


CREDIT CARD

Section Three: Challenges for financial services providers

Financial services providers face growing pressure from the FCA to proactively identify and support customers who may be vulnerable. Many firms also see potential business benefits, from increased customer satisfaction to swifter resolution of problem debts. However few firms are currently using data in this way.

This section explores the challenges of using data to identify potential vulnerability and intervene, drawing on extensive engagement with financial services providers, including a half-day conference, two private roundtable discussions and depth interviews. The barriers fall into four broad categories:

1. **Data protection**
2. **Technical limitations**
3. **Managing customer expectations**
4. **Managing risks.**

3.1 Data protection

Data protection is a key area of financial and reputational risk for firms, although data protection regulations are not intended to stifle innovation. The new, stronger General Data Protection Regulation (GDPR) is intended to ensure personal data is used to meet people's needs,[20] which arguably is the aim of identifying vulnerability in financial data. The FCA has also encouraged providers to proactively intervene to support vulnerable customers for years,[21] and this is already recognised as good practice by industry bodies.[22] However, increased scrutiny following some public scandals around data misuse and a lack of regulatory clarity has created some hesitation around using data to identify potentially vulnerable customers.

The Information Commissioner's Office (ICO) has offered little insight about how data protection regulations might be interpreted in the context of financial services. While the regulators issued a joint statement insisting that GDPR is compatible with FCA rules,[23] some financial services providers who took part in this project feel regulators' expectations are inconsistent.

Firms wishing to process data must consider the context and identify an appropriate legal basis for the analysis under GDPR.[24] As Figure 6 shows, this is a complex exercise.

20. Recital 4. General Data Protection Regulation. (EU) 2016/679.
21. Financial Conduct Authority. Occasional Paper No. 8: Consumer Vulnerability. 2015. Among a list of tips for providers on developing good practice, the FCA suggests: "ability to spot abnormal patterns or danger signals and act before people are actually in difficulties. Encourage proactive intervention."
22. Lending Standards Board. The Standards of Lending Practice: Personal Customers. 2017.
23. Financial Conduct Authority. FCA and ICO publish joint update on GDPR. 2018. https://www.fca.org.uk/news/statements/fca-and-ico-publish-joint-update-gdpr
24. Information Commissioner's Office. Lawful basis for processing. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ – particularly "How do we decide which lawful basis applies?"

Figure 6: Legal bases that financial services providers could use to process customer data in order to provide proactive support

Used when personal data must be processed to comply with a legal obligation or regulatory requirement – for instance when reporting customers suspected of money laundering to the National Crime Agency.[25] While the FCA encourages proactive intervention to support vulnerable customers, it is not a specific requirement, so it is not clear that firms can use "legal obligation" in this case.

Often used to assess how customers use products to inform improvements. Providers are expected to balance their interests against customers', and should not use this basis if they can reasonably achieve the same result in another, less intrusive, way. There is likely a strong business case for providing proactive support, as doing so should reduce customer arrears and improve customer relations. Legitimate interest may be particularly suitable where firms are transparent about data use, are undertaking activities that consumers would reasonably expect and if the intervention is clearly in customers' interests, so balancing interests is straightforward.

Providers might use this basis when delivering core elements of their service, such as issuing a payment card or recovering debt, but shouldn't use it for tangential purposes like improving products. A provider could use this basis if proactive support was a contractual service agreed with customers.

Providers can process personal data when a customer has explicitly agreed for them to do so. Consent must be specific and easy to withdraw. Many providers use this basis for marketing. A drawback is it can require significant customer engagement to collect and maintain consent. The ICO advises that "If consent is difficult, look for a different lawful basis".[26]

Source: Money and Mental Health analysis of GDPR and ICO guidance. 2019.

25. Information Commissioner's Office. Legal obligation. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/
26. Information Commissioner's Office. Consent. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

Some providers also report being uncertain about whether, or when, financial data could count as "special category data", which is afforded extra protection under GDPR.[27] If financial data revealed that someone was a member of a political party or paying for therapy, for example, this might be classed as special category data. In this case, providers must comply with additional conditions to process data, which may include seeking explicit consent or demonstrating substantial public interest in their activity. Using less granular financial data may avoid the 'special category data' dilemma, but could also limit firms' ability to identify vulnerability.

It is important that providers carefully consider the data protection implications of their activities and take responsibility, but the combination of regulatory uncertainty and risk aversion appears to be stifling innovation which could improve outcomes for consumers.

3.2 Technical limitations

Some providers highlight technical challenges around data infrastructure, data quality and skills and expertise that might limit their ability to identify vulnerable customers using financial data and increase the risk of errors.

Data infrastructure

Banks' efforts to use data productively are often stymied by fragmented legacy systems which make it difficult to achieve a holistic view of a customer's finances. Data from different products may be siloed, and banking groups with multiple brands can have different systems in each one. Many providers are working to integrate systems, but this is often a slow and expensive process.

Data quality

Providers do not always hold accurate information about the time, location or counterparty of transactions, due to lags in transaction processing and unreliable merchant information. While extra information about the transaction can be added, this is costly, and the principle of data minimisation encourages providers not to do so unless they have a clear purpose.[28]

Most providers also only have a partial view of their customers' finances, and different people can use the same financial product in vastly different ways. For instance, the same current account product could be used as a primary account, just for household bills, or for discretionary spending. This inconsistency can make it harder for providers to interpret the data they hold, both at an aggregate and individual customer level. Providers of 'low touch' products like savings accounts or loans have far less data to draw on. Financial data also only captures part of a person's situation, and without further context can be difficult to decipher.

Skills and expertise

While techniques like trigger-based analysis are commonplace, some providers do not have the capability to perform more sophisticated forms of analysis. Where providers have invested in data analytics expertise, this capacity is often focused on other areas of the business, rather than being used to support vulnerable customers.

27. Article 9. General Data Protection Regulation. (EU) 2016/679.
28. Article 5. General Data Protection Regulation. (EU) 2016/679. Data minimisation is one of the seven key principles of the GDPR. Data processors are encouraged not to collect or use more personal data than they need for any particular purpose.

3.3 Managing customer expectations

Many financial services providers are concerned about how using data to identify vulnerability might be perceived by customers. Providers highlight challenges in understanding what their customers want, communicating about new uses of data and managing expectations about how any insight is used.

Knowing how best to intervene

Many providers feel unsure about how their customers would like them to use financial data, and what good interventions would look like if potential vulnerability is identified. There is a growing pool of research on consumer attitudes, but relatively little has been tested in practice.

Communication challenges

Providers want to explain what they are doing with customers' data and why. However, it can be challenging to explain this complex analysis in a way that is easily understood, and make sure that this information reaches customers.

Further communication challenges may arise when firms identify somebody who may be struggling. As highlighted in Section Two, even among people who think that financial services providers should provide proactive support, some thought that they might be distressed or react negatively in the moment if they were alerted to a potential problem. It can be challenging to support vulnerable customers, and some providers are concerned that their frontline staff might struggle to handle this situation or it could generate complaints.

3.4 Managing risks

Firms also face potential regulatory and liability risks if they use financial data to identify potential vulnerability.

It is unclear what would constitute 'fair treatment' if a customer who was identified as potentially vulnerable did not respond to attempts to offer support. Taking further action, for example blocking payments, may cause distress to the customer and result in complaints. But failing to take action could leave the firm exposed to additional liability if the customer subsequently experiences substantial detriment, for example running up large debts.

Providers would also have to decide how, if at all, the insight gained from their analysis would affect customers' access to credit and other products. It may be unethical or even against regulatory requirements for a creditor not to include this information in an affordability assessment, although consumers express clear concerns about this information being used in credit decisions.

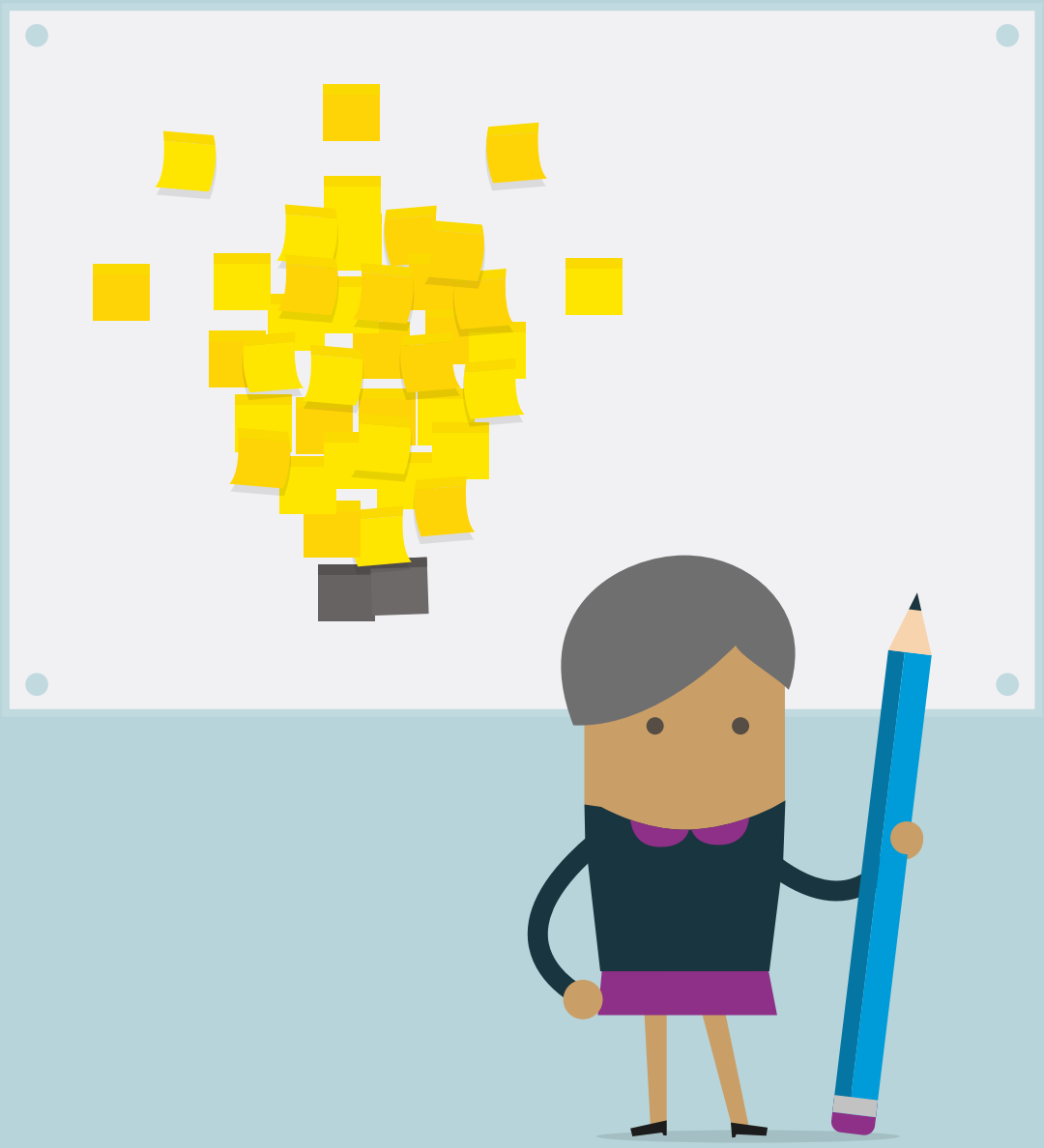
Providers must weigh these risks against the potential gains that providing proactive support could bring.

Section Three summary

Extensive engagement with financial services providers has revealed a number of challenges that currently hold them back from using transaction data to proactively support customers at risk of financial difficulty:

- **Data protection** While the ICO encourages innovation, there is a lack of clarity about how data protection rules apply in the context of proactive support
- **Technical limitations** Many providers face data infrastructure and quality challenges, and providers only have a partial view of most customer's finances
- **Managing customer expectations** Well-meaning offers of support could be received badly and jeopardise customer relations
- **Regulatory and liability risks** Where customers don't respond to initial interventions, or customers identified as potentially vulnerable go on to apply for credit or other products.

Part Two



Section Four: Designing interventions

The research presented in Sections Two and Three identified several challenges around the idea of using data to identify vulnerability.

Consumers' main concerns were:

- Privacy, including the risk of data leaks, hacking and unauthorised sharing
- Practical implications, including whether banks would treat them differently after identifying vulnerability in their data, in terms of access to credit, targeted marketing or reducing their financial autonomy. Many consumers also had concerns about how effective firms' interventions would be
- The emotional consequences of receiving messages from firms informing them of potential financial problems.

Firms' main concerns were:

- Meeting data protection obligations, including understanding what legal basis should be used for this kind of data analysis
- Technical limitations in their access to data and ability to spot potential vulnerabilities
- Managing customer expectations, including understanding how best to intervene and how to communicate with customers about this work
- Managing regulatory and liability risks.

To address these concerns, we need to work through a series of issues:

1. **Protecting privacy**

   To address concerns about how and why data is used, we need to answer questions about how customers are informed about the use of financial data to identify vulnerability, and consider how to help customers stay in control.

2. **Designing and delivering the intervention**

   To deal with the challenge of managing customer expectations, ensure the intervention is effective, and overcome technical limitations, we need to consider what financial services providers should do when they spot a potential problem.

3. **Managing spillovers to other products and services**

   To answer ethical questions and concerns about customers being treated differently if banks conduct this type of analysis and possible spillovers to other services, we should examine how consumers feel about data being used for different purposes, and consider the safeguards that could be put in place.

In this section we develop a set of practical best practice principles for firms. These are suggestions, drawing on the evidence available about consumer preferences, on how banks and building societies may wish to proceed when developing programmes to identify vulnerability using financial data. As this approach is so new, we would also recommend that firms proceed on a 'test and learn' basis, co-producing their approach with customers, including people experiencing mental health problems, to maximise the benefits and minimise the risks of this type of data analysis and interventions.

4.1 Protecting privacy

Many people expressed concerns about how and why firms might use their financial data, and some felt that firms should only use this data to identify vulnerability when they have specific consent to do so. Firms face a challenge to provide customers with meaningful choice and control over how their data is used, while maximising the benefits for the customers most in need of support.

> "My biggest concern would be privacy and control over my own finances. I like to have complete control but would also appreciate sound practical advice."
>
> *Expert by experience*

Relying on explicit consent to provide this support may mean that the people who are most in need of help could miss out. Consent can be arduous to collect and maintain, and people experiencing mental health problems or other difficulties may be less likely to respond to messages about opting in. Unintentionally, this approach could sharpen existing inequalities between more engaged consumers and those who are vulnerable.

By being transparent about how and why they are using financial data, and building choice into their support offering, firms can empower customers to make decisions about their finances and address many concerns and uncertainties.

> "Banks would need to be completely open and honest about the details and explain them in plain language to help those who may have difficulty with understanding."
>
> *Expert by experience*

Firms should give customers a choice, and make it easy for them to opt out of proactive support if they wish. Some participants advocated a degree of friction in this process, to protect against hasty decisions to opt out during a period of poor mental health.

> "I would be concerned, however, that there are certain kinds of mental illness which might cause you (against your own best interests) to opt out of monitoring at exactly the time you most need support, because you want to be left alone."
>
> *Expert by experience*

Research participants also suggested that firms could go further, and give customers more precise control over what their bank or building society looks for in their data. Eight in ten people (83%) feel that being able to choose what kinds of problems the bank or building society look for would be an important safeguard.[29]

> "I wouldn't like my bank to be involved in anything OTHER than something I had explicitly made them aware of – and then for them to monitor that with my authority, such as in my case, gambling problems. I would feel uncomfortable about them looking at my account in general."
>
> *Expert by experience*

Best practice

Be transparent about how and why customers' financial data is being used, and offer customers meaningful choice and control over how their data is used. Customers should have the option to opt out of analysis aiming to identify vulnerability and offer proactive support, and should be offered control over which financial warning signs the firms looks for.

29. Online survey of 2,103 people, carried out by Populus 21-22 August 2019. Data is weighted to be nationally representative.

4.2 Designing and delivering the intervention

Both consumers and firms expressed concerns about whether interventions targeted at people identified as being potentially vulnerable would actually work. This is a critical question for businesses, as they will require reasonable grounds for making investment in these programmes. Equally, for consumers, efficacy may be an important justification for potential loss of privacy.

Banks could intervene in a range of ways when they identify possible vulnerability. Figure 7 summarises the options.

To understand how customers might balance the benefits and risks of different interventions, we asked Research Community participants how they would want their bank to respond in various scenarios. The results are illustrated in Figure 8.

Figure 7: Options for intervention

	What would this look like?	Pros	Cons
Just tell me	Firms would simply notify customers of potential indicators of vulnerability, for example by text message.	Could help customers to respond to changes in their financial circumstances without undermining their autonomy.	Onus on the customer to recognise the message and work out how to respond, both of which can be difficult for customers who are unwell.
Tell me and tell me where to find support	Firms notifies customers of potential problems and signposts to a source of support, for example information on their website or from a charity.	Could help customers to find additional help which they would otherwise be unaware of, for example specialist debt advice.	If a person was not well enough or otherwise unable to follow up on the firm's suggestion, the message might not succeed in preventing harm.
Tell me and offer practical support (e.g. help to set up a spending limit on my account)	Firms would inform customers of potential problems, and offer tools to help, for example spending controls.	Practical support may empower customers to change their behaviour or take action to resolve problems.	Practical help may not be possible in all situations. Success may also depend on whether the customer is well enough to engage.
Take immediate action to protect me, for example, blocking payments	When firms notice a problem, they immediately take action to reduce the likelihood of harm.	Could help prevent further harm, especially if customers are unable to engage with messages.	Could undermine the customers' autonomy and independence. May cause distress or inconvenience if payments are blocked against customers' wishes.

Source: Money and Mental Health Policy Institute. 2019.

Figure 8: What action would you want your bank or building society to take if they spotted the following problems in your financial data?

	Do nothing	Just tell me	Tell me and tell me where to find support	Tell me and offer practical support (e.g. help to set spending limit on my account)	Take immediate action to protect me (e.g. blocking payments)
You are a victim of fraud	1%	2%	8%	9%	80%
You are the victim of a scam	0%	2%	10%	10%	77%
You spend an unusual amount of money on gambling	8%	7%	20%	24%	41%
You enter an unarranged overdraft	3%	19%	22%	39%	17%
You don't make a regular payment - for instance you miss a bill payment	4%	26%	29%	35%	6%
Your income drops - for instance because of a change of job or a reduction in benefits	13%	12%	31%	39%	5%
You spend money in places that are unusual for you - for example, unfamiliar locations	8%	38%	15%	18%	20%
You spend money at unusual times - for instance in the middle of the night	16%	29%	16%	21%	18%
You spend much more or less than usual	15%	31%	21%	26%	7%
You enter an arranged overdraft	17%	40%	16%	23%	5%

Source: Money and Mental Health survey of 540 people with lived experience of mental health problems. Base varies by row, between 403 and 448.

In the case of fraud and scams, most participants want their bank to take immediate action to help, for example by blocking payments. Four in ten Research Community members would also like their bank to take immediate action if they spend an unusual amount of money on gambling. There is a general view that some support is needed in this scenario; only 7% thought that a bank just telling them about the issue would be sufficient. By contrast, in response to a fall in income, unarranged overdraft use or missed regular payments, Research Community members preferred being informed of the situation and offered help, rather than a more active intervention.

Preferences about what banks should do when spending behaviour changed were much more dispersed. This suggests that the best way forward for banks may be to allow customers to personalise the intervention that they receive, which may also increase efficacy.

"The timing and wording of support options need to be tailored to each situation, i.e. if they suspect fraud they need to act immediately however if they are just identifying spending has increased this month there could be a valid reason for it so offering details of debt charities and support the bank can offer may not be needed and seen as offensive."

Expert by experience

Best practice

Different issues require different interventions. Where there are diverse preferences over the best type of intervention for a specific trigger, firm should consider allowing customers to personalise the intervention they receive.

The choice of communication channel for any messages is also likely to have a significant impact on effectiveness. In public polling, 87% of people thought that being able to choose how their bank or building society contacted them if they found a problem was an important measure in developing these programmes.[30]

This could be particularly important for people experiencing mental health problems, many of whom will struggle with one or more communication channels.[31] While, generally, people experiencing mental health problems preferred the idea of being notified in writing — with text (67%) and email (64%) most popular — there was a diversity of opinion, as illustrated in Figure 9. Allowing people to choose a channel is likely to substantially increase the chances that customers receive and engage with messages.

The tone of communications was arguably more important to respondents with mental health problems than the channel, with many emphasising that a friendly and supportive tone was essential to help them respond to the message. This could also soften the emotional impact of receiving these messages when things are starting to go wrong financially.

"Generating 'friendly' communications is important. When I am at my most depressed, I feel overwhelmed and under attack; I might not open an email that's got a subject of 'You've exceeded your overdraft limit'. It would be more likely that I would open one with the subject 'We can help you manage your cash flow if you would like us to'."

Expert by experience

One idea, consistent with the notion of customer control, was for people to draft their own support messages, or choose from a menu of options.

30. Online survey of 2,103 people, carried out by Populus 21-22 August 2019. Data is weighted to be nationally representative.
31. Holkar M, Evans K and Langston K. Access essentials. Money and Mental Health Policy Institute. 2018.

"I would like my bank to contact me, but in a comfortable non-threatening way, because I could feel like I was being accused of something. Maybe a prearranged message that I could reply to if I need help?"

Expert by experience

Best practice

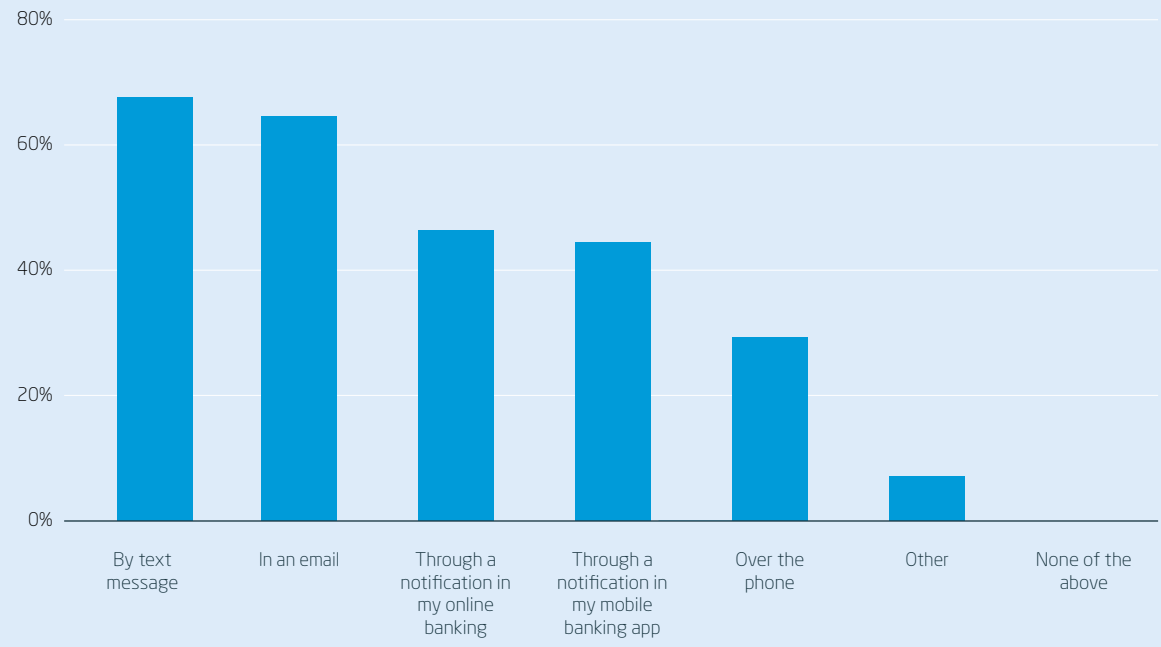
Allow people to choose which communication channels are used to send them messages about potential vulnerabilities or things that could help, and consider allowing them to choose from a menu of interventions which they think would best meet their needs.

Best practice

Ensure the tone of messages is friendly and supportive, signposting customers to steps they can take to improve their situation. Avoid simply informing people of issues, which can generate feelings of guilt without improving their ability to rectify the situation.

Many participants with mental health problems felt that, while computers could be used to spot problems in data, the offer of support should come from a human. It is important that vulnerable customers have a clear route to human support if they need it.

Figure 9: How respondents would like to be contacted by their bank or building society if they spotted something unusual in their data



Source: Money and Mental Health survey of 540 people with lived experience of mental health problems. Base for this question: 448 people.

"A person could look in more detail and ring you if something doesn't seem right, a computer might not respond in the right way at the right time."

Expert by experience

Best practice

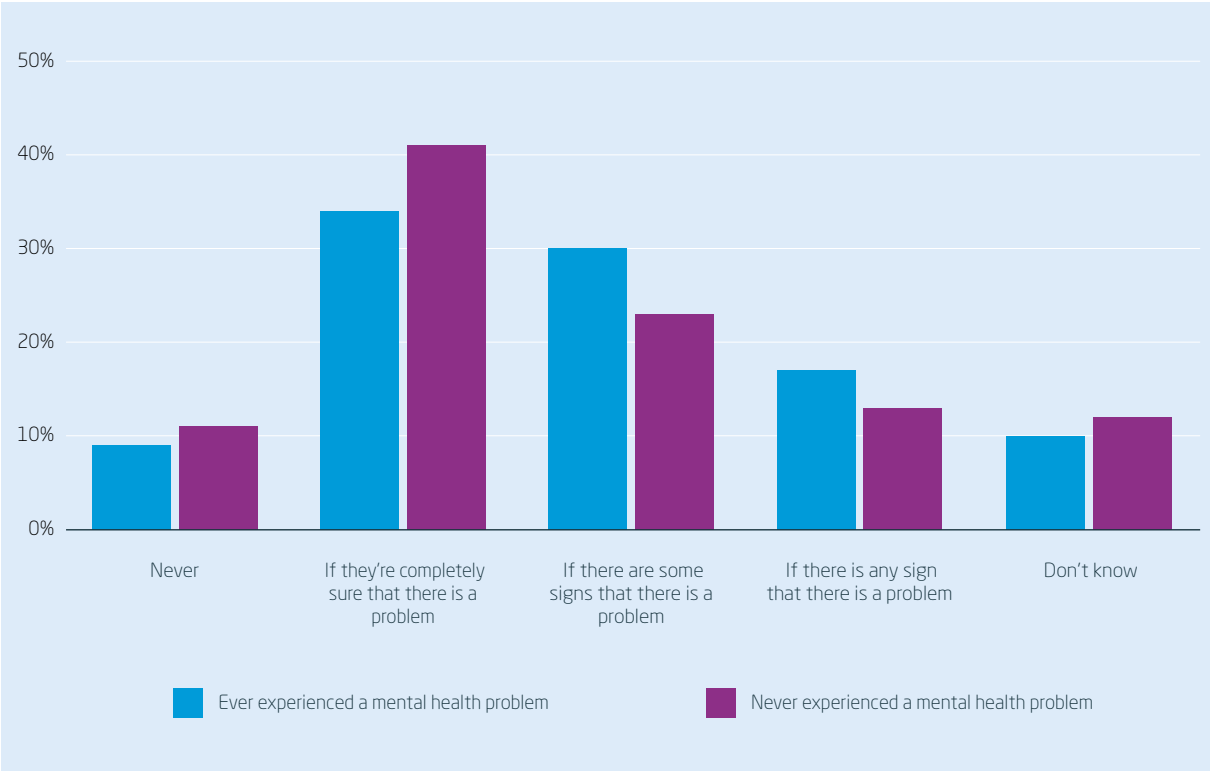
While computers may do most of the work of identifying vulnerability and sending automated messages, ensure there is a pathway to support from a person if the customer needs it.

How banks should respond if a customer doesn't react to an intervention is another tricky ethical question.

Some participants feared having their financial autonomy reduced if they didn't respond to messages and banks took additional steps to protect them, but others thought this could be useful. Again, flexibility and allowing the customer to choose may be the way through.

Challenges around data availability may be best addressed by considering what sort of organisation undertakes the data analysis. While the customer's existing bank or building society might be the simplest option, where a person uses several different providers, aggregator services may be better able to keep an eye on a person's holistic financial situation and identify changes accurately. Incorporating non-financial data, like information about energy and telecoms use, could also help to provide a fuller understanding of a customer's situation.

Figure 10: Level of certainty people would want financial services providers to have before contacting them about a potential problem, by mental health problem



Source: Online survey of 2,103 people, carried out by Populus 21-22 August 2019. Data is weighted to be nationally representative.

Best practice

Consider the potential benefits of account aggregation and bringing in non-financial data, to improve data quality and accuracy of analysis.

In general, however, people are happy for their banks to contact them even if they are not entirely sure there is a problem. Across the population, 40% would want their bank to get in touch when there were some signs that there was a problem, even if they are not certain. Only one in ten (10%) would prefer that their bank or building society never contacted them to offer help if there was a potential problem.

People who have experienced mental health problems, in general, would be more keen for their bank and building society to get in touch even if they were less confident about what the data was showing. Nearly half (47%) of people who have experienced a mental health problem would be happy for their bank to get in touch when there are at least some signs of difficulty, compared to just 36% of people who have never experienced a mental health condition.

Best practice

Be open with consumers about the limitations of this type of data analysis and the possibility of inaccurate analysis.

4.3 Managing spillovers to other products and services

For people with mental health problems, a significant concern was whether insights gleaned from their data for the purpose of offering support would affect the rest of their relationship with their bank or building society, including their access to credit. Across the population, however, many customers are happy for banks to use their data to decide eligibility for financial products and to inform the design of new products and services, as illustrated in Figure 11.

The relatively high levels of tolerance for data being used for purposes beyond identifying vulnerability may be helpful to firms, who might face regulatory or ethical challenges if they ignored certain data points when making lending decisions.

Across each of these questions, more than one in six people said that they did not know whether this was acceptable or unacceptable, demonstrating substantial uncertainty about how data should be used. Nine in ten people (89%) think it is important that banks and building societies clearly explain what they are using financial information for in a way they can understand, and the same proportion think it is important that their bank or building society clearly explains the risks and benefits of how they use financial data.[32]

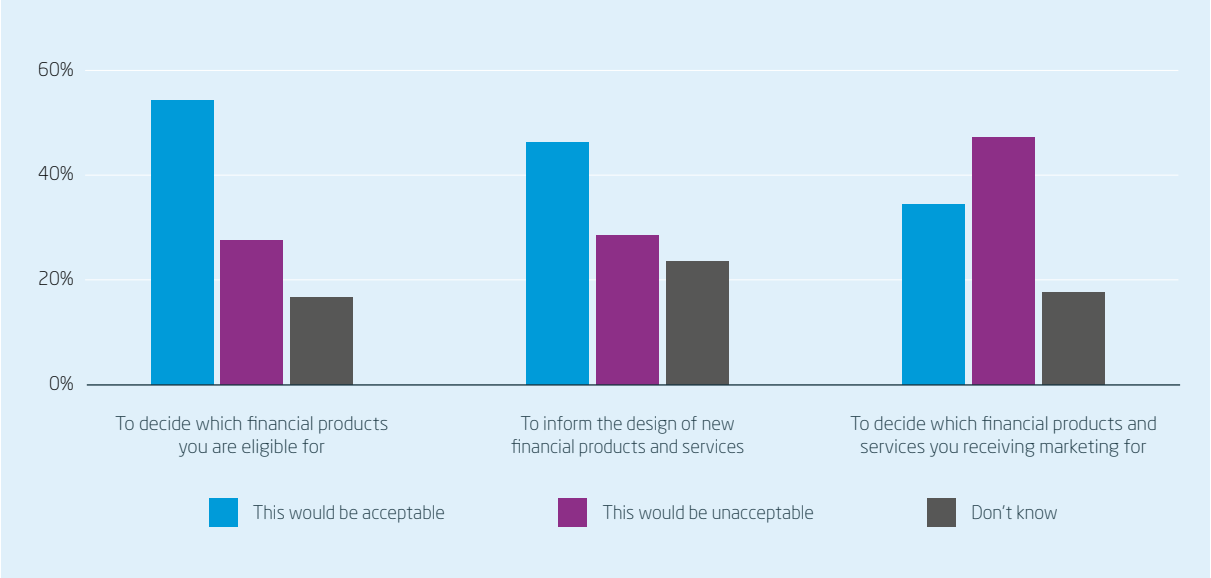
Best practice

Carefully consider the pros and cons of using information about potential vulnerabilities derived from financial data to make decisions about other products.

Be open with customers about what data is being used for and the risks and benefits involved, so that they can make informed decisions.

32. Online survey of 2,103 people, carried out by Populus 21-22 August 2019. Data is weighted to be nationally representative.

Figure 11: Consumer views on when it is acceptable for firms to use their financial data



Source: Source: Online survey of 2,103 people, carried out by Populus 21-22 August 2019. Data is weighted to be nationally representative.

Section Four summary

To protect privacy, firms should provide customers with choice and control. This should include the option to opt out of analysis aiming to identify potential vulnerability, and giving customers the opportunity to choose what types of potential vulnerability they are comfortable with their bank or building society looking for.

When designing and delivering interventions as a result of something spotted in data, firms should:

- Be mindful that different issues require different interventions, and consider letting customers choose what should happen in specific scenarios
- Allow people to choose which communication channels are used to send them messages
- Ensure the tone of messages is friendly and the content is focused on seeking support and resolving the problem
- Consider the benefits of account aggregation to minimise challenges around data limitations
- Be open with consumers about the possibility of inaccurate results.

Testing and co-producing interventions with customers would help firms to develop interventions that balance the risks and benefits of identifying potential vulnerability in financial data.

Section Five: Broader policy recommendations

The best practice recommendations presented in Section Four should help firms resolve questions about how best to go about identifying vulnerability through financial data and offer customers support. However, some significant questions remain that cannot be answered through consumer research alone. These include:

1. **Data protection challenges**

   How do data protection regulations apply in the specific context of processing financial data to identify vulnerability and provide support?

2. **Ensuring efficacy**

   Firms can learn lots about what good interventions look like from listening to and testing propositions with customers. A separate challenge, however, is identifying potential signs of vulnerability with reasonable accuracy, reducing the number of false alarms and missed opportunities to help.

3. **Managing spillovers to other services**

   To answer questions about whether data indicating potential vulnerability should affect access to credit, firms are likely to need further regulatory guidance and room to explore ethical challenges.

In this section, we set out the broader policy changes needed to address these challenges, and to realise the vision of using data to offer timely support to people in potentially vulnerable situations.

5.1 Overcoming data protection challenges

Financial services providers cite uncertainty about regulation as a key factor holding back innovation. The FCA and ICO have stated that their rules are compatible, and both claim to encourage innovation. However, many providers feel that existing guidance is too high level to be instructive. Regulators must recognise that this uncertainty can drive risk aversion and inaction, particularly in an environment of intense scrutiny on data protection and the treatment of vulnerable consumers.

The current lack of regulatory clarity essentially imposes a cost on providers who wish to innovate, either in investment in legal or regulatory advice, or acceptance of risk, which can be prohibitive, especially for smaller firms. When a firm does invest, and reaches an opinion about how regulatory principles might apply in a specific context, this insight is held privately. This creates a risk that some providers might go ahead and offer this kind of support, while others hold back. It could also create further inequities in markets where switching remains infrequent, as some customers are able to access this support while others are not. Greater clarity from the regulators could reduce these costs, encourage innovation and ensure this vital support is available across the market.

Some work to clarify regulatory expectations is already underway. The FCA is currently developing guidance to help providers understand their responsibilities towards vulnerable consumers, with input from the ICO, which has also has produced some guidance for financial services firms. However, to date, the ICO has focused more on enforcement than on providing specific guidance, and the regulators have not produced detailed joint guidance about the many areas where data protection and financial regulation interact. We are pleased to see the FCA and ICO strengthen their

commitment to collaboration.[33] As a next step, both regulators should consider what guidance is needed to help firms unlock the potential benefits for consumers of using data to identify vulnerability, and provide clarity on the regulatory context.

The FCA and ICO should issue joint guidance to help financial services providers understand how their regulatory principles apply in the specific case of using financial data to identify potential vulnerability and offer proactive support.

While this guidance will not remove the need for firms to interpret the law in specific situations, it should address key areas of uncertainty such as:

- Which legal bases could be used to analyse customer transaction data in order to provide proactive support?
- When, if ever, is financial transaction data classed as special category data? How should special category financial transaction data be dealt with?

This may require a greater shift from the ICO, who have a less developed policy function. **The Government should ensure the ICO has sufficient funding to proactively engage with firms exploring innovative uses of data and can provide anticipatory regulation.**

5.2 Ensuring efficacy

Support for innovators

To address problems at the market level, as well as providing guidance, the FCA and ICO should continue to work together to support innovation at the individual provider level. The FCA has supported the ICO in the development of its regulatory sandbox, and the ICO has provided tailored input to the FCA's Innovation Hub, which also contains a regulatory sandbox.

The sandbox approach allows providers to test innovative propositions with real consumers. The provider and regulator work together to understand how regulations apply in a new context, and the provider is supported to ensure that consumer protection is built into their business model, and that test participants are not put at risk.

The FCA and ICO should seek out and support providers who want to test out innovative uses of financial data to proactively support customers who are potentially vulnerable.

Innovators may be best supported through the proposed cross-sector sandbox, rather than existing FCA or ICO innovation schemes. The FCA has recognised that some providers previously supported through Project Innovate have wanted guidance with data protection requirements that was outside their current support offering.[34] These use cases would likely benefit substantially from the support of both regulators, to make sure that both data protection and wider consumer protection considerations are made as the innovation is developed and tested.

33. Information Commissioner's Office and Financial Conduct Authority. Memorandum of Understanding between the Information Commissioner and the Financial Conduct Authority. 2019.
34. Financial Conduct Authority. The Impact and Effectiveness of Innovate. 2019.

Improve understanding of when to help

There is a growing body of evidence setting out how customers would like to be supported in moments of vulnerability. However, questions about when to provide support, and what the triggers for intervention should be, are harder for providers to answer in isolation, particularly if data is fragmented, or they only see part of a customer's financial life. Research into the financial patterns that might indicate that somebody is at risk of financial difficulty is hamstrung by a lack of access to large volumes of anonymised financial data.

The government should create a repository or 'data trust' of anonymised financial data — and allow researchers access — to unpick these patterns.

Like the 100,000 Genome project in the treatment of cancer and rare genetic diseases,[35] this could yield a world-class understanding of peoples' financial circumstances, and transform our ability to identify customers who need help. Based on this understanding, innovators could develop tools to pick up on the warning signs of financial difficulty and offer proactive support.

5.3 Managing spillovers to other products and services

A further challenge for financial services providers is understanding whether insights around vulnerability derived from financial data should or should not be used to promote or make decisions about other products. There is a possible tension here between the FCA's guidance that firms must treat customers fairly — including those who are potentially vulnerable — and the need to rigorously assess credit affordability, which could have significant implications for the availability and pricing of credit and insurance products.

To help providers navigate these tensions, the FCA should provide further guidance about how these principles may interact, or a space for firms to explore these issues and share best practice.

This should include exploration of the following questions:

- If a provider identifies that a customer is at significant risk of financial detriment, what does their obligation to treat the customer fairly entail?
- What should the provider do if the customer does not respond to an offer of support?

35. Genomics England. The 100,000 Genomes Project. https://www.genomicsengland.co.uk/about-genomics-england/the-100000-genomes-project/

5.4 Conclusion

There is enormous potential for financial data to be used to identify customers who are potentially vulnerable, and to offer support. But to get there in a way which is safe, ethical and balances the rights and needs of consumers and firms' priorities, we need to create opportunities for customers to input into the design of new systems and processes, and for firms to share best practice.

Supporting the needs of vulnerable customers should not be an area where firms compete, but where they cooperate to ensure standards are as high as possible across the board, and that customers know what to expect. In addition to each of the policy recommendations and best practice guidance above, therefore, we call on the FCA, ICO, government and other bodies – including the CDEI and Office for AI – to make spaces for firms to share best practice, and for firms to continue engaging with consumers on these delicate issues. A significant benefit of this research has been creating a space for discussion between firms, through our workshops held jointly with the FCA. Money and Mental Health would be glad to continue playing this role, if financial services providers would like further support as they seek to design and implement systems to identify customers who are potentially vulnerable and offer targeted support.

Section Five summary

While best practice can help firms resolve some questions about how best to use financial data to identify and respond to indications of customer vulnerability, some broader questions raised by this idea require input from policymakers and regulators.

- The FCA and ICO should:
  - Issue joint guidance to help financial services providers understand how regulatory principles could apply in the specific case of using financial data to identify customers who are struggling and offer proactive support
  - Seek out and support providers who want to test using financial data to proactively support customers.
- The government should:
  - Ensure the ICO has sufficient funding to enable them to engage with firms and other regulators as issues emerge
  - Create a repository or 'data trust' of anonymised financial financial data to allow researchers to identify more patterns which could indicate potential vulnerability.
- The FCA should:
  - Provide further guidance to firms or create a space to share best practice around the difficult ethical issues which could be raised when data is used to both identify possible vulnerability and assess credit-worthiness.


IMPOSSIBLE

MONEY AND MENTAL HEALTH
POLICY INSTITUTE

Kindly sponsored by Barclays. This report represents the research and views solely of the authors and of the Money and Mental Health Policy Institute and does not represent the views or experiences of Barclays.