House of Commons

Treasury Committee

# IT failures in the Financial Services Sector

## Second Report of Session 2019–20

HC 224

House of Commons

Treasury Committee

# IT failures in the Financial Services Sector

## Second Report of Session 2019–20

*Report, together with formal minutes relating to the report*

*Ordered by the House of Commons to be printed 22 October 2019*

**HC 224**
Published on 28 October 2019
by authority of the House of Commons

## The Treasury Committee

The Treasury Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of HM Treasury, HM Revenue and Customs and associated public bodies.

### Membership

Mel Stride MP (Chair) *(Conservative, Central Devon)*

Rushanara Ali MP *(Labour, Bethnal Green and Bow)*

Mr Steve Baker MP *(Conservative, Wycombe)*

Colin Clark MP *(Conservative, Gordon)*

Mr Simon Clarke MP *(Conservative, Middlesbrough South and East Cleveland)*

Charlie Elphicke MP *(Independent, Dover)*

Alison McGovern MP *(Labour, Wirral South)*

Catherine McKinnell MP *(Labour, Newcastle upon Tyne North)*

Wes Streeting MP *(Labour, Ilford North)*

Alison Thewliss MP *(Scottish National Party, Glasgow Central)*

### Powers

The committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No. 152. These are available on the internet via www.parliament.uk.

### Publication



Committee reports are published on the Committee's website at www.parliament.uk/treascom and in print by Order of the House.

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

### Committee staff

The current staff of the Committee are Gail Bartlett (Second Clerk), Emily Buckland (on secondment from the Bank of England), Sarah Goodwin (on secondment from the Prudential Regulation Authority), Rachel Kift (on secondment from the National Audit Office), Dan Lee (Senior Economist), Gosia McBride (Clerk), Aruni Muthumala (Senior Economist), Matt Panteli (Senior Media and Policy Officer), Yasmin Raza (on secondment from the Financial Conduct Authority), Anne Stark (on secondment from HM Revenue & Customs), Baris Tufekci (Committee Support Assistant), Adam Wales (Chief Policy Adviser), Maciej Wenerski (Senior Committee Assistant), and Marcus Wilton (Senior Economist).

### Contacts

All correspondence should be addressed to the Clerk of the Treasury Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 5769; the Committee's email address is treascom@parliament.uk.

You can follow the Committee on Twitter using @commonstreasury.

# Contents

# Summary

After a number of significant IT failures, such as that experienced by TSB in 2018, this inquiry provided an opportunity to look 'under the bonnet' of the financial services sector to ask why IT failures were happening, and how the industry and the Regulators could have prevented such incidents.

Bank branches are disappearing from our high streets and local communities, and cash machines are being withdrawn. Customers are increasingly being expected to use digital services, and yet these services are being significantly disrupted due to IT failures. Consumers suffer from harm when these IT failures occur. They have been left without access to their vital financial services and have been left unable to make payments or withdraw cash. Small businesses have been left without the basic banking services necessary to run their businesses.

While completely uninterrupted access to banking services is not achievable, prolonged IT failures should not be tolerated. We believe the current level and frequency of disruption and consumer harm is unacceptable. Nevertheless, we realise and accept that some IT failure is inevitable. The Regulators must make plain to financial services firms what their tolerance levels for failure are. It is crucial that the Regulators must not allow firms to set their own tolerance levels for disruption too high.

It is essential that firms, and individuals within firms, are held to account for their failures, and we welcome the focus on accountability that has been brought to bear by the Senior Managers Regime. However, so far, there have been no successful enforcement cases under the Senior Managers Regime following IT failures, and we are concerned that this is evidence of an ineffective enforcement regime. The Regulators must consider if there are any barriers to its effective operation.

The Senior Managers Regime does not apply to Financial Market Infrastructure (FMI), for example payment systems. Disruption at FMI firms can affect customers as significantly as disruption within their own providers. The Government should therefore expand the Senior Managers Regime to include FMI firms supervised by the Bank of England, to ensure senior individuals in FMI firms are also accountable.

In their supervision of operational resilience, the Regulators need to draw on expert and practitioner experience. In recent years the Regulators have increased their resources dedicated to operational resilience, but they must do more. If necessary, they should increase industry levies to fund the experts they need.

Many services, such as Financial Market Infrastructure and technology, are provided by third parties. If one of the large third-party providers were to fail, it could potentially affect not just consumer access, but the stability of the financial system itself.

The provision of cloud services to financial services sector firms is highly concentrated. The services provided are often critical. The case for their regulation is therefore overwhelming and the Committee urges the Government to consider how best to regulate cloud service providers.

# Introduction

1. The Treasury Committee launched its *IT failures in the financial services sector* inquiry on 23 November 2018. It followed a series of high-profile service disruptions within the financial services sector, most notably the TSB IT migration in 2018. Issues following the migration caused significant disruption to customers for a prolonged period of time, and we have an ongoing inquiry into *Service Disruption at TSB*[1]. There have also been many other incidents, including those at Visa and Barclays.

2. Previously, in the wake of significant incidents we had routinely written to the affected firms to seek further information about the incident in question, typically: the root cause, the scale of the incident, the firm's response, and any arrangements for customer compensation. While we may continue this practice in the future, this inquiry provided an opportunity to take a more holistic approach, looking 'under the bonnet' of the financial services sector to examine why operational incidents were becoming more frequent, how firms should have guarded against and responded to them, and the role of the Regulators in preventing and mitigating the impact of incidents through their rule books and their operational policies.

3. We held the following oral evidence sessions:

- **9 July 2019: A roundtable discussion with** Simon Chard, Financial Services Partner, PwC; Sarah Isted, Financial Services Risk and Regulation, PwC; Marcus Scott, Chief Operating Officer, TheCityUK.
- **17 July 2019: Financial services sector firms**: Graham Bastin, Head of Operational Resilience, Barclays; Anne Boden MBE, Chief Executive Officer, Starling Bank; Ian Lundberg, Chief Officer, Senior Vice President, Client Services Europe, Visa.
- **24 July 2019: Financial services sector regulators:** Alison Barker, Director of Specialist Supervision, FCA; Lyndon Nelson, Deputy Chief Executive Officer and Executive Director for Regulatory Operations and Supervisory Risk Specialists, PRA; David Bailey, Executive Director for Financial Market Infrastructure, Bank of England.

4. We would like to thank all those who provided written and oral evidence during this inquiry.

5. We were assisted in this inquiry by Gareth Lewis as our specialist adviser.[2] We are grateful for his contribution to this inquiry.

1 Treasury Committee, Service Disruption at TSB Inquiry, accessed 22/10/2019

2 Gareth Lewis has declared interests in relation to his work as a Specialist Adviser on this inquiry as follows: appearing on an Amazon Web Services conference panel, and potential consulting work for Google, Cutover and an independent consulting house.

# 1 IT incidents

## The shift to digital services

6. There has been an increasing demand for digital services in the financial services sector. Research by UK Finance found that 71 per cent of UK adults used online banking in 2017, and that this trend has been increasing.[3] At the same time, the number of high-street bank branches has been falling, with a 17 per cent reduction in the number of branches between 2012 and 2018.[4] The Bank of England, Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) (hereafter, "the Regulators"), explained that "customer and market participant expectations about the availability of financial services have changed dramatically, with 24-hour access to services often expected."[5] So when customers' access to financial services is disrupted, and in particular to banking and payments services, it causes significant concern.

7. This change in customer demand is matched with an ever-increasing use of technology by financial services firms to deliver their products and services. The Regulators explained that "to meet these [customer] demands, firms have turned to technology to improve their offered services, and we have recently seen the rise of different business models, for example digitally-native banks based on smartphone apps".[6]

8. Increasing use of technology can reduce costs for financial services sector firms and improve their resilience. PwC explained that:

> Broader technological innovation also has the potential to improve the overall resilience of financial services. [ … ] The greater diversity in accessing services provided by technology, means consumers have more options should one channel be impaired. FinTech solutions also have the potential to significantly improve operational efficiency.[7]

9. However, new technology and innovation can also create risks. PwC explained that:

> The financial services sector is on the whole, becoming more complex [ … ] and large financial services firms are providing, in some cases, thousands of services to clients with a very significant amount of operational infrastructure required to support. [ … ] Increased use of technology creates more points of failure than was previously the case under less diverse delivery models.[8]

10. **There has been a shift in the way that customers access their financial services, with an increasing number of customers using digital services. As customers come to rely more heavily on digital channels, and given that many high-street branches are closing, the resilience and availability of digital channels is being brought into sharper focus. Given these exacting expectations, it is likely that even brief service disruptions may cause significant concern among consumers.**

3 UK Finance, The Way We Bank Now 2018, May 2018
4 Bank branch and ATM statistics, CBP08570, House of Commons Library, May 2019
5 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
6 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
7 PwC (OPR0008)
8 PwC (OPR0008)

11. **Financial services sector firms are increasingly utilising technology to improve their services. This can have efficiency and resilience benefits yet can also increase the complexity and risk in firms' IT architectures. While customers may benefit from new features or digital services, they also suffer when IT failures occur.**

## The increasing focus on operational resilience

12. The Regulators explained that "A resilient financial system is one that can absorb shocks rather than contribute to them", and defined operational resilience as "the ability to prevent, adapt and respond to, and recover and learn from, technology, cyber-related and any other operational incidents".[9] Improved operational resilience is a way firms can reduce the number and impact of IT or operational incidents.

13. In the past, the industry and Regulators have focused on financial and conduct over operational risks. Whilst there has been a focus on business continuity (for example flood or power issues) as an operational risk in the recent past, the number and severity of IT related incidents has resulted in a refocusing of efforts in this area. Operational resilience is now considered a priority issue, both from a regulatory perspective and within the financial services sector. Barclays described the issue of disruptions for customers as one of its "greatest priorities",[10] and Visa claimed that "There has never been a more important time for the financial services sector to enhance its current approach to operational resilience".[11] In oral evidence to us in January 2019, Andrew Bailey, Chief Executive of the FCA, explained that:

> As we have hopefully mitigated some of the key risks of the financial crisis, the relative standing of operational risk, both growing as a risk in its own right, and as we have mitigated other things, has come up.[12]

14. The Regulators are moving towards closer supervision of operational risks and resilience. In July 2018 the Regulators jointly published a Discussion Paper, 'Building the UK financial sector's operational resilience',[13] which was a milestone. The Discussion Paper set out the premise that "it would be neither possible nor an efficient use of resources to attempt to make every component of an organisation completely resilient to operational disruption".[14] The Regulators' Discussion Paper "suggests that firms and FMIs [Financial Market Infrastructure] should map their important business services to underlying systems and processes that support their delivery, and identify their tolerance for disruption under the assumption that disruption will occur (impact tolerance)".[15]

Impact tolerance will be discussed further in Chapter 2.

15. The focus on operational resilience will probably continue. PwC claims that:

> There is more to be done achieve the desired level of operational resilience [ … ] a range of developments impacting the financial services sector, such

9 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
10 Barclays (OPR0009)
11 Visa (OPR0007)
12 Treasury Committee: Oral evidence: The work of the Financial Conduct Authority, HC 475, 15 January 2019 [Q416]
13 Discussion Paper: Building the UK financial sector's operational resilience, Bank of England, PRA, FCA. July 2018
14 Discussion Paper: Building the UK financial sector's operational resilience, Bank of England, PRA, FCA. July 2018
15 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)

> as increased complexity, interconnectedness, third party dependencies and initiatives such as open banking mean we believe operational resilience will remain a significant challenge over the medium term.[16]

16. **We welcome the increasing focus on operational resilience among both industry and the Regulators. Further regulatory intervention is needed to improve the operational resilience of the financial services sector, as was required over the past decade for its financial resilience. The Regulators must give as much prominence to regulating operational risk and resilience as they currently afford to regulating prudential and conduct risks.**

## The prevalence of IT incidents

### *The number of IT incidents*

17. IT failures, or incidents (used interchangeably), within the financial services sector appear to be becoming more common. Over the past 18 months there have been major incidents at TSB and Visa, along with a litany of incidents at other firms. This increasing trend is recognised by the FCA, which stated in 2018 that "outages in the financial services sector are becoming more frequent and publicised" and that "the number of incidents reported to the FCA has increased by 187 per cent in the past year".[17] Furthermore, the Regulators reported that 65 per cent of the incidents notified to it in 2018 were from the retail banking sector, including payment services firms, over five times the next highest sector, wholesale financial markets.[18]

18. A number of firms qualified the figures for the increase in the number of IT incidents in evidence to us. Many incidents experienced by firms are relatively minor, and often do not impact customers. Anne Boden, CEO of Starling Bank, explained that "There are big incidents that hit the press and everybody talks about [ … ] but all banks have small things."[19] We also heard that some firms have experienced a reduction in the number of IT incidents. For example, Barclays explained that "operational incidents across Barclays due to technology issues are becoming less frequent year-on-year, with a 15 per cent reduction (2016 to 2017) and a further 13 per cent reduction (2017 to 2018)".[20] Similarly, RBS said that the number of the most critical incidents, as defined by customer impact, had reduced from 318 in 2014, to 19 in 2018.[21]

### *The impact of IT incidents*

19. IT incidents in financial services sector firms can have a significant impact on customers, and recent high-profile IT failures have demonstrated how significant and widespread this impact can be. TSB explained that customers "are increasingly using digital services to meet their everyday banking needs. This means that when banks have technical problems more of their customers are likely to be impacted and be aware of the

16 PwC (OPR0008)
17 FCA, Cyber and Technology Resilience: Themes from cross-sector survey 2017–18, November 2018
18 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
19 Q98
20 Barclays (OPR0009)
21 RBS (OPR0004)

issue than ever before".[22] PwC noted that "in the majority of cases customer inconvenience and distress is the main impact, but extreme or wide ranging impacts from major outages also result in financial detriment to consumers".[23]

20. Alison Barker, Director of Specialist Supervision at the FCA, gave examples of the impact on customers.

> The types of harms that we have seen include the Tesco Bank incident that affected Tesco customers, and we have issued a final notice on that. People were recompensed in the end, but they lost money over that weekend, which is a very stressful situation for consumers to face. Likewise, with TSB people could not access accounts and pay bills. [ … ] I would not class them as inconvenience; people really did suffer.[24]

During oral evidence sessions for our *Service Disruption at TSB* inquiry, cases of customer impact raised by Members included the following:

- I have not been able to access my account for two weeks now. I have fluctuating balances, no idea which direct debits and standing orders have been paid, and my data has been compromised. [ … ] I have been unable to use my debit card for purchases as, for a week, my balance was zero. This meant I was unable to withdraw cash.[25]

- She told me how she sent five emails without response, she spent five hours on the phone to you at 30p per minute [ … ] She relies on pension credit. Her account is now in debit. She said, "I am at my wit's end, no electricity or gas, running on emergency, which is about to be cut off. Help please".[26]

- Unfortunately, after nearly two weeks, we will not be able to submit our formal mortgage application as the lender—thankfully not TSB—has requested three months of bank statements. We are still unable to download our bank statements [ … ] "We are now faced with the possibility we could miss out on buying the house our family needs".[27]

- [A Constituent] who runs a small business and employs eight people, contacted me to say, "My balance is showing £0 when I know there is more than that in there. My standing order has not been paid [ … ] not to mention staff also not being paid."[28]

21. An important consideration for firms during an IT incident, is the effect on vulnerable customers. In written evidence, the Regulators explained that:

> The FCA expects firms to consider the needs of vulnerable customers by providing assistance on a proactive basis, and considering whether it

22 TSB Bank (OPR0010)
23 PwC (OPR0008)
24 Q261
25 Treasury Committee: Oral evidence: Service Disruption at TSB, HC 1009, 2 May 2018 [Q3]
26 Treasury Committee: Oral evidence: Service Disruption at TSB, HC 1009, 2 May 2018 [Q127]
27 Treasury Committee: Oral evidence: Service Disruption at TSB, HC 1009, 2 May 2018 [Q5]
28 Treasury Committee: Oral evidence: Service Disruption at TSB, HC 1009, 2 May 2018 [Q134]

> is possible to prioritise recovery in a way that restores services on which vulnerable customers may depend, such as access to cash, pre-paid cards or benefits payments.[29]

22. There may also be second order impacts of IT incidents. Customers may be exposed to further threats. For example, PwC explained that "Operational incidents may also be a trigger for a cyber-attack / cyber fraud where consumers' data and money are clearly vulnerable."[30] There may also be contagion to other providers' customers. PwC highlighted that "an operational incident in one financial institution may mean another that is reliant on it for critical services (e.g. access to payment systems) can no longer serve its own customers".[31]

23. The impact of IT incidents may go beyond consumer harm, to undermine the viability of a firm, or financial stability. Lyndon Nelson, Deputy Chief Executive Officer and Executive Director for Regulatory Operations and Supervisory Risk Specialists, PRA, outlined the potential levels of impact of an IT incident:

> At the lowest end, it is essentially the ability of management to run their bank or their insurance company if the IT system is gone. If the IT system continues to cause a problem, then we may be getting into the safety and soundness of firms [ … ] Then, fundamentally, it could also then cause either a financial stability or systemic issue if it then has knock-on consequences.[32]

This is not theoretical. There have been cases where the viability of firms has been questioned. Speaking about the IT failure at TSB, Sam Woods, Deputy Governor Prudential Regulation and Chief Executive Officer of the PRA, told us that compared to the FCA's objectives (for example individual consumer protection), "[T]there is a higher bar for it to get to a safety and soundness issue for us in the PRA. [The TSB incident] certainly met that bar".[33]

24. **Operational incidents in the financial services sector are increasing in frequency. While we recognise that many incidents have limited customer impact, recent high-profile cases have shown the harm to customers that can be caused. The impact of IT incidents can range from inconvenience to customers through to customer harm, and on to matters of a firm's viability or financial stability. Financial services providers must treat their ability to manage and prevent incidents with a level of seriousness appropriate to the significant impact when incidents occur.**

## Incident Reporting

25. The Regulators collect data on incidents reported by financial services sector firms. Barclays highlighted one form of reporting, explaining that "Under the Second Payment Services Directive ('PSD2'), we report all incidents above a certain threshold, which impact any Payment Account [ … ] to the FCA".[34] Yet wider reporting of incidents is partly

29 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
30 PwC (OPR0008)
31 PwC (OPR0008)
32 Q213
33 Treasury Committee: Oral Evidence: The work of the Prudential Regulation Authority, HC 704, 23 January 2019 [Q168]
34 Barclays (OPR0009)

determined by what firms themselves record as incidents. The Center for Evidence Based Management[35] explained that "the systems and processes for recording incidents varies widely" and where systems and processes are poor, "incidents may not be consistently recorded and information about the causes of those incidents is unclear or wrong".[36]

26. The Regulators acknowledged there are issues with reporting. Alison Barker, FCA, explained that: "We still think that we have overall under-reporting. When you think about it across the financial sector, if 65 per cent of it is retail banks, we have under-reporting in other sectors."[37]

27. The Center for Evidence Based Management highlighted the improvements needed to incident reporting. They explained that "Developing a better evidence-based understanding of this area requires more analysis but also better data and more consistent collection of data on failures."[38]

28. Currently some incident data is published, for example incidents affecting current accounts.[39] Lyndon Nelson, PRA, explained that "There is standardised reporting on technology, which we got through the industry, so they do currently publish some of that. I am sure it could go further."[40] Furthermore, David Bailey, Executive Director for Financial Market Infrastructure at the Bank of England, added that "in our annual report every year, we publish the operational availability of the systems that we supervise".[41] However he cautioned that "It can be helpful if consumers can compare availability and functionality, but if you have cyber incidents, you do not want to publicly reveal vulnerabilities in the system".[42]

29. Some have argued for greater transparency of service availability and incident data. The ITRS Group[43] suggested that:

> Organisations should be made to publish the availability and performance targets they expect of each application, and then publish what they are actually achieving. This would automatically highlight where they are falling short of their targets. (Availability is often specified, but performance less so).[44]

30. **The lack of consistent and accurate recording of data on operational incidents is concerning. The Regulators should conduct an exercise to assess the accuracy and consistency of incident reporting. If necessary, the Regulators should clarify standards, guidance and definitions for industry on what incidents firms should both record and report. They should also consider the need to expand current reporting requirements, to cover broader services provided by firms. Higher quality incident reporting will serve to improve the ability of both the Regulators and industry to identify the biggest risks to the operational resilience of the sector.**

35 A non-profit organisation that promotes evidence-based practice in the field of management and leadership.
36 Center for Evidence-Based Management (OPR0003)
37 Q234
38 Center for Evidence-Based Management (OPR0003)
39 FCA, FCA mandated and voluntary information on current account services, accessed 20 September 2019
40 Q236
41 Q236
42 Q236
43 A provider of production software tools to financial institutions.
44 ITRS Group (OPR0001)

31. **It is very difficult for customers to determine which financial services providers are operationally resilient, and to make clear comparisons across the industry. The Regulators should require clearer and more prominent public reporting to empower customers to make informed decisions regarding which provider they use, and to increase firms' focus on operational resilience. Where firms already publish incident information, this should be given greater prominence in information made available to prospective and existing customers, such as that given to wait times and complaints, which are visibly displayed in bank branches for all to see.**

# 2 The role of the Regulators

## Regulatory approach

32. Financial services sector firms are regulated by a number of different bodies. For the purpose of this inquiry we heard oral evidence from the Bank of England, FCA, and PRA. However, various other bodies have also been responsible for the regulation of the sector, including the Payments Systems Regulator (PSR), and other cross-cutting bodies such as the Information Commissioner (ICO). Marcus Scott, Chief Operating Officer, TheCityUK, told us that "Many of our member firms have up to nine regulators [ … ] and that is quite complex."[45]

33. There is a role for the financial services Regulators in specifically reducing both the number and impact of IT failures in the financial services sector. The Regulators told us:

> While we expect firms and FMIs to manage the risks arising from use of technology, we also accept that we have an important role in strengthening the operational resilience of the financial system and in helping to reduce the impact of operational incidents when they occur.[46]

34. The role of the Regulators in operational resilience more generally is still developing. They explained that:

> Compared to our frameworks for capital, liquidity, OCIR [Operational Continuity in Resolution], and senior management accountability, the regulatory framework for operational resilience has scope to be developed. We are therefore considering how we might supplement existing requirements.[47]

Charles Randall, Chair of the FCA, commented that:

> Technology change means major new risks to our objectives can develop more rapidly than ever. These risks increasingly come from beyond large authorised firms and regulated products, such as when scammers use the internet to target victims. We must continue to develop our own use of technology and our supervision and enforcement capabilities to respond rapidly where our remit allows.[48]

35. The Regulators published a joint Discussion Paper (DP), 'Building the UK financial sector's operational resilience', in July 2018. The Regulators' "collaboration on this paper reflects the interconnectedness of the financial system and a shared interest in the opportunities and threats posed by developments in technology".[49] In written evidence they explained the purpose of the DP.

45 Q76
46 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
47 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
48 FCA, Annual Report and Accounts 2018/19, HC (2017–19) 2415, 9 July 2019
49 Bank of England, Prudential Regulation Authority, and Financial Conduct Authority, Discussion Paper, Building the UK financial sector's operational resilience, July 2018.

> The DP reminded firms and FMIs of existing requirements relating to operational resilience, and suggested ways of strengthening operational resilience and that firms and FMIs could:
>
> - assume severe disruptive events will happen and plan on that basis;
> - focus on the wider impact on end users of disruption to the supply of products and services ("business services"), not just on system recovery;
> - set impact tolerances and use scenario testing as a way of enhancing existing arrangements; and
> - identify resilience gaps, and invest in the ability to maintain continuity of supply of products and services.[50]

36. The proposed approach in the DP was supported by many respondents. Graham Bastin, Head of Operational Resilience at Barclays, commented that "The thing that we really welcomed was the customer lens that they were looking at".[51] Ian Lundberg, Chief Officer, Senior Vice President, Client Services Europe, Visa, told us that "Absolutely it resonated with us. [ … ] We welcomed [ … ] the idea of looking at the payments ecosystem in total, and the interdependencies between us all."[52]

37. Lyndon Nelson, Deputy Chief Executive Officer and Executive Director for Regulatory Operations and Supervisory Risk Specialists, PRA, commented that the DP:

> Has received a lot of positive comment [ … ] The main constructive comment we have had back is that the firms are trying to work out how operational resilience fits in with some of the other requirements that the regulators already have on operational continuity and resolution, or in terms of operational risk and the capital they might hold against that.[53]

38. The Regulators are currently considering responses to the July 2018 DP. Lyndon Nelson, PRA, explained that: "we intend to come back in about October with a consultation paper. I cannot be too precise on the date".[54] Consultation papers set out draft policy, and the Regulators seek responses before policy is finalised.

39. When asked whether implementing the proposed approach would reduce the disruptions that financial services customers experience, Lyndon Nelson remarked that "You would hope that would be the outcome of the policy. [ … ] consumers and constituents will see something very different. They will get their service—it may be slightly clunky or slightly late, but it certainly will not be at the level of disruption that we have had so far".[55]

40. **Regulatory supervision of operational resilience may require a different approach to that currently adopted for of prudential and conduct risks. While the Regulators are still developing their approach to supervising firms' operational resilience, there is an**

50 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
51 Q89
52 Q92
53 Q215
54 Q215
55 Qq221–222

**opportunity to consider whether current practice is the best model of supervision for this risk. The approach to supervision must be agile, and be able to adapt as operational resilience risks change, including those introduced as new technologies are adopted.**

41. **It is promising to hear that firms are broadly supportive of the approach taken by the Regulators in their July 2018 Discussion Paper. We encourage the Regulators to continue to engage with industry when developing operational resilience requirements further, to ensure that these are practical and effective. The Regulators should publish further guidance for firms on how their different operational resilience requirements interact, and their expectations of firms when implementing them. This should be done as the policy is developed, and not after firms have begun implementation.**

42. **The PRA has given us assurances that if the approach in the Discussion Paper is implemented, the level of disruption will fall. This remains to be seen. The Regulators should set out publicly how they intend to measure the effectiveness of future policy in achieving this aim. We will continue to scrutinise the progress made by the Regulators to improve the sector's operational resilience as part of its regular work.**

43. **Given the importance of operational resilience, and the fast-moving nature of the risks, we urge the Regulators to prioritise the publication of their final policy and guidance. In responding to this report, the Regulators should set out their upcoming timetable for publication.**

### *Impact tolerances*

44. The Regulators said they were "considering ways of strengthening the operational resilience of the financial sector, and one possible enhancement is for firms and FMIs to set impact tolerances".[56] This is motivated by the premise in the DP that: "it would be neither possible nor an efficient use of resources to attempt to make every component of an organisation completely resilient to operational disruption".[57] The Regulators set out how this could be applied:

- The FPC [Financial Policy Committee] has agreed that it will set impact tolerances for vital services that the financial system provides to the real economy.
- The Authorities consider that firms and FMIs should be responsible for determining their own tolerance levels, but there is a role for the Authorities to challenge these tolerances.[58]

Firms would be expected to then "test their ability to stay within these tolerances through severe but plausible scenarios".[59]

45. This raises the question of where firms might set such tolerances. PwC argued that impact tolerances will be guided by customer demand, economic and societal importance

56 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012) The Regulators in written evidence define tolerances: "An impact tolerance describes a firm's or FMI's tolerance for disruption to a particular business service, under the assumption that disruption to the systems and processes supporting that service will occur. Impact tolerance is expressed by reference to specific outcomes and metrics. Such metrics could include the maximum tolerable duration or volume of disruption, a measure of data integrity or the number of customers affected."

57 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)

58 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)

59 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)

of the service, and substitutability.[60] RBS "believes the regulators have a role to play by identifying and providing guidance on specific service impact tolerances they would expect to see".[61] Also, the impact of an incident may differ when viewed with the different regulatory lenses of consumer harm, safety and soundness of firms and financial stability, so the impact tolerances may have to vary based on these objectives.

46. A similar approach to setting impact tolerances is already employed for FMI. David Bailey, Executive Director for Financial Market Infrastructure at the Bank of England, explained that "all FMIs should have plans in place to be able to recover from an outage within two hours; but certainly to ensure that all payments are settled by the end of the intended value date[62]."[63]

47. **We accept that completely uninterrupted access to banking services is not achievable, yet prolonged or regular IT failures are unacceptable. Recent high-profile incidents have caused significant harm to consumers and businesses, and we regard the current level of disruption from incidents as too high. We understand that impact tolerance will vary based on the regulatory objective in question (for example preventing consumer harm); the consumer group; and the importance of the product or service. Nevertheless, it is crucial that the Regulators maintain a very low tolerance for disruption to the most important services.**

48. **We recommend that the Regulators provide clear guidance to firms on their expectations around the definition of business services and the level of impact tolerances. While the Regulators' current expectation is that firms would set their own impact tolerances, ultimately firms must not be allowed to set tolerance for disruption too high. The Regulators must prohibit this to avoid lax operational resilience, which could in turn lead to a financial stability crisis or widespread consumer harm.**

49. **The Regulators suggested in their Discussion Paper that firms would be expected to meet their impact tolerances in severe but plausible scenarios. We are concerned what the impact would be of an IT failure in scenarios where firms are not expected to meet their impact tolerance. In response to this report, the Regulators should describe extreme scenarios under which firms would not be expected to meet their own impact tolerance, and what the regulatory response would be to protect consumers from harm in such scenarios.**

## The Regulators' incident management

50. The Regulators explained that they have a role "in helping to reduce the impact of operational incidents when they occur".[64] Where the Regulators need to coordinate during an incident, they can use the Authorities Response Framework (ARF). The Regulators explained that the ARF is used for serious incidents by the Regulators and the Treasury

60 PwC (OPR0008)
61 RBS (OPR0004)
62 The value date is "the day on which the payment, transfer instruction, or other obligation is due and the associated funds and securities are typically available to the receiving participant". BIS-IOSCO, Principles for financial market infrastructures, April 2012.
63 Q220
64 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)

but can also be expanded to include other agencies. They explain that the "ARF provides an important co-ordination function for the authorities [ … ]. It allows intelligence to be pooled and common issues to be discussed and approaches agreed".[65]

51. Alison Barker, FCA, explained the role of the FCA during an incident:

> As the first responder, we will establish the facts of what is happening and establish the key point of contact within the institution. We will inevitably contact the [Bank of England] and the Treasury. There will then be the co-ordinating authorities call, which will have a set agenda around ensuring that we know what has happened, that we understand the impacts, that we know who is doing what at the firm, that we are clear that the firm understands what it has going on and what level of response we need to have.[66]

52. The ARF was initiated by the FCA after the TSB migration. The FCA in a letter to us, set out its work following the migration:

> The FCA has continuously engaged with TSB since 20 April. This includes on-site visits to TSB's Head Office and other TSB sites to observe progress and monitor its approach to identifying and resolving the issues [ … ]. We also review daily management information from TSB to ensure we understand the steps TSB is taking to remedy the situation, and challenge TSB where needed.[67]

53. The FCA also has staff on standby, should incidents occur. Alison Barker, FCA, highlighted that "we will be monitoring things and we have teams on call over every single weekend and over bank holidays to monitor incidents".[68] She reassured us that the FCA have estimated that they can run at least 10 incidents at the same time.[69]

54. Andrew Bailey, Chief Executive of the FCA, in evidence to our *Service disruption at TSB* inquiry, accepted that "there is a lot still to learn" about the TSB case.[70] More broadly, in relation to both the TSB and Visa incidents, he said that the FCA "seek to learn from all these incidents but none of us can give [the Committee] an assurance that these things will never happen again".[71]

55. **The Regulators have a vital role during significant incidents. While the responsibility for managing incidents rests with financial services firms, where a firm's response proves ineffective and there is a risk to the Regulators' objectives, the Regulators must be willing and able to take appropriate action to mitigate risks to their objectives.**

65 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
66 Q251
67 Treasury Committee, Correspondence from the Chief Executive of the FCA to Chair, 30 May 2018
68 Q252
69 Q258
70 Treasury Committee: Oral Evidence: Service Disruption at TSB, HC 1009, 6 June 2018 [Q234]
71 Treasury Committee: Oral Evidence: Service Disruption at TSB, HC 1009, 6 June 2018 [Q234]

## Creating and enforcing accountability

### *Individual accountability*

56. One way to create an environment whereby firms focus on their operational resilience is to clearly identify who is responsible for such resilience within a firm. The Regulators explained that they require:

> Specified types of firms to appoint managers, approved by the regulator, who are responsible for specific areas and for each of the firms' business functions and activities. The Senior Management Function (SMF) 24 is the Chief Operations function, with responsibility for a firm's internal operations and technology. SMF24 currently applies to banks, dual-regulated investment firms and building societies, and is being extended to 'enhanced' FCA solo regulated firms from December 2019. We expect senior management to be responsible for their firms' proactive operational resilience as well as when incidents occur.[72]

57. Lyndon Nelson, PRA, explained that "the SMR bites even at pre-enforcement. When we are talking about some of these big programmes [ … ], one of the big things that the supervisor does is make sure who is responsible".[73] Graham Bastin, Barclays, commented that the Senior Managers Regime "has sharpened the focus. We have the governance structures [ … ] where it is very clear where the accountability for operational technology resilience lies."[74]

58. In the Treasury Committee's *Work of the PRA* inquiry oral evidence session in July 2018, we asked what penalties would be expected if firms did not meet impact tolerances. Sam Woods, Deputy Governor Prudential Regulation and Chief Executive Officer of the PRA, told us that "We have the full range of our regime to deploy, so we do not need a new penalty regime to attach to this".[75] Similarly, during oral evidence to us on 15 January 2019, Andrew Bailey, FCA, commented on the possible sanctions the FCA can use when IT outages occur as follows:

> I will say two things on that. First, it feeds through into the remuneration policy, so we expect banks' policies on variable remuneration to reflect operational reliance. [ … ] If we find it is not, we will act, because it is important that it is. That goes to the second point, which is that it is a responsibility under the senior managers regime.[76]

59. However, the Senior Managers Regime does not apply to all firms. David Bailey, Bank of England, told us that "We do not have that same senior managers regime applicable to financial market infrastructure. [ … ] It is an area where accountability in the firms that I

72 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
73 Q303
74 Q189
75 Treasury Committee: Oral evidence: The work of the Prudential Regulation Authority, HC 704, 11 July 2018 [Q116]
76 Treasury Committee: Oral evidence: The work of the Financial Conduct Authority, HC475,15 January 2019 [Q418]

supervise could be enhanced".[77] The Financial Policy Committee in its July 2019 Financial Stability Report noted "that there is a strong case for extending the Senior Managers and Certification Regime to FMIs".[78]

### *Firm-level enforcement*

60. In addition to individuals, the Regulators can also impose sanctions on financial services sector firms. The Regulators gave examples of where they have held financial services sector firms to account.

> As can be evidenced from the previously mentioned enforcement action we took against RBS Group for its system failures in 2012, the recent financial penalty imposed on Tesco Personal Finance plc for failing to protect its personal current account holders against a cyber-attack in 2016, and the current investigations of TSB and Equifax, we have continued to use our relevant powers to hold firms to account when they fail to comply with our requirements in relation to serious operational incidents.[79]

61. Yet, as we have seen following TSB's IT failure in April 2018, investigating in the event of failures is a slow process. At the time of publication, neither the report commissioned by TSB (the 'Slaughter and May' report) nor the regulatory investigation, have concluded.

62. **Holding individuals and firms to account when IT failures happen is essential, not only to prevent individuals making the same mistakes again, but also to focus the attention of senior management on the risk of incidents and incident management. The Regulators must use the enforcement tools at their disposal to hold individuals and firms to account for their role in IT failures and poor operational resilience. The regulatory mechanisms to ensure accountability for failures must have teeth, and equally as importantly, be seen to have teeth.**

63. **We support the increasing focus on accountability and responsibility brought about by the Senior Managers Regime. However, we have yet to see a successful enforcement case under the Regime against an individual following an IT failure. We are concerned that this may be evidence of an ineffective regime to support enforcement. We accept that not all IT failures would result in enforcement action by the Regulators. However, the Regulators should consider whether there are any barriers to the effective operation of the regime, and whether any changes to the requirements or standards are necessary to ensure that individuals can be held accountable. If future incidents continue to occur without any sanction to individuals under the Regime, us as a Committee, and Parliament, will have to consider whether the powers it has given to the Regulators are fit for purpose.**

64. **The length of time it has taken for customers and Parliament to be provided with a comprehensive independent account of what happened during the TSB IT failure, who was at fault, and why the recovery process took so long is unacceptable. The Regulators**

77 Q270
78 Bank of England, Financial Stability Report, July 2019
79 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)

**must provide a full report of their investigation into the incident in their response to this report, or failing this, provide us with an update on timelines and issue the full report as soon as possible.**

65. **Remuneration structures throughout firms should reflect the importance of operational resilience. When appropriately used, these structures can help improve the prominence of operational resilience, and the requisite level of attention to preventing IT failures. If the Regulators observe that firms are not adequately taking operational performance into account when determining remuneration for senior staff within financial services firms, they must intervene.**

66. **As we have seen from recent examples, such as the Visa outage in 2018, operational incidents at Financial Market Infrastructure (FMI) firms can have as much effect on customers as bank incidents. It is therefore vital that senior management at FMI firms are accountable for their management of operational incidents. There does not appear to be any justification for keeping FMI outside of the Senior Managers Regime. The Government should expand the Senior Managers Regime to include FMI supervised by the Bank of England.**

## Regulatory burden and coordination

67. If regulation places an excessive burden on firms, this could harm their resilience. UK Finance argued that legislative and regulatory requirements underpin more of firms' change than previously.[80] Similarly, Barclays told us that:

> A number of major technology change programmes have been mandated by Government or regulators, to transform the financial services sector and provide services digitally [ … ] many of these mandated reforms are significant change programmes with implementation often required simultaneously. This can sometimes create competing requirements or conflicting demand that may generate technology and operational risk.[81]

Conversely, Anne Boden, CEO of Starling Bank, commented that "on regulatory burden, we do not have a significant burden from regulatory changes, because we have new software and new procedures".[82]

68. In January 2019, we questioned Sam Woods, PRA, on whether regulators were creating risk through excessive demands. He responded that:

> As is often the case, members of some financial institutions may be expressing themselves more vividly than the facts support. The easiest way to express it is that a good chunk, say 20 per cent, of those numbers [on incidents] is cyber. I can assure you that the PRA is not launching cyberattacks on any financial institution. [ … ] There is a grain of truth in what you have been told, in the sense that there is a lot of change.[83]

80 UK Finance (OPR0005)
81 Barclays (OPR0009)
82 Q143
83 Treasury Committee: Oral evidence: The work of the Prudential Regulation Authority, HC704, 23 January 2019 [Q161]

69. Furthermore, Lyndon Nelson, PRA, explained that the cumulative burden of regulatory change on firms "is always difficult to assess". In relation to this burden, he commented that "I would not accept it domestically, but for the global firms, there is no question but they have been hit by a variety of different standards". [84]

70. Yet firms have raised this risk with the Regulators. Graham Bastin, Barclays, told us that:

> When we are executing the volume of change that I referenced earlier[85] and we can see there are collisions or compression on that change schedule, we are very happy to push back on where those changes are coming from and to explain the consequences, or the unintended consequences.[86]

71. The coordination between the Regulators on their July 2018 Discussion Paper was welcomed by a number of firms. RBS "welcomes the open, challenging and collaborative approach taken by the regulators".[87] Yet we also heard that regulatory demands could be better coordinated. UK Finance commented that the risks of regulatory change are "exacerbated by an absence of coordination between public authorities over substance, timing and prioritisation".[88] Also, Graham Bastin, Barclays, commented that:

> I think the discussion papers stimulated a conversation around something called air traffic control. If we could see greater coalition and co-ordination across the different regulators, not just in the UK but internationally, that would be super-helpful.[89]

72. In his Mansion House speech in June 2019, the then Chancellor announced "a major, long-term review into the future of our regulatory framework", and commented that "I have heard the message from business that there is a critical need for greater "air traffic control" to manage the cumulative impact of regulatory change emanating from different sources".[90] The Treasury launched a call for evidence on regulatory coordination in July 2019 which forms the first part of this review. This "looks at how government and the regulators work together to coordinate their activities to ensure the best outcomes for the financial services sector, consumers of financial services, and the UK as a whole."[91]

73. Regarding 'air traffic control', Alison Barker, Director of Specialist Supervision at the FCA, commented that:

> The chief executives of our organisations, the CMA and the Payment Systems Regulator are all very committed. There has been a discussion with the Chancellor. They will take forward what ideas come through the call for input. There is an idea that there will be some consultation or wider discussion later in the year.[92]

84 Q230
85 25,000 changes a month. Q200
86 Q200
87 RBS (OPR0004)
88 UK Finance (OPR0005)
89 Q200
90 The Rt Hon Philip Hammond MP, Mansion House dinner speech 2019, 20 June 2019
91 The Treasury, Financial Services Future Regulatory Framework Review, Call for Evidence: Regulatory Coordination, July 2019
92 Q229

74. **Change is one of the biggest causes of operational incidents, and the Regulators are one of the biggest causes of change. It is vital that the Regulators do not inadvertently increase the risk of an operational incident by placing excessive or poorly coordinated requirements on firms. While it is concerning to hear firms criticise a lack of effective regulatory coordination, industry criticism of regulatory requirements must be viewed sceptically, as industry has an incentive to lobby for reduced regulatory burden. The same industry praised the joint approach by the FCA, PRA and Bank of England put forward in their July 2018 Discussion Paper.**

75. **We welcome the then Chancellor's announcement of a review into the future regulatory framework for the financial services sector, and the subsequent call for evidence on regulatory coordination. The Treasury should implement a continuing coordinating forum to assess the cumulative burden of regulatory change, and to facilitate a permanent "air traffic control" in the financial services sector. This would help ensure that the Regulators themselves do not create operational risk through the volume and timing of their regulatory demands.**

## Regulatory resourcing and expertise

76. The Regulators explained their approach to resourcing and staff skills and experience in relation to operational resilience, stating that they:

> Employ experts in both technology and cyber resilience who provide support to front-line supervisors to assess firms' and FMIs' resilience. Many of these experts hold recognised industry qualifications which, to be maintained, require continuous professional development and certification on an annual basis.[93]

Furthermore, the Regulators emphasised their ability to contract external resources. David Bailey, Bank of England, explained that "we make quite extensive use of external resources, so that we can commission expert resources to come into a firm and perform assessments, which adds to the expertise we can draw on".[94]

77. However, we heard that the Regulators need to improve their skills and experience related to operational resilience. PwC explained that "the expertise and experience of operational resilience topics is less widespread in supervisory and policy teams in the PRA and FCA, than more typical prudential and conduct risks."[95] Simon Chard, Financial Services Partner, PwC, added in oral evidence that firms have told them "that they would appreciate being able to have a discussion on those topics and more resource within the regulator to discuss those topics with them".[96]

78. The skills and experience issue was recognised by the Regulators. Lyndon Nelson, PRA, remarked on training supervisory staff, that "we would acknowledge that we have to get the supervisors further up the curve".[97] Also, in oral evidence, the Regulators described the training programmes for supervisory staff.[98] However, in written evidence

93 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
94 Q224
95 PwC (OPR0008)
96 Q78
97 Q225
98 Q226

they wrote that "recruiting and retaining these experts continues to be challenging, given the demand for their skills and the Authorities' resource constraints".[99] Lyndon Nelson, PRA, described some of the challenges that the PRA faces:

> The main constraint, to be honest, is probably a budgetary one. We have a number of other priorities. [ … ] I am happy with the resource settlement that we have got. [ … ] We could go quicker if we had more, but I think it is the right balance.[100]

Alison Barker, FCA, was asked whether salaries were a challenge in recruiting the right people. She explained that "It can be, but we focus on what benefits you get from working at a regulator. People often come to work at a regulator because there is a sense of purpose".[101]

79. Given the need to improve resourcing at the Regulators, PwC suggested that:

> There may need to be consideration as to whether greater resources and more subject matter experts (enhanced through secondments from the private sector where appropriate, or by recruiting more senior advisers with expertise in an operational resilience discipline) assigned to operational resilience may be necessary.[102]

80. **The Regulators have an important role in overseeing and challenging firms' approach to operational resilience and preventing IT incidents. They need the appropriate skills and experience to do so. The Regulators have improved their capability over recent years, yet they must do more. While training programmes may assist the Regulators in building supervisory skills, expert and practitioner experience are also important. We therefore expect the Regulators to increase their capability, particularly at the more senior levels.**

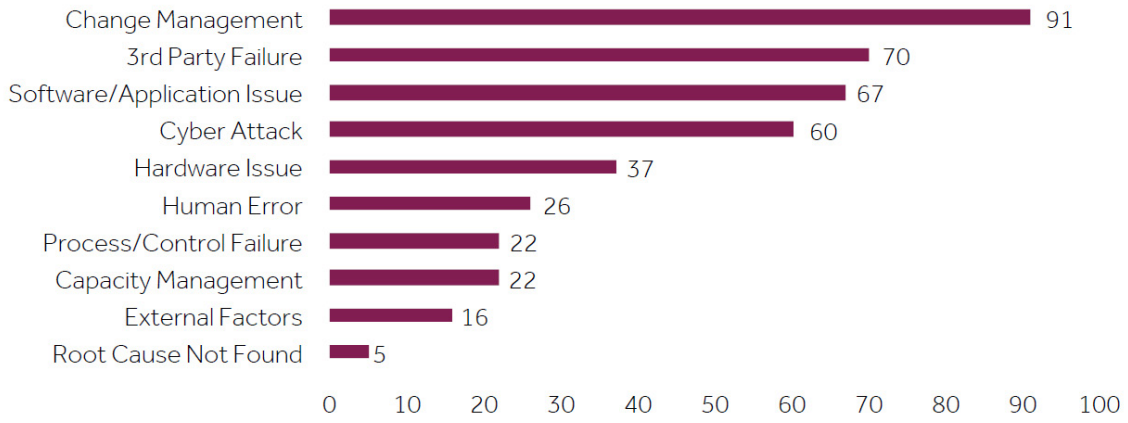
81. **We accept the Regulators' current budgets make hiring staff with skills and experience in operational resilience challenging. The Regulators should increase financial sector levies to ensure they can hire the staff with the expertise and practitioner experience they need. We do not expect to hear after the fact, perhaps in reaction to a major incident, that supervisory resources were inadequate.**

99 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
100 Q226
101 Q227
102 PwC (OPR0008)

# 3 Common causes of IT incidents

82. We took evidence on the common causes of IT incidents in the financial services sector. Many respondents referred to data published by the FCA. The most common root causes of incidents reported to the FCA in the year to September 2018 are shown in the graph below:[103]

**Figure 1: Root Cause Trend: Oct-17 to Sep-18**




Note: There are 186 cases (29% of total incidents) where firms have not yet informed us of the specific root cause of the incident. We remain in discussions with relevant firms to obtain this information.

Some of the common causes are examined in more detail in the following sections. The risks created by legacy systems are covered first as this permeates multiple causes of IT failures.

## Legacy systems

83. Aging architecture, or the use of legacy systems is often referred to as a cause of IT incidents. While some firms described the modern state of their systems, and significant investment in upgrading legacy systems, the Regulators outlined the continuing prevalence of legacy architecture:

> We have observed that legacy systems still support important business services in some firms and FMIs. [ … ] Firms and FMIs have built or procured digital services for their customers which often sit over the top of legacy systems rather than fully replacing them.[104]

Firms were themselves concerned about this risk. The Regulators told us larger firms were concerned about:

> The scale of system obsolescence, and the absence of a common mechanism by which to assess the range of risks (for example, strategy, costs, service availability, security etc.) and therefore to inform mitigation. [105]

103 FCA, Cyber and Technology Resilience: Themes from cross-sector survey 2017–18, November 2018
104 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
105 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)

84. PwC explained that legacy systems can make managing cyber risk particularly difficult:

> One of the challenges with legacy systems is that many mainframe systems were designed before the introduction of the internet. In our experience, it has been problematic for some firms over recent years to ensure that these systems are protected from cyber attacks and that information is secured.[106]

85. Legacy systems can also make change difficult, partly because they are often complex, as their use has evolved over many years. In oral evidence to our *Economic Crime* inquiry, Chris Hemsley, Co-managing Director of the Payment Systems Regulator, explained that the introduction of confirmation of payee would mean that "the individual IT systems all then need to be updated. That in itself, because of the legacy systems and the range of different systems that exist, is much more complicated."[107] Similarly, Robin Bulloch, Lloyds Banking Group, told us in our C*onsumers' access to financial services* inquiry, that:

> We have systems that are sizeable in scale [ … ] but, when we are lifting the bonnet and going to change the engine, it takes time, because we have to be very careful about the changes that we make, and we would absolutely wish to guarantee that the changes are done once, rather than trying to do things quickly and finding that we have not done what we intended.[108]

86. Furthermore, the Regulators explained that legacy systems often involve key person risk:

> The challenges of maintaining older systems is exacerbated where the engineers and other experts with the knowledge to support them have left or retired, reducing the knowledge base available over time. The documentation on these systems relied on by their successors may not always be adequate.[109]

87. Yet some firms observed that not all legacy systems are problematic. Barclays explained that "While a system running a service will inevitably age, this does not necessarily mean that it poses greater risk."[110] Also, PwC commented that "we don't believe that "legacy" and "fragile" should be used interchangeably when applied to systems [ … ]. There are some very stable and secure systems that have been in place for a number of years".[111]

88. Many respondents agreed that updating legacy systems, even if the upgrade was needed, created significant risks. The Regulators explained that "Firms and FMIs may prefer to patch and upgrade their systems where the risk appetite for wholesale transformation and system replacement is low".[112] Similarly, the Center for Evidence-Based Management explained that:

> Deciding to replace a firm's core systems is possibly one of the riskiest strategic technology decisions that a board can make. [ … ] It is often

106 PwC (OPR0008)
107 Treasury Committee: Oral evidence: Economic Crime, HC 940, 15 May 2019 [Q860]
108 Treasury Committee: Oral evidence: Consumers' access to financial services, HC 1642, 5 February 2019 [Q242]
109 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
110 Barclays (OPR0009)
111 PwC (OPR0008)
112 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)

> referred to as the apocryphal 'changing the engine while the plane is in flight', the risk being that business-as-usual may be severely disrupted during the several years of strategy execution.[113]

There are also cost reasons for not investing in legacy architecture. PwC emphasised that:

> Since the financial crisis profitability in the banking sector in the UK (and globally) has been depressed compared to previous periods. Most major financial institutions have attempted to cut costs significantly, and this, in our experience, has resulted in reduced expenditure on technology upgrades and other important infrastructure improvements.[114]

89. Yet, there are also factors that may prompt the reduction in legacy risks in the future. Lyndon Nelson, Deputy Chief Executive Officer and Executive Director for Regulatory Operations and Supervisory Risk Specialists, PRA, admitted that firms with legacy systems "cannot carry on with the legacies and the approach that they have, because I think it would become a front office business issue about them not being agile enough, when consumers are demanding those things."[115] Similarly, PwC explained the role of competition, as "New entrants to the market that are able to build bespoke and coherent systems will, in our view, have an advantage over incumbent firms."[116]

90. The Regulators may also need to promote change themselves. Charles Randall, Chair of the FCA, told us that "As a regulator, we need to have a level of intervention that ensures the management of a firm does not sit there saying, "This is such a nightmare; I will leave it to the next lot"."[117] Lyndon Nelson, PRA, described how the business services approach in the Regulator's Discussion Paper may reduce the use of legacy systems:

> I am hoping that the discussion paper [ … ] will effectively eliminate that; because, [ … ] the firm will have to think about what services to provide to the consumer, for example, and what is in the production line to get that service to them. Our best estimate is that, if there is a legacy system in there, their response time or their recovery time is going to be a lot higher.[118]

91. On regulatory role, the Center for Evidence-Based Management recommended that where firms are not addressing legacy risks they should be mandated to make preparations on how to mitigate those risks:

> Supervisors should require that firms produce concrete plans to mitigate any serious core systems risks, if necessary, initiating a CSR [core systems replacement] programme.[119]

113 Center for Evidence-Based Management (OPR0003)
114 PwC (OPR0008)
115 Q269
116 PwC (OPR0008)
117 Treasury Committee: Oral evidence: The work of the Financial Conduct Authority, 15 January 2019, HC 475 [Q420]
118 Q274
119 Center for Evidence-Based Management (OPR0003)

The Regulators also have the option of other tools to understand the risks of legacy systems, for example commissioning Section 166 skilled persons reviews.[120]

92. **Many financial institutions face the challenge of aging, legacy infrastructure that is hard to maintain, yet expensive and risky to replace. We do not believe enough is being done by firms to mitigate the operational risks they face from their own legacy technology, such as by moving to newer technology.**

93. **While legacy systems can in some cases be robust, firms must ensure that their use remains appropriate. This should include considering the availability of expertise to maintain the systems, and the system's resilience, and their remaining useful life. Firms must not use the cost or difficulty of upgrades as excuses to not make vital upgrades to legacy systems. Regulators should have a strong framework to oversee firms' assessments, and challenge these where necessary.**

94. **We welcome the indications from the Regulators that the approach set out in the Discussion Paper, if adopted, should trigger an improvement in firms' management of legacy systems. However, given the potential for short-sightedness by management teams, if improvements are not forthcoming, the Regulators must intervene to ensure that firms are not exposing customers to risks due to legacy IT systems. The Regulators should make use of their full range of the tools to achieve this, including commissioning independent Section 166 skilled person reviews.**

## Level of change and change management

95. The level of change the financial services sector is currently undertaking is significant. RBS highlighted that:

> We are facing rapid and significant changes at an industry level. Industry changes include Open Banking [ … ] computing capability associated with cloud computing and agile delivery methodologies.[121]

96. Change management was reported as one of the largest causes of operational incidents in the financial services sector, accounting for 20 per cent of the incidents reported to the FCA in the year to September 2018.[122] Some of the most high-profile and damaging incidents have occurred as a result of poorly implemented change, and these IT failures caused significant disruption and inconvenience for customers. The Regulators highlighted two cases:

- The RBS 2012 incident which was "an example of where poor change management affected over 6.5 million customers over several weeks".[123]
- The TSB 2018 incident: "TSB's online banking and mobile banking applications suffered disruption following a major upgrade of the bank's systems. Disruption

120 Financial Services and Markets Act 2000 (as amended), Section 166.The Regulators can appoint an independent skilled person to provide them with information or documents to assist them in regulation of a firm or the industry.

121 RBS (OPR0004)

122 FCA, Cyber and Technology Resilience: Themes from cross-sector survey 2017–18, November 2018

123 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)

> continued initially for over three weeks, with customers unable to access accounts online or via mobile devices and, in some cases, being able to view other customers' account balances when they were able to log in."[124]

97. The Regulators explained how firms should manage risks of change programmes:

> We expect firms and FMIs to have robust controls in place [ … ], including strong governance and senior management oversight, clear approvals processes, and independent testing. [125]

Megan Butler, FCA, highlighted in a speech that "we are worried that a lot of firms seem overly confident about their ability to manage flagship IT change programmes and keep their systems up to date".[126] Similarly, Lyndon Nelson, PRA, explained that "there are a number of weaknesses in risk management".[127]

98. One of the most important preventative measures against IT incidents as a result of system change is testing before the new system goes live to all customers. Speaking about Barclays' incident in September 2018, Graham Bastin, Head of Operational Resilience, Barclays, explained that "The change itself had been tested thoroughly, but when it went into the live production environment, we should have tested it for a little bit longer with customers, so that we might have been able to see this issue and back it out".[128]

99. The Center for Evidence-Based Management explained that "Every time a system is changed and either code released or hardware upgraded there is a risk of making a mistake", and that problems can arise when you see "aggressive management pushing changes to be released before they are fully tested in order to meet deadlines"[129]. In the case of TSB's incident in 2018, Andrew Bailey, FCA, told us that "testing is going to be one of the key questions".[130]

100. We also heard that the approach to change matters. Anne Boden, CEO of Starling Bank, explained that:

> Modern technology is now released and change managed by implementing a little bit of change often. By having a little bit of change [ … ] and doing it several times a day, you minimise the impact of that change. We all know that when you do big change—big migrations, big separations of banks, and big migrations of systems—we put customers at risk.[131]

101. Despite the risks, many instances of change have been successful. The FCA highlighted in a previous Committee session the successful implementation of ring-fencing.[132] This demonstrated that in the right circumstances the industry had the capability to deliver major change initiatives.

---

124 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
125 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
126 Megan Butler, Speech: Cyber and technology resilience in UK financial services. 27 November 2018.
127 Q278
128 Q206
129 Center for Evidence-Based Management (OPR0003)
130 Treasury Committee: Oral evidence: Service Disruption at TSB, HC 1009, 6 June 2018 [Q180]
131 Q124
132 Treasury Committee: Oral evidence: The Work of the Financial Conduct Authority, HC 475, 15 January [Q419]

102. Given cases of good and poor change management, the Regulators claimed that "This is an area where greater information-sharing about best practice would help to strengthen operational resilience".[133] Industry collaboration is covered further in Chapter 5 of this report.

103. The Regulators have considered initial learnings from the TSB migration. Sam Woods, Deputy Governor Prudential Regulation and Chief Executive Officer of the PRA, told us that the PRA:

> Put in place an extra capital requirement [ … ] precisely to cover an unspecified possibility of it going wrong. I can tell you, now that it has gone wrong, it has proved very expensive. It is a very good thing we have that capital requirement in place. That is one learning for us: that we should always do that where firms have a big programme of this kind.[134]

104. **Poor change management is one of the primary causes of IT failures. As firms embrace new technology to improve customer experience, and grapple with upgrading legacy systems to meet the expectations of digital banking, further IT change in the financial services sector is inevitable. It is important that firms have strong and well-rehearsed change management procedures. As a matter of urgency, firms should address any issues identified in their risk management, including ensuring that they have sufficient skills and experience to manage change.**

105. **We are concerned that time and cost pressures may cause firms to cut corners when implementing change programmes, for example by compressing testing schedules. Firms engaging in change programmes should not be allowed to gamble with their service availability.**

106. **While we accept that the ultimate responsibility for executing change programmes lies with firms, there is a role for the Regulators where customers are at risk. In their unique position with oversight over many change projects, the Regulators should ensure that best practice and lessons learnt from past change projects are disseminated to the industry.**

107. **The Regulators must also review their approach to supervising firms' large-scale change programmes to ensure that proactive intervention is possible, ahead of IT failures, so that customers are protected. This should include the level of engagement with firms, the level of specialist resource required, and the degree of assurance sought.**

## Outsourcing and third-party failure

108. In addition to in-house provision of services, financial services sector firms rely on third parties to provide services, for example technology and business processes. The Regulators wrote that "Industry trends show that firms and FMIs are increasing their use of third parties".[135] Some firms described a reversing trend and that they had begun to bring some services back in house. For example, Graham Bastin, Barclays, explained that "with outsourced providers we have insourced about 65 per cent of our suppliers".[136]

133 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
134 Treasury Committee: Oral evidence: The Work of the Prudential Regulation Authority, HC 704, 23 January [Q170]
135 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
136 Q150

109. Overseeing firms' outsourcing arrangements is important to the Regulators, who explained that "Outsourcing and wider use of third-party providers is a priority area of focus for the Authorities[137]".[138] Alison Barker, Director of Specialist Supervision at the FCA, explained that the FCA does not have a preference for insourcing or outsourcing but firms "can't outsource the responsibility for overseeing that it is working and understanding the impact of it when it does not work."[139]

110. There are risks involved in outsourcing. The Regulators stated that increased outsourcing has "a consequent implication for the operational resilience of firms and FMIs, and potentially the market, should an issue arise at a third-party supplier".[140] The FCA reported that third party failure is the second most common cause of incidents in the financial services sector.[141]

111. Some firms have difficulties in managing third parties, which can weaken their operational resilience. PwC described some of the issues that firms face:

> We observe that some firms currently struggle with third party management across their operations. [ … ] The current approach in firms to vendor management and supplier risk is often siloed, with individual teams focusing on different areas. In our opinion, there is more work needed by firms to gain visibility across the vendor landscape, to reduce the risk of outages and accidental information disclosure.[142]

Also, Megan Butler, FCA, highlighted in a speech that:

> Only 66 per cent of large firms, and 59 per cent of smaller firms, tell us that they understand the response and recovery plans of their third parties. On top of this, we know there is a real problem at the moment around recruiting the right skills at the top level; to steer, set strategy and oversee this model.[143]

112. Despite the risks inherent in outsourcing there are also many benefits. UK Finance explained that "Outsourcing should also allow a firm's management to increase its focus on the core business functions, expand the availability of business services, and accelerate the delivery of such services".[144] Furthermore, PwC stated that firms are "increasingly seeking to outsource critical functions to a concentrated set of vendors to reduce costs and gain access to external capabilities".[145]

113. **Given the prominence of operational incidents caused by third parties, we support the need for the industry to improve risk management of third-party relationships. Firms cannot use third party failures as an excuse when incidents occur. If the**

137 The Authorities refers to the Financial Conduct Authority, the Bank of England, and the Prudential Regulation Authority
138 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
139 Q298
140 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
141 FCA, Cyber and Technology Resilience: Themes from cross-sector survey 2017–18, November 2018
142 PwC (OPR0008)
143 Megan Butler, Speech: Cyber and technology resilience in UK financial services. 27 November 2018.
144 UK Finance (OPR0005)
145 PwC (OPR0008)

**Regulators are not observing a good standard of management of third parties by regulated firms, they should amend, as appropriate, their rules or guidance to prompt an improvement.**

## Cyber risk

114. Cyber attack was the fourth most common cause of incidents, as reported by the FCA.[146] PwC described how cyber risk can affect financial services sector firms:

> Cyber-attacks on the financial services sector are increasingly common and represent a growing risk. Denial of service (DoS) attacks are one of the most common [ … ] and are designed to shut down machines or networks by flooding the target with traffic, making them unavailable to intended users. Over the last few years a number of banks have been victims of DoS attacks with disruption lasting up to 48 hours.[147]

115. Cyber attacks on the financial services sector can also take the form of malicious attacks for financial gain. For example, Tesco Bank suffered a cyber attack in 2016,[148] which resulted in current account holders having unauthorised transactions on their accounts. Attackers may also seek to gain access to the wealth of data held by financial services firms. This could have a significant impact, not only on data security, but also if the data is corrupted.

116. The impact of cyber attacks can be long lasting. David Bailey, Executive Director for Financial Market Infrastructure at the Bank of England, explained that slow recovery times might be necessary in the "case of a cyber-attack which compromises the data integrity sitting within a financial market infrastructure, because quite frankly it is not worth coming back up if the data is corrupted".[149] Lyndon Nelson, PRA, commented that recovery time following a data integrity issue "could be months".[150]

117. Many financial services sector firms described combatting cyber risk as a priority. TheCityUK found that cyber attacks were referred to as the "most urgent concern" amongst industry executives.[151] Furthermore, there is a good level of coordination between firms on cyber risks. Graham Bastin, Head of Operational Resilience at Barclays, told us that:

> The highest levels of collaboration that I see are around cyber. The banks and the financial industry generally have determined that there is no competitive advantage from being better than the other guy at cyber. So we work with the intelligence agencies, the cyber-defence agency, GCHQ. We share information and intelligence for the benefit of all.[152]

118. **Cyber attacks are increasingly a concern for financial services sector firms. We welcome the level of coordination and priority given by firms in combatting cyber risks. We encourage the participation of all firms and the Regulators in these interactions.**

146 FCA, Cyber and Technology Resilience: Themes from cross-sector survey 2017–18, November 2018
147 PwC (OPR0008)
148 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
149 Q220
150 Q287
151 TheCityUK, Operational resilience in financial services: time to act. 6 June 2019
152 Q134

# 4 Emerging risks to operational resilience

## Concentration risk

119. There are many cases where financial services sector firms use the same third-party providers. Barclays described some of these common providers:

> Banks operate within an ecosystem of connected entities, many of which are suppliers or organisations that provide services directly or indirectly to the UK financial services sector, e.g. telecommunication network providers, technology providers, card transaction acquirers, card transaction processors (e.g. VISA Europe), central bank and market infrastructure providers and cash management providers.[153]

While this is not a new phenomenon, as technologies develop new sources of concentration risk emerge, for example firms' use of cloud service providers.

120. When financial services sector firms use common providers, this can create concentration risk. If one of these suppliers was to fail, there could be an impact on many financial services sector firms. PwC explained this risk:

> Failures in third party providers can result in significant disruption. The interconnectedness of the financial services industry means that localised outages can lead to contagion to other institutions. There is potential for global issues to develop, especially where multiple firms depend on the same service provider.[154]

TSB gave an example of such an incident:

> On the morning of 28 September 2018, a number of banks, including TSB, experienced service issues which started at the same time, and were all resolved a few hours later. For TSB, the cause was an incident at a third-party supplier—a supplier common to all the banks encountering problems that morning.[155]

121. However, concentration among a small number of providers may not necessarily mean reduced resilience. PwC argued that:

> It is also not automatically the case that a small number of providers represents a decrease in sectoral resilience. In some cases these large providers are better able to manage operational challenges than multiple potential points of failure. In the event of a widespread cyber attack, for example, large technology companies are likely to be better placed to defend themselves than a large number of smaller firms. [156]

153 Barclays (OPR0009)
154 PwC (OPR0008)
155 TSB Bank (OPR0010)
156 PwC (OPR0008)

### Financial Market Infrastructure (FMI)

122. One prominent source of concentration risk is FMI.[157] Given the systemic risks that stem from the use of FMI, some of these firms are supervised by the Bank of England. The Regulators explained the supervision of FMI:

> As they sit at the heart of the financial system, FMIs need to operate smoothly every day, so their availability and resilience is one of the key objectives of the Bank's supervisors. FMIs have stringent requirements placed on them in line with the Principles for Financial Market Infrastructures (PFMI). Supervisory reviews also focus on the firms that provide critical services to FMIs, those that FMIs outsource to more generally, and on business continuity plans.[158]

The Bank of England has tools to mitigate systemic risk. David Bailey, Executive Director for Financial Market Infrastructure at the Bank of England, explained that:

> The infrastructure that underpins several of the payment systems [ … ]—faster payments, Bacs and LINK—is all provided by a single firm, Vocalink. Last year [ … ] it had reached a significance that meant we needed to recommend to the Treasury that it was brought within the regulatory perimeter. [ … ]
>
> We can also think about how to expand the regulatory perimeter when activities expand. Again, we recommended this, and the Treasury made a change via the Digital Economy Act two years ago that enabled us to supervise not just inter-bank payment systems, but payment systems that might operate in a way that facilitated payments between individuals without a bank intermediating them.[159]

### Cloud service providers

123. Cloud services providers are a recent example of where firms are increasingly using common suppliers. Mark Carney, Governor of the Bank of England, highlighted in a speech that "A quarter of major banks' activities and almost a third of all UK payments activity are already hosted on the Cloud, and there are considerable opportunities for even more intensive usage".[160]

124. There are significant potential benefits of using the cloud for the financial services sector. The Regulators recognised the benefits in terms of "cost savings and faster deployment cycles".[161] Sam Woods, Deputy Governor Prudential Regulation and Chief Executive Officer of the PRA, explained that "It is not necessarily a bad thing that firms are moving more stuff to the cloud. [ … ] It may be that the cyber resilience of some cloud

157 "FMIs are networks of users that transact with each other. They exist to reduce the risks and costs involved in making payments and settling trades in financial instruments". The Bank of England's regulation of FMIs includes payment systems, central securities depositories, and central counterparties. Bank of England, The Bank of England's supervision of financial market infrastructures—Annual Report, 20 February 2018

158 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)

159 Q301

160 Mark Carney, Speech: Enable, Empower, Ensure: A New Finance for the New Economy, 20 June 2019

161 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)

providers is higher than that of some individual firms". [162] Furthermore, RBS explained that the use of cloud "permits increased physical robustness and stability as architectures are no longer bound to limited large expensive assets such as datacentres".[163]

125. Despite the benefits of cloud services, there are also risks. The Regulators summarised them as follows:

> Cloud services also pose unique risks, including to data sensitivity, cross-border infrastructure and market concentration. [ … ] At the system level, some third-party providers (including cloud service provides) may be a key point of concentration and present a single point of failure risk where an operational incident could have a widespread impact on the system.[164]

126. Given the risks of the cloud, Sam Woods, PRA, told us that "We have recently instituted a new process within supervision in order to guide the supervisors as to whether something is important enough to require a deep inquiry from us, or whether it is a more routine thing that we can let go".[165]

127. The PRA is actively in discussions with some of the cloud service providers themselves. It has also focused its attention on particular risks, for example Lyndon Nelson, Deputy Chief Executive Officer and Executive Director for Regulatory Operations and Supervisory Risk Specialists, PRA, highlighted the PRA's focus on "how firms can exit and enter these contracts, and how much choice they actually have about what contractual terms they have, because obviously they have regulatory obligations."[166]

### *Potential solutions to concentration risk*

128. While concentration risk in some areas, for example FMI, is being addressed, other sources of concentration risk remain. The Regulators explained that the Financial Policy Committee monitors concentration risk "as part of its broader financial stability agenda".[167]

129. Yet the Regulators also described a role for firms:

> The Discussion Paper suggests that firms and FMIs should map their important business services to underlying systems and processes that support their delivery, and identify their tolerance for disruption under the assumption that disruption will occur (impact tolerance); we believe this could help identify and mitigate the risks arising from dependencies on critical third-party suppliers/vendors.[168]

130. To improve the understanding of concentration risk firms have suggested there is the need for a sector map. PwC highlighted that identifying where firms use the same provider is "something which is not always obvious, or easy, to determine".[169] TSB argued

162 Treasury Committee: Oral evidence: The work of the Prudential Regulation Authority, HC 704,23 January 2019 [Q167]
163 RBS (OPR0004)
164 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
165 Treasury Committee: Oral evidence: The work of the Prudential Regulation Authority, HC 704,23 January 2019 [Q167]
166 Q300
167 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
168 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
169 PwC (OPR0008)

that "To better understand the location and nature of concentration risk, we think it would be helpful if the Regulators mapped the common systems and components in financial services".[170] However, Lyndon Nelson, PRA, explained that "We are very nervous about having a map, because it would be wonderful for people who want to cause us harm"[171] and told us that "We have the ability to pull that map together."[172]

131. One way to mitigate concentration risk, is to regulate the common providers, as is done for some FMI firms. PwC explained that:

> Systemic providers of services should be held—and indeed hold themselves—to a higher standard of resilience. [ … ] The regulatory perimeter is also an important consideration for the regulators in meeting their objectives. There are institutions that are increasingly systemically important to the financial system (such as large technology firms) that are not regulated by the financial services regulators.[173]

In oral evidence, Simon Chard, Financial Services Partner, PwC, added that:

> Our view is that you need to do that understanding where the map is, where the participants are and where the risk is. We certainly feel that it may be a consequence of that that the regulatory perimeter is moved or other firms are brought into that. [174]

132. There are other options, short of bringing common suppliers fully into the regulatory perimeter. TSB suggested that:

> The Committee may wish to consider whether the development of mandatory common standards for critical and common suppliers could improve overall operational resilience. Suppliers would have to meet and maintain these standards in order to supply financial services companies.[175]

Similarly, UK finance suggested that:

> The Government and/or regulators might enable there to be a form of utility assurance on the outsource providers' operational resilience [ … ] This could align to European Banking Authority guidelines such that there are pooled audits organised jointly with other clients of the same outsource provider [ … ] in order to use audit resources more efficiently and to decrease the organisational burden on both the clients and the outsource provider.[176]

133. Finally, concentration risk could be mitigated if firms were able to switch between providers in the event of an incident. PwC explained that:

> Greater substitutability between these [critical] providers would clearly be welcome, and something industry and regulators should continue to focus on. It should be noted though there are significant operational and

170 TSB Bank (OPR0010)
171 Q308
172 Q309
173 PwC (OPR0008)
174 Q81
175 TSB Bank (OPR0010)
176 UK Finance (OPR0005)

> commercial challenges around achieving the degree of substitutability that would mitigate fully a serious operational incident at one of these key service providers. It is unlikely, for example, that firms would ever be able to automatically reroute trades into a different CCP or change cloud provider, at very short notice.[177]

Yet progress towards substitutability has been made in some cases. For example, in 2018, "Visa handled 18.9 million transactions for UK issuers as part of [their] stand-in processing service".[178]

134. **Producing a sector map would allow the Regulators to better identify and understand those commonly used service providers whose disruption could have major implications for the provision of financial services. We are sceptical of the Regulators' argument that the creation of the map would be a target for those trying to cause harm. The Regulators commonly create documents which need a similarly high degree of security to prevent the information contained in them falling into the wrong hands. Moreover, some elements of the map are well known. The Regulators should therefore reconsider the case for conducting a sector mapping exercise, including consideration of the security concerns it may create. If they conclude that it would not be in the public interest, they should set out to this Committee how they are identifying and continually monitoring the risks of common critical service providers and interconnectivity in the financial services sector.**

135. **Where the Regulators identify that third-party providers are becoming a potential source of concentration risk, they should highlight this risk, and consider whether action is required to mitigate it. Where common providers are systemic, and concentration risk is high or becoming high, the Financial Policy Committee should in each case consider recommending to the Treasury that these should be regulated, as the Financial Policy Committee has done for FMI.**

136. **The cloud service provider market stood out as a source of concentration risk during the inquiry. This market is already highly concentrated and there is probably nothing the Government or Regulators can do to reduce this concentration in the short or medium term. The consequences of a major operational incident at a large cloud service provider could be significant, and not just limited to the financial services sector. The case for the regulation of these providers to ensure high standards of operational resilience is therefore considerable. The Government should urgently consider how best to regulate cloud service providers. Regulating them as critical infrastructure, while complex, may be necessary.**

137. **There are other ways to mitigate concentration risk, including establishing channels of communication with common suppliers to use during an incident, utilising the EBA process of leveraging pooled audit arrangements for cloud service providers, and potentially building applications able to substitute a critical supplier with another. We expect industry, industry bodies, and the Regulators to act on initiatives such as these.**

177 PwC (OPR0008)
178 Visa (OPR0007)

## New technologies

138. The use of new technology and innovation in the financial services sector presents an opportunity to provide new features and services for customers, potentially at lower cost. New technologies can also facilitate improved operational resilience. The Regulators explained that "the implementation of new technologies in financial services can enhance risk management. For instance, the latest machine learning techniques can be used to provide more robust insights that help firms mitigate risk."[179]

139. However, new technologies can also pose a risk to the operational resilience of financial services firms. PwC explained that:

> The rate of innovation in cloud, AI [Artificial Intelligence], robotics and Distributed Ledger Technology (DLT), could lead to vulnerability. We are in the middle of a technological revolution which requires firms to adopt relatively untested technologies while navigating the challenges posed by legacy systems which do not have embedded resilience.[180]

140. There are also wider risks to consider. For example, there are potential downsides of the use of AI. Anne Boden, CEO of Starling Bank, explained that AI:

> Can perpetuate prejudice and can, in some cases, perpetuate the situation regarding the financial systems of certain people in one way and that of other people in a very different way. We need to get the models right. They need to be fair and we need to be doing it with our eyes open.[181]

141. The Bank of England and the FCA surveyed firms on Artificial Intelligence and machine learning to understand their use and impact on financial services. The results were published in October 2019, and the Bank of England and the FCA have announced their intention to establish a public-private working group on AI to explore further.[182] In addition, Lyndon Nelson, PRA, commented that:

> The way in which some of the models are established means that they either reflect the biases of humanity or put those in. The important thing for the regulator is that these cannot be a black box. The management need to understand what outcomes they come up with, and the regulator needs to understand those as well.[183]

142. We also examined the risks of Open Banking,[184] and whether there is a trade-off between customer convenience and security. Anne Boden, Starling Bank, told us that "I would never launch anything that is not secure",[185] and Graham Bastin, Head of Operational Resilience at Barclays, said that Barclays "would never consciously launch

179 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
180 PwC (OPR0008)
181 Q175
182 Bank of England and FCA, Machine learning in UK financial services, October 2019
183 Q296
184 "Open Banking is designed to bring more competition and innovation to financial services. It was set up by the Competition and Markets Authority on behalf of the UK Government." "Open Banking is the secure way to give providers access to your financial information." https://www.openbanking.org.uk/customers/what-is-open-banking/
185 Q152

anything that was unstable".[186] On data security, Anne Boden of Starling Bank told us:

> You then have FinTechs, which do not have banking licences but are regulated within the open banking regime and can consume that data. The banks have responsibility for our customers and we are responsible for compensating our customers if something goes wrong when a customer shares their data with a regulated FinTech.[187]

We also heard from Alison Barker, Director of Specialist Supervision at the FCA, about the risks of Open Banking:

> We are aware of the comments where people say, "If you have access to banking systems, will that create more risk?" We are monitoring that closely. In our statistics of the things that have been notified to us, 0.2 per cent relate to Open Banking. We have not seen any issues coming through, but we are aware of the risks and have very closely assessed the information service providers to make sure that their technology is appropriate and strong.[188]

143. When asked whether customer demand for new technology or functions is causing harm, Alison Barker, FCA, explained that "No, I think it goes back to the point that we expect firms to understand and manage the change and understand the business services, and understand what the impacts of any outages should be."[189]

144. The Regulators are assessing the impact of new technologies on the sector. They gave examples of the FCA's Regulatory Sandbox, which "provides firms the opportunity to test innovative propositions in a real market and with real consumers, but with appropriate safeguards and oversight", and the Bank of England's Fintech Hub, which focuses on "the policy implications of fintech".[190]

### *Regulation of new technology firms*

145. New technology-driven firms are entering the market, taking advantage of new ways of reaching customers and offering new services. Barclays highlighted that "technology firms, which predominantly operate in sectors traditionally far removed from the regulated financial services sector, are increasingly starting to engage in financial services activities, while existing outside of the regulatory perimeter".[191]

146. Representatives of the industry and some firms were keen to ensure the consistency of regulation. Marcus Scott, Chief Operating Officer, TheCityUK explained that new technology firms should be held to the same standard of resilience:

> We need to make sure that that new technology is resilient. It is not subject to perhaps the same regulations because it is not consumer-facing, but it should be subject to the same operational resilience standards.[192]

186 Q155
187 Q156
188 Q290
189 Q233
190 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
191 Barclays (OPR0009)
192 Q64

Marcus Scott, TheCityUK, also explained that new unregulated entrants to the market:

> Brings in the issue of where to put the regulatory perimeter, so that everyone is operating under the same set of rules. There has been a tendency to look at new technologies and say that we do not want to stifle them, which is right. At the same time, they need to be regulated in a way that makes sure they are operating under the same set of rules.[193]

Similarly, Barclays argued that regulation should be guided by the principle of "same activity, same risk, same regulation".[194]

147. When asked by us if technology companies structuring their activities to avoid regulation was concerning, Alison Barker, FCA, commented:

> Not particularly, but we always have challenges with the perimeter and who is on which side of it, so we do watch that carefully. If we have firms doing activities that ought to be regulated, but they are doing them and they are not regulated, we take specific action.[195]

Furthermore, Lyndon Nelson, PRA, added that "The Financial Policy Committee has a legal responsibility, and it looks at that."[196]

148. In his Mansion House dinner speech in June 2019, the then Chancellor announced a "Treasury-led review of the payments landscape [ … ] to make sure that our regulation and infrastructure keeps pace with the dizzying array of new payments models".[197]

149. **New technology and innovation in the financial services sector can facilitate new services for customers and provide opportunities to improve firms' operational resilience. We support innovation where it benefits customers but with these benefits also come risks. Given the competition between firms to provide new technology driven services for customers, the Regulators should ensure they have the capability and capacity to monitor the use of new technologies in the financial services sector. Regulators must also assess whether firms are rolling out new technologies before they have proven their resilience.**

150. **It is right that firms and the Regulators are considering other downside risks from new technology, such as possible discriminatory effects. As the use of new technologies such as artificial intelligence and machine learning increase, both firms and Regulators must monitor their potential to be discriminatory. If these risks cannot be rigorously identified and mitigated, firms should not use these technologies. We urge the Regulators to set clear guidance for the sector.**

151. **As established financial services firms share data with new entrants, for example as a result of Open Banking, they must ensure that the data is secure before customers are allowed to use the service. While we received assurances from a number of banks**

193 Q30
194 Barclays (OPR0009)
195 Q291
196 Q292
197 The Rt Hon Philip Hammond MP, Mansion House dinner speech 2019, 20 June 2019

**that they would not put customers at risk by launching an unstable or insecure system, the stakes are high, and the level of oversight over smaller fintech providers may not be the same.**

152. **Some firms expressed the concern that new technology companies may be operating with a lower level of regulation than that of traditional financial services providers, while operating in similar sectors. We welcomed the Regulators explaining that they are monitoring this risk, and that the Financial Policy Committee considers this risk under its responsibility to identify risks beyond the regulatory perimeter. We also expect particular attention to be given to firms deliberately avoiding regulation. We believe that activities should be subject to the same standards of regulation, whatever type of firm is conducting them.**

153. **We urge the Government to consider the review of the payments landscape as a priority, and request that the Government set out the scope and timelines for the review in response to this report.**

## The wider financial services sector

154. Many of the most significant IT failures have originated in the retail banking and payments sector. While this may be the case given the complexity of banks and payment systems, and the impact on customers when these services are disrupted, IT incidents originating in other sectors could also be impactful.

155. PwC explained that they assessed the maturity of operational risk management to be highest amongst retail banks and investment banks, with insurance, asset management and wealth management lower down the spectrum of maturity.[198]

156. **The majority of evidence received in this inquiry relates to the banking and payments sectors. While this is unsurprising given the expectations of consumers for these services and the recent high-profile outages, we are also interested in the operational resilience of other areas of the financial services sector. All financial services firms, and the Regulators, should be alert to the causes and consequences of IT incidents across the sector, and should take the necessary steps to reduce any risks. If the Regulators have identified specific risks from IT failures of other sectors, they should briefly set out in their response to this report how these risks are being identified and mitigated.**

198 PwC (OPR0008)

# 5 Operational resilience and incident management

## Firms' management of operational resilience

### *Investment*

157. Improving operational resilience will require a level of investment by financial services firms. As previously described in Chapter 3, PwC commented that "Since the financial crisis profitability in the banking sector in the UK (and globally) has been depressed" which resulted in "reduced expenditure on technology upgrades and other important infrastructure improvements".[199] A lack of investment can increase the risk of incidents. PwC added that "Many financial services have complex legacy technology without ongoing investment to upgrade or replace these systems the risk of issues increases over time".[200]

158. Some firms explained that they are increasing their investment in operational resilience capability. For example, Graham Bastin, Head of Operational Resilience at Barclays, highlighted that they "have probably spent upwards of £1 billion over the last three years".[201] PwC explained that it expects investment to increase, and that "The Q4 2018 results of our latest PwC & CBI Financial Services survey found spending on IT, which was already strong in the previous quarters, is expected to increase further".[202]

159. Whether or not investment in operational resilience is sufficient at present, in its recent report TheCityUK commented that "in contrast to the investments already made across financial services to address financial resilience, the cost of achieving operational resilience will be small".[203]

160. **We heard that the level of investment in technology following the financial crisis has been affected by cost-cutting by financial services firms. Whilst some firms argued that they have invested in technology, many consumers would be disappointed that cost control has affected important investment in firms' IT and operational resilience. Given the profits generated by the financial services sector, this is not an acceptable position.**

### *Industry skills and experience*

161. The increasing reliance on technology in the financial services sector, and the complexity of firms' IT architecture has created greater demand for technical skills in the sector. Marcus Scott, TheCityUK, told us that the volume of skills available is an issue as:

199 PwC (OPR0008)
200 PwC (OPR0008)
201 Q86
202 PwC (OPR0008)
203 The City UK, Operational resilience in financial services: time to act, 6 June 2019

> One of the biggest challenges now is that our industry is competing with the rest of the economy for, more or less, the same skillset. This is only anecdotal, but one of our members, which was a bank, lost a team of web developers to [ … ] [a] takeaway company. [204]

162. The demands for skills in the financial services sector may necessitate looking further afield in different sectors to recruit staff. Sarah Isted, PwC, explained that that firms might need to bring in "people from outside financial services to bring a different perspective and particularly to bring the customer view to it".[205]

163. In response to the increasing demand for skills that Barclays were facing, Graham Bastin, Head of Operational Resilience, explained that it had "set up a technology campus in the north-west of England" where there are now 5,000 people.[206] This included hiring about 600 apprentices as Barclays "saw the need to bring in talent where we could do the knowledge transfer between some of the older technologies and move towards digital and mobile [ … ] and give those people a career path where they would stay with us for a long period of time".[207]

164. There is also the need for operational resilience skillsets and experience on the boards and senior management teams of financial services firms. Sarah Isted told us that "Given it is a newer area [ … ] making sure you have the right people with the right skills both to do the work and to review and oversee it will be critical".[208]

165. During oral evidence in January 2019, Sam Woods, Deputy Governor Prudential Regulation and Chief Executive Officer of the PRA, was asked whether the PRA had rejected people at interviews for Senior Managers Regime functions for a lack of operational resilience experience. He replied that:

> Coming to cyber and [operations] in particular, I am not aware and I do not think we have rejected anyone on those grounds alone. However, we have made a point to a number of boards that we think they need to build up their expertise in this area, as indeed many other institutions and we ourselves are building it up. That is a concern about the degree of experience at the top of these institutions in that particular field.[209]

166. **Firms face challenges in hiring skilled and experienced staff to manage technology related risks, and we were encouraged to hear about some of the programmes that firms are investing in to train and develop staff. The financial services industry should work with universities and further education providers to develop the skills they need. There is an opportunity for firms to develop their own talent, and to recruit from a broad and diverse pool to improve their operational resilience capability.**

167. **Given the PRA's concern about the level of operational resilience experience on the boards of some financial services firms, we expect the Regulators to ensure that**

204 Q16
205 Q9
206 Q96
207 Q96
208 Q45
209 Treasury Committee: Oral evidence: The work of the Prudential Regulation Authority, HC 704, 23 January 2019 [Q165]

**firms are focussed on recruiting the right skills and experience for their boards and senior management and that they are developing diverse pipelines of talent for the future.**

## Industry collaboration

### *Collaboration and information sharing*

168. There is a level of coordination within the financial services industry, through which firms share experience to improve sector resilience. The Regulators explained the importance of this collaboration:

> We firmly believe that strengthening operational resilience requires collaboration. Regulators, firms, FMIs and technology providers should continue to work together to address the opportunities and risks presented by technology with respect to operational resilience, as part of the wider co-operation and collaboration on operational resilience being advocated by the Authorities.[210]

169. Financial services sector firms described how they collaborate with others within the industry. Asked whether firms work together to deal with incidents, Ian Lundberg, Chief Officer, Senior Vice President, Client Services Europe, Visa, told us that "From a Visa perspective, the answer is yes. The network is connecting the issuers to the acquirers, so we do work together. Across the board, we need to work collectively".[211] Anne Boden, CEO of Starling Bank, told us that "when we had a Visa incident, UK Finance gave us advice, and we collaborated in that environment to ensure that all customers had the right information".[212]

170. We also heard of the role of coordinating bodies and working groups to facilitate collaboration. Ian Lundberg, Visa, outlined that:

> UK Finance [ … ] has got roundtables on incident management communications. We are involved in them, with a number of other members of UK Finance. There is a cross-market operational working group led by both the Bank and UK Finance, and we participate in that. Also, the British Standards Institution is in the process of putting together an ISO on operational resilience.[213]

171. Even so, evidence was presented to us that there is scope for more collaboration. In its recent cyber and technology survey the FCA highlighted that firms are not contributing as much as they could be:

- Larger firms, particularly in the retail and wholesale banking sectors, are more willing to share information through established mechanisms than those in other sectors. [ … ]

210 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
211 Q133
212 Q135
213 Q137

- Some firms said that they choose not to share relevant information or had an ad-hoc approach to information sharing or gathering. [ … ]
- Many firms reported that they [ … ] subscribe to networks and information-sharing platforms to monitor for events or incidents but are not routinely contributing to them. [ … ]
- This lack of consistency suggests that there could be more effective collaboration across the industry. We encourage all firms to take a more open approach to information sharing with their peers.[214]

Similarly, the Regulators explained that the Cross Market Operational Resilience Group[215] "concluded that there is a need for greater co-ordination and more rapid information sharing"[216] during incidents. The Regulators also explained the Bank of England's role in co-chairing the Cross Market Operational Resilience Group, and that they "recognise that we can go further".[217]

172. We received evidence from a number of respondents highlighting that the most collaborative approach was taken to cyber risk. Graham Bastin, Barclays, thought that there was the most collaboration on cyber risk and that "We could do more along those lines in some of the other areas of resilience".[218] Visa also supported this approach, explaining that:

> There are a number of lessons to learn from the UK's cyber strategy, such as the industry's collaboration across the public and private sector with the National Cyber Security Centre (NCSC), that can be adopted in the field of operational resilience.[219]

173. Internationally there are examples of private sector collaboration to facilitate improvements in the operational resilience of the sector. One commonly cited example is Sheltered Harbor. PwC explained that "The Sheltered Harbor initiative in the US, where institutions backup critical customer account data each night in an encrypted, separate data centre is an example of an initiative that could be explored in the UK".[220] Regarding Sheltered Harbor and industry collaboration, Lyndon Nelson, Deputy Chief Executive Officer and Executive Director for Regulatory Operations and Supervisory Risk Specialists, PRA, commented that industry needs to collaborate as whilst the Central Bank has tools to use for financial resilience, in the case of operational resilience "if a firm the size of Barclays or HSBC said that our retail banking system isn't working, there is nothing the Central Bank can do.[221]

214 FCA, "Cyber and Technology Resilience: Themes from cross-sector survey 2017–18", November 2018
215 The Cross-Market Operational Resilience Group (CMORG) "is chaired by the Bank and the industry, and provides a platform for co-ordinating and promoting work both aimed at strengthening the resilience of the financial sector and improving its ability to respond to operational incidents." Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
216 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
217 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
218 Q134
219 Visa (OPR0007)
220 PwC (OPR0008)
221 Q246

174. **There are benefits to industry taking a collaborative approach, sharing information and working together to improve the resilience of the sector. Cross-industry bodies such as UK Finance and TheCityUK should work with industry to identify and facilitate further areas of collaboration.**

175. **In their response to this report, we expect the Regulators to set out their plans to build on their existing work facilitating industry collaboration. This should include encouraging participation of firms of all sizes, and highlighting where they think industry could go further. Where firms are reluctant to collaborate due to competitive pressures or commercial interest, such as becoming more secure but not sharing best practice in order to develop a commercial advantage, there is a role for the Regulators to encourage collaboration.**

176. **It is not acceptable for customers to be at risk of severe operational disruption to their banking services for an indefinite period, and for there to be no way to for the Regulators to help them, due to there being "nothing the central bank can do" as we have heard. If the industry is unwilling or incapable of collectively preventing such disruption, for example by creating critical data backups and operational plans to mitigate against the consequences of cyber attack, then the Regulators must act. In the absence of market initiative, the Regulators should take stronger action to foster market solutions, or to enforce regulatory ones, to mitigate the risks of severe operational disruption.**

### *Sector exercises*

177. In preparation for incidents, many firms[222] run exercises to practice scenarios that could occur and rehearse responses. Visa emphasised the importance of financial institutions working together with other providers in the "ecosystem" as part of such scenario testing. Visa explained that it is:

> Critical to consider and plan [ … ] which approach to use in different scenarios, including the roles and responsibilities of different parties and how best to communicate with end-users. We would also support and encourage cross-industry planning to develop and formalise these arrangements, coupled with ongoing joint scenario testing and table-top exercises.[223]

178. The Regulators have a role to play in setting up sector exercises. Lyndon Nelson, PRA, told us that they have run at least 10 exercises.[224] He described one scenario whereby they simulated a cyber-incident spreading from parts of the G7, which was:

> Testing protocols, communications, how we would deal with issues and how do we inform people about the tools that we would use. [ … ] We essentially ran the same scenario in what we call our simex—simulation exercise. [ … ] About 70 banks, insurance companies and other companies,

222 Equifax (OPR0006), Barclays (OPR0009), RBS (OPR0004)
223 Visa (OPR0007)
224 Q240

> and FMIs were involved in the simex. [ … ] We also do desktops, so we did a desktop with the US Treasury Secretary, where we go through some of the issues that principals—the Chancellor was there—might face.[225]

Graham Bastin, Barclays, explained that they are currently working with the PRA on a future industry-wide payments stress test.[226]

179. Following sector exercises, the PRA has shared lessons learnt. Lyndon Nelson PRA, told us that:

> We issue a report. [ … ] That will have within it a number of work programmes—we will look at one on data integrity, and one on what we would do if a major institution was incapacitated. We are looking at communications. [ … ] We will obviously talk to individual firms as supervisors, and about how they would deal with an incident and what actions they need to take.[227]

180. **Sector exercises are a valuable tool for improving the industry's preparedness for incidents and identifying any potential areas of weakness. Such exercises can provide the opportunity for firms to rehearse responses to incidents and share best practice.**

181. **The Regulators should continue to facilitate sector exercises and should seek, in collaboration with industry and industry bodies, to expand the programme, in particular where new risks are identified, and where it is reasonably practical to include a wider range of firms. The Regulators should ensure that lessons learnt reports are shared with industry promptly after exercises.**

## Firm's Incident management

### *Best practice in incident management*

182. It is widely accepted that operational incidents will happen irrespective of how much a firm invests in prevention, and the Regulators have stated they believe that "disruptions and failures will inevitably occur".[228] This means that firms need to prepare in advance for how they would respond to an incident or multiple simultaneous incidents. For example, firms may have in place Business Continuity Plans to guide incident responses, including processes for convening crisis leadership teams. Alison Barker, Director of Specialist Supervision at the FCA, told us:

> Although we want firms to focus on prevention of disruption and plan properly, [ … ] we also have strong messages around, "Be prepared. Make sure you understand how you will respond and recover from an incident. [ … ]." That is because firms that are not well prepared cause more disruption to consumers.[229]

225 Q239
226 Q139, Q142
227 Q244
228 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
229 Q219

183. When firms experience incidents, the severity, length and impact on customers is highly dependent on the ability of the firm to manage the incident. The Regulators highlighted that the key factors assisting in successful incident recovery were "strong communication and coordination; senior management involvement, visibility, and strategic direction; and a controlled management of fixes."[230] However, they also brought to our attention that they "recognise that more can and should be done to share best practice in relation to change and incident management".[231]

184. Where there have been significant IT failures, it has been apparent in many cases that adequate recovery plans did not exist, resulting in significant disruption. Lyndon Nelson, PRA, emphasised the importance of firms having alternative arrangements.

> In some of the instances we have seen, there really was not an adequate plan B. [ … ] If the hypothetical service—somebody getting their mortgage granted or their deposit paid—is primarily delivered through a computer system that is now out, what is the plan B.[232]

185. Banks described how alternative channels for delivering services to customers can help them minimise the impact of an incident on their customers. Barclays told us that its multi-channel strategy:

> Ensures customers have alternative access to our services, in the event of unavoidable outages that affect their preferred channel. Very specifically, these channels (mobile, online, phone, etc.) are supported on different technology systems to ensure we can continue to service our customers through one channel in the event of difficulty in another.[233]

186. Firms agreed that there was a need to prioritise bringing services back on line after an incident, to ensure that the most critical services were available for customers.[234] Graham Bastin, Barclays, explained that:

> "Get my balance" is probably the most used and the most important service to our customers, along with "Make a payment" and so on, so the level of resilience we put around those services is higher than that for some of the other services, such as "Change of address", which is less time critical.[235]

187. **Firms are right to adopt a 'when not if' mindset on operational incidents. Given this, and the impact on customers when incidents occur, it is vital that firms have robust procedures in place to be followed in the event of an incident and a viable 'Plan B'. The Regulators should ensure that assessing the adequacy of both the incident management procedures and evidence of exercising them, forms a fundamental part of their supervisory engagement. To drive up standards, the Regulators, or industry bodies, should issue best practice guidance against which firms can assess their own procedures.**

230 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
231 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
232 Qq221–222
233 Barclays (OPR0009)
234 Qq99–100
235 Q99

### *Customer communications*

188. When communications are not well handled and timely, incidents can escalate. Poor communications have affected firms in recent high-profile incidents. PwC explained that "In some cases the level of distress is exacerbated by a lack of clear communication from the firm to its customers or when customers cannot reach a member of staff".[236] For example, Visa was criticised for the handling of communications during its June 2018 incident, and was subsequently subject to specific directions from the Payment Systems Regulator.[237] Similarly, the FCA criticised the quality of TSB's communications following its IT migration. Andrew Bailey wrote to us saying:

> The FCA has been dissatisfied with TSB's communications with its customers and we have had concerns that TSB was not being open and transparent about the issues experienced. [ … ] TSB referred to "the vast majority" of customers being able to access their online accounts, at a time when there was a successful first-time login rate of only 50 per cent on the web channel.[238]

189. A number of respondents highlighted the value of proactive communications. The Regulators explained how some firms approach communications during an incident.

> Some firms take a proactive approach, communicating with customers clearly through all available channels (applications, web pages, call centre messages, email, signing up for text updates) to keep them informed or advise them of the alternative channels that are continuing to operate and have capacity. [ … ] Effective communication early on allows customers to understand and manage the consequences of an incident.[239]

190. Graham Bastin, Barclays, emphasised the value of communicating with customers in the event of an incident. He told us that:

> If you send a text or some other kind of alert, even when a feature on the digital mobile app is unavailable, or if you signpost that there is going to be a planned disruption at a weekend, which we have done fairly recently, that is really welcomed.[240]

191. However, UK Finance highlighted a trade-off firms face when communicating with customers.

> At the outset of an incident, the cause and impacted parties are not always fully clear and there is a balance between early and accurate communication. For example, there is a risk of broadcasting to all customers about a service issue when only some may be affected. This could generate a spike in calls to contact centres by concerned customers, adversely impacting a firm's ability to help those actually affected.[241]

236 PwC (OPR0008)
237 Payment Systems Regulator, PSR PS19/3, Specific Direction 9, May 2019
238 Treasury Committee, Correspondence from the Chief Executive of the FCA to Chair, 30 May 2018
239 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)
240 Q98
241 UK Finance (OPR0005)

Therefore, UK finance argued that:

> While there may be common principles that can be drawn up concerning operational incidents, the form and timing of customer interaction should remain a matter of proprietorial judgement—in the full knowledge of the potential for customer detriment and, in extreme circumstances, reputational damage for the firm.[242]

192. There may be misleading information circulated during incidents—whether deliberate or accidental—which can heighten their impact, and could be exploited by malicious actors. Customers need to be able to trust the information they receive when an incident is happening. Equifax commented that:

> In our experience, many consumers look for official government information to validate the authenticity of any communications they receive from a company in such circumstances. Throughout our incident, the National Cyber Security Centre (NCSC) website provided the most useful and understandable information to which we could signpost consumers.[243]

Given this, Equifax suggested a solution:

> We believe a central portal could help UK consumers to verify information about an incident that they may have received directly via email, phone or letter. [ … ] At present there are a number of organisations that provide such information, but this is often disparate, incomplete and lacking profile or trust among consumers. We would welcome the Treasury Committee's consideration of whether a visible Central Government-led portal could help signpost, reassure and better equip consumers.[244]

193. Lyndon Nelson, PRA, explained that senior figures in the Regulators and Government would communicate externally if necessary. In response to a question from us on who would reassure the population, he told us that "In the exercises that we run, we absolutely contemplate asking the Governor, the Chancellor or whoever to do these things, because that is what we think is the right response at the time".[245]

194. **Poor customer communications can exacerbate the impact of an operational incident, and previous high-profile outages have demonstrated this all too clearly. Clear, timely and accurate communications must ensure that customers are aware of the incident and that they receive advice on remediation timelines and alternative access. Customers have the right to this information.**

195. **While accuracy of communications is important in order to avoid misinformation, firms should not unnecessarily delay or withhold information, even where reports of an incident may risk their reputation. It should not be left to a firm's discretion as to whether to communicate to customers or not. If in rare circumstances there is a valid reason not to inform customers, this should require regulatory permission, and must not cause greater harm to customers.**

242 UK Finance (OPR0005)
243 Equifax (OPR0006)
244 Equifax (OPR0006)
245 Q264

196. **Customers need to be able to trust the information they receive during an IT incident from a financial services provider. Where communications are ineffective, or in major incidents where there is the need for a central source of trusted information, the Regulators should step in, which might include circulating information via a centralised portal.**

### *Customer complaints and compensation*

197. A number of firms explained in evidence to us that they compensate customers affected by IT incidents. RBS wrote that "Any customer who advises us that they have been affected by an incident will not be left out of pocket".[246] Additionally, the FCA explained that "there are clear rules setting out timescales that we expect firms to follow when a complaint is received. For most complaints about payment services, firms have 15 days to resolve a complaint, and up to eight weeks to resolve all other complaints".[247]

198. While firms described thorough compensation processes for when customers had been impacted by an incident, in practice, customers have struggled to make contact with firms and have had to wait for prolonged periods of time for compensation to be paid. For example, TSB reported on 27 July 2018 that only 37 per cent of the complaints related to its IT migration (in April 2018) had been resolved.[248] In February 2019 TSB announced that they had resolved "90 per cent (181,000) of the 204,000 customer complaints received since migration".[249]

199. **We are shocked to hear of the time taken for some customers to have complaints answered following an IT failure. This is an unacceptable position for customers and could lead to greater harm. Firms must act swiftly and fairly in responding to complaints and awarding compensation where customers have experienced harm or financial loss as a result of an IT incident. Given increasing demand on complaints teams following an incident, firms must be able to quickly scale up their capability. The FCA must ensure that firms are resolving complaints and awarding any compensation quickly and take action where this is not the case.**

246 RBS (OPR0004)
247 Treasury Committee, Correspondence from Director of Specialist Supervision, FCA, to Clerk, 13 August 2019
248 TSB, We're getting back on track and remain committed to putting things right, 27 July 2018
249 TSB, TSB announces 2018 full year results, 1 February 2019

# Conclusions and recommendations

## IT incidents

1. There has been a shift in the way that customers access their financial services, with an increasing number of customers using digital services. As customers come to rely more heavily on digital channels, and given that many high-street branches are closing, the resilience and availability of digital channels is being brought into sharper focus. Given these exacting expectations, it is likely that even brief service disruptions may cause significant concern among consumers. (Paragraph 10)

2. Financial services sector firms are increasingly utilising technology to improve their services. This can have efficiency and resilience benefits yet can also increase the complexity and risk in firms' IT architectures. While customers may benefit from new features or digital services, they also suffer when IT failures occur. (Paragraph 11)

3. We welcome the increasing focus on operational resilience among both industry and the Regulators. Further regulatory intervention is needed to improve the operational resilience of the financial services sector, as was required over the past decade for its financial resilience. The Regulators must give as much prominence to regulating operational risk and resilience as they currently afford to regulating prudential and conduct risks. (Paragraph 16)

4. Operational incidents in the financial services sector are increasing in frequency. While we recognise that many incidents have limited customer impact, recent high-profile cases have shown the harm to customers that can be caused. The impact of IT incidents can range from inconvenience to customers through to customer harm, and on to matters of a firm's viability or financial stability. Financial services providers must treat their ability to manage and prevent incidents with a level of seriousness appropriate to the significant impact when incidents occur. (Paragraph 24)

5. The lack of consistent and accurate recording of data on operational incidents is concerning. The Regulators should conduct an exercise to assess the accuracy and consistency of incident reporting. If necessary, the Regulators should clarify standards, guidance and definitions for industry on what incidents firms should both record and report. They should also consider the need to expand current reporting requirements, to cover broader services provided by firms. Higher quality incident reporting will serve to improve the ability of both the Regulators and industry to identify the biggest risks to the operational resilience of the sector. (Paragraph 30)

6. It is very difficult for customers to determine which financial services providers are operationally resilient, and to make clear comparisons across the industry. The Regulators should require clearer and more prominent public reporting to empower customers to make informed decisions regarding which provider they use, and to increase firms' focus on operational resilience. Where firms already publish incident information, this should be given greater prominence in information

made available to prospective and existing customers, such as that given to wait times and complaints, which are visibly displayed in bank branches for all to see. (Paragraph 31)

## The role of the Regulators

7. Regulatory supervision of operational resilience may require a different approach to that currently adopted for of prudential and conduct risks. While the Regulators are still developing their approach to supervising firms' operational resilience, there is an opportunity to consider whether current practice is the best model of supervision for this risk. The approach to supervision must be agile, and be able to adapt as operational resilience risks change, including those introduced as new technologies are adopted. (Paragraph 40)

8. It is promising to hear that firms are broadly supportive of the approach taken by the Regulators in their July 2018 Discussion Paper. We encourage the Regulators to continue to engage with industry when developing operational resilience requirements further, to ensure that these are practical and effective. The Regulators should publish further guidance for firms on how their different operational resilience requirements interact, and their expectations of firms when implementing them. This should be done as the policy is developed, and not after firms have begun implementation. (Paragraph 41)

9. The PRA has given us assurances that if the approach in the Discussion Paper is implemented, the level of disruption will fall. This remains to be seen. The Regulators should set out publicly how they intend to measure the effectiveness of future policy in achieving this aim. We will continue to scrutinise the progress made by the Regulators to improve the sector's operational resilience as part of its regular work. (Paragraph 42)

10. Given the importance of operational resilience, and the fast-moving nature of the risks, we urge the Regulators to prioritise the publication of their final policy and guidance. In responding to this report, the Regulators should set out their upcoming timetable for publication. (Paragraph 43)

11. We accept that completely uninterrupted access to banking services is not achievable, yet prolonged or regular IT failures are unacceptable. Recent high-profile incidents have caused significant harm to consumers and businesses, and we regard the current level of disruption from incidents as too high. We understand that impact tolerance will vary based on the regulatory objective in question (for example preventing consumer harm); the consumer group; and the importance of the product or service. Nevertheless, it is crucial that the Regulators maintain a very low tolerance for disruption to the most important services. (Paragraph 47)

12. We recommend that the Regulators provide clear guidance to firms on their expectations around the definition of business services and the level of impact tolerances. While the Regulators' current expectation is that firms would set their own impact tolerances, ultimately firms must not be allowed to set tolerance for

disruption too high. The Regulators must prohibit this to avoid lax operational resilience, which could in turn lead to a financial stability crisis or widespread consumer harm. (Paragraph 48)

13. The Regulators suggested in their Discussion Paper that firms would be expected to meet their impact tolerances in severe but plausible scenarios. We are concerned what the impact would be of an IT failure in scenarios where firms are not expected to meet their impact tolerance. In response to this report, the Regulators should describe extreme scenarios under which firms would not be expected to meet their own impact tolerance, and what the regulatory response would be to protect consumers from harm in such scenarios. (Paragraph 49)

14. The Regulators have a vital role during significant incidents. While the responsibility for managing incidents rests with financial services firms, where a firm's response proves ineffective and there is a risk to the Regulators' objectives, the Regulators must be willing and able to take appropriate action to mitigate risks to their objectives. (Paragraph 55)

15. Holding individuals and firms to account when IT failures happen is essential, not only to prevent individuals making the same mistakes again, but also to focus the attention of senior management on the risk of incidents and incident management. The Regulators must use the enforcement tools at their disposal to hold individuals and firms to account for their role in IT failures and poor operational resilience. The regulatory mechanisms to ensure accountability for failures must have teeth, and equally as importantly, be seen to have teeth. (Paragraph 62)

16. We support the increasing focus on accountability and responsibility brought about by the Senior Managers Regime. However, we have yet to see a successful enforcement case under the Regime against an individual following an IT failure. We are concerned that this may be evidence of an ineffective regime to support enforcement. We accept that not all IT failures would result in enforcement action by the Regulators. However, the Regulators should consider whether there are any barriers to the effective operation of the regime, and whether any changes to the requirements or standards are necessary to ensure that individuals can be held accountable. If future incidents continue to occur without any sanction to individuals under the Regime, us as a Committee, and Parliament, will have to consider whether the powers it has given to the Regulators are fit for purpose. (Paragraph 63)

17. The length of time it has taken for customers and Parliament to be provided with a comprehensive independent account of what happened during the TSB IT failure, who was at fault, and why the recovery process took so long is unacceptable. The Regulators must provide a full report of their investigation into the incident in their response to this report, or failing this, provide us with an update on timelines and issue the full report as soon as possible. (Paragraph 64)

18. Remuneration structures throughout firms should reflect the importance of operational resilience. When appropriately used, these structures can help improve the prominence of operational resilience, and the requisite level of attention to

preventing IT failures. If the Regulators observe that firms are not adequately taking operational performance into account when determining remuneration for senior staff within financial services firms, they must intervene. (Paragraph 65)

19. As we have seen from recent examples, such as the Visa outage in 2018, operational incidents at Financial Market Infrastructure (FMI) firms can have as much effect on customers as bank incidents. It is therefore vital that senior management at FMI firms are accountable for their management of operational incidents. There does not appear to be any justification for keeping FMI outside of the Senior Managers Regime. The Government should expand the Senior Managers Regime to include FMI supervised by the Bank of England. (Paragraph 66)

20. Change is one of the biggest causes of operational incidents, and the Regulators are one of the biggest causes of change. It is vital that the Regulators do not inadvertently increase the risk of an operational incident by placing excessive or poorly coordinated requirements on firms. While it is concerning to hear firms criticise a lack of effective regulatory coordination, industry criticism of regulatory requirements must be viewed sceptically, as industry has an incentive to lobby for reduced regulatory burden. The same industry praised the joint approach by the FCA, PRA and Bank of England put forward in their July 2018 Discussion Paper. (Paragraph 74)

21. We welcome the then Chancellor's announcement of a review into the future regulatory framework for the financial services sector, and the subsequent call for evidence on regulatory coordination. The Treasury should implement a continuing coordinating forum to assess the cumulative burden of regulatory change, and to facilitate a permanent "air traffic control" in the financial services sector. This would help ensure that the Regulators themselves do not create operational risk through the volume and timing of their regulatory demands. (Paragraph 75)

22. The Regulators have an important role in overseeing and challenging firms' approach to operational resilience and preventing IT incidents. They need the appropriate skills and experience to do so. The Regulators have improved their capability over recent years, yet they must do more. While training programmes may assist the Regulators in building supervisory skills, expert and practitioner experience are also important. We therefore expect the Regulators to increase their capability, particularly at the more senior levels. (Paragraph 80)

23. We accept the Regulators' current budgets make hiring staff with skills and experience in operational resilience challenging. The Regulators should increase financial sector levies to ensure they can hire the staff with the expertise and practitioner experience they need. We do not expect to hear after the fact, perhaps in reaction to a major incident, that supervisory resources were inadequate. (Paragraph 81)

## Common causes of IT incidents

24. Many financial institutions face the challenge of aging, legacy infrastructure that is hard to maintain, yet expensive and risky to replace. We do not believe enough is being done by firms to mitigate the operational risks they face from their own legacy technology, such as by moving to newer technology. (Paragraph 92)

25. While legacy systems can in some cases be robust, firms must ensure that their use remains appropriate. This should include considering the availability of expertise to maintain the systems, and the system's resilience, and their remaining useful life. Firms must not use the cost or difficulty of upgrades as excuses to not make vital upgrades to legacy systems. Regulators should have a strong framework to oversee firms' assessments, and challenge these where necessary. (Paragraph 93)

26. We welcome the indications from the Regulators that the approach set out in the Discussion Paper, if adopted, should trigger an improvement in firms' management of legacy systems. However, given the potential for short-sightedness by management teams, if improvements are not forthcoming, the Regulators must intervene to ensure that firms are not exposing customers to risks due to legacy IT systems. The Regulators should make use of their full range of the tools to achieve this, including commissioning independent Section 166 skilled person reviews. (Paragraph 94)

27. Poor change management is one of the primary causes of IT failures. As firms embrace new technology to improve customer experience, and grapple with upgrading legacy systems to meet the expectations of digital banking, further IT change in the financial services sector is inevitable. It is important that firms have strong and well-rehearsed change management procedures. As a matter of urgency, firms should address any issues identified in their risk management, including ensuring that they have sufficient skills and experience to manage change. (Paragraph 104)

28. We are concerned that time and cost pressures may cause firms to cut corners when implementing change programmes, for example by compressing testing schedules. Firms engaging in change programmes should not be allowed to gamble with their service availability. (Paragraph 105)

29. While we accept that the ultimate responsibility for executing change programmes lies with firms, there is a role for the Regulators where customers are at risk. In their unique position with oversight over many change projects, the Regulators should ensure that best practice and lessons learnt from past change projects are disseminated to the industry. (Paragraph 106)

30. The Regulators must also review their approach to supervising firms' large-scale change programmes to ensure that proactive intervention is possible, ahead of IT failures, so that customers are protected. This should include the level of engagement with firms, the level of specialist resource required, and the degree of assurance sought. (Paragraph 107)

31. Given the prominence of operational incidents caused by third parties, we support the need for the industry to improve risk management of third-party relationships. Firms cannot use third party failures as an excuse when incidents occur. If the Regulators are not observing a good standard of management of third parties by regulated firms, they should amend, as appropriate, their rules or guidance to prompt an improvement. (Paragraph 113)

32. Cyber attacks are increasingly a concern for financial services sector firms. We welcome the level of coordination and priority given by firms in combatting cyber risks. We encourage the participation of all firms and the Regulators in these interactions. (Paragraph 118)

## Emerging risks to operational resilience

33. Producing a sector map would allow the Regulators to better identify and understand those commonly used service providers whose disruption could have major implications for the provision of financial services. We are sceptical of the Regulators' argument that the creation of the map would be a target for those trying to cause harm. The Regulators commonly create documents which need a similarly high degree of security to prevent the information contained in them falling into the wrong hands. Moreover, some elements of the map are well known. The Regulators should therefore reconsider the case for conducting a sector mapping exercise, including consideration of the security concerns it may create. If they conclude that it would not be in the public interest, they should set out to this Committee how they are identifying and continually monitoring the risks of common critical service providers and interconnectivity in the financial services sector. (Paragraph 134)

34. Where the Regulators identify that third-party providers are becoming a potential source of concentration risk, they should highlight this risk, and consider whether action is required to mitigate it. Where common providers are systemic, and concentration risk is high or becoming high, the Financial Policy Committee should in each case consider recommending to the Treasury that these should be regulated, as the Financial Policy Committee has done for FMI. (Paragraph 135)

35. The cloud service provider market stood out as a source of concentration risk during the inquiry. This market is already highly concentrated and there is probably nothing the Government or Regulators can do to reduce this concentration in the short or medium term. The consequences of a major operational incident at a large cloud service provider could be significant, and not just limited to the financial services sector. The case for the regulation of these providers to ensure high standards of operational resilience is therefore considerable. The Government should urgently consider how best to regulate cloud service providers. Regulating them as critical infrastructure, while complex, may be necessary. (Paragraph 136)

36. There are other ways to mitigate concentration risk, including establishing channels of communication with common suppliers to use during an incident, utilising the EBA process of leveraging pooled audit arrangements for cloud service providers, and potentially building applications able to substitute a critical supplier with another. We expect industry, industry bodies, and the Regulators to act on initiatives such as these. (Paragraph 137)

37. New technology and innovation in the financial services sector can facilitate new services for customers and provide opportunities to improve firms' operational resilience. We support innovation where it benefits customers but with these benefits also come risks. Given the competition between firms to provide new technology driven services for customers, the Regulators should ensure they have the capability and capacity to monitor the use of new technologies in the financial services sector. Regulators must also assess whether firms are rolling out new technologies before they have proven their resilience. (Paragraph 149)

38. It is right that firms and the Regulators are considering other downside risks from new technology, such as possible discriminatory effects. As the use of new technologies

such as artificial intelligence and machine learning increase, both firms and Regulators must monitor their potential to be discriminatory. If these risks cannot be rigorously identified and mitigated, firms should not use these technologies. We urge the Regulators to set clear guidance for the sector. (Paragraph 150)

39. As established financial services firms share data with new entrants, for example as a result of Open Banking, they must ensure that the data is secure before customers are allowed to use the service. While we received assurances from a number of banks that they would not put customers at risk by launching an unstable or insecure system, the stakes are high, and the level of oversight over smaller fintech providers may not be the same. (Paragraph 151)

40. Some firms expressed the concern that new technology companies may be operating with a lower level of regulation than that of traditional financial services providers, while operating in similar sectors. We welcomed the Regulators explaining that they are monitoring this risk, and that the Financial Policy Committee considers this risk under its responsibility to identify risks beyond the regulatory perimeter. We also expect particular attention to be given to firms deliberately avoiding regulation. We believe that activities should be subject to the same standards of regulation, whatever type of firm is conducting them. (Paragraph 152)

41. We urge the Government to consider the review of the payments landscape as a priority, and request that the Government set out the scope and timelines for the review in response to this report. (Paragraph 153)

42. The majority of evidence received in this inquiry relates to the banking and payments sectors. While this is unsurprising given the expectations of consumers for these services and the recent high-profile outages, we are also interested in the operational resilience of other areas of the financial services sector. All financial services firms, and the Regulators, should be alert to the causes and consequences of IT incidents across the sector, and should take the necessary steps to reduce any risks. If the Regulators have identified specific risks from IT failures of other sectors, they should briefly set out in their response to this report how these risks are being identified and mitigated. (Paragraph 156)

## Operational resilience and incident management

43. We heard that the level of investment in technology following the financial crisis has been affected by cost-cutting by financial services firms. Whilst some firms argued that they have invested in technology, many consumers would be disappointed that cost control has affected important investment in firms' IT and operational resilience. Given the profits generated by the financial services sector, this is not an acceptable position. (Paragraph 160)

44. Firms face challenges in hiring skilled and experienced staff to manage technology related risks, and we were encouraged to hear about some of the programmes that firms are investing in to train and develop staff. The financial services industry should work with universities and further education providers to develop the

skills they need. There is an opportunity for firms to develop their own talent, and to recruit from a broad and diverse pool to improve their operational resilience capability. (Paragraph 166)

45. Given the PRA's concern about the level of operational resilience experience on the boards of some financial services firms, we expect the Regulators to ensure that firms are focussed on recruiting the right skills and experience for their boards and senior management and that they are developing diverse pipelines of talent for the future. (Paragraph 167)

46. There are benefits to industry taking a collaborative approach, sharing information and working together to improve the resilience of the sector. Cross-industry bodies such as UK Finance and TheCityUK should work with industry to identify and facilitate further areas of collaboration. (Paragraph 174)

47. In their response to this report, we expect the Regulators to set out their plans to build on their existing work facilitating industry collaboration. This should include encouraging participation of firms of all sizes, and highlighting where they think industry could go further. Where firms are reluctant to collaborate due to competitive pressures or commercial interest, such as becoming more secure but not sharing best practice in order to develop a commercial advantage, there is a role for the Regulators to encourage collaboration. (Paragraph 175)

48. It is not acceptable for customers to be at risk of severe operational disruption to their banking services for an indefinite period, and for there to be no way to for the Regulators to help them, due to there being "nothing the central bank can do" as we have heard. If the industry is unwilling or incapable of collectively preventing such disruption, for example by creating critical data backups and operational plans to mitigate against the consequences of cyber attack, then the Regulators must act. In the absence of market initiative, the Regulators should take stronger action to foster market solutions, or to enforce regulatory ones, to mitigate the risks of severe operational disruption. (Paragraph 176)

49. Sector exercises are a valuable tool for improving the industry's preparedness for incidents and identifying any potential areas of weakness. Such exercises can provide the opportunity for firms to rehearse responses to incidents and share best practice. (Paragraph 180)

50. The Regulators should continue to facilitate sector exercises and should seek, in collaboration with industry and industry bodies, to expand the programme, in particular where new risks are identified, and where it is reasonably practical to include a wider range of firms. The Regulators should ensure that lessons learnt reports are shared with industry promptly after exercises. (Paragraph 181)

51. Firms are right to adopt a 'when not if' mindset on operational incidents. Given this, and the impact on customers when incidents occur, it is vital that firms have robust procedures in place to be followed in the event of an incident and a viable 'Plan B'. The Regulators should ensure that assessing the adequacy of both the incident management procedures and evidence of exercising them, forms a fundamental part

of their supervisory engagement. To drive up standards, the Regulators, or industry bodies, should issue best practice guidance against which firms can assess their own procedures. (Paragraph 187)

52. Poor customer communications can exacerbate the impact of an operational incident, and previous high-profile outages have demonstrated this all too clearly. Clear, timely and accurate communications must ensure that customers are aware of the incident and that they receive advice on remediation timelines and alternative access. Customers have the right to this information. (Paragraph 194)

53. While accuracy of communications is important in order to avoid misinformation, firms should not unnecessarily delay or withhold information, even where reports of an incident may risk their reputation. It should not be left to a firm's discretion as to whether to communicate to customers or not. If in rare circumstances there is a valid reason not to inform customers, this should require regulatory permission, and must not cause greater harm to customers. (Paragraph 195)

54. Customers need to be able to trust the information they receive during an IT incident from a financial services provider. Where communications are ineffective, or in major incidents where there is the need for a central source of trusted information, the Regulators should step in, which might include circulating information via a centralised portal. (Paragraph 196)

55. We are shocked to hear of the time taken for some customers to have complaints answered following an IT failure. This is an unacceptable position for customers and could lead to greater harm. Firms must act swiftly and fairly in responding to complaints and awarding compensation where customers have experienced harm or financial loss as a result of an IT incident. Given increasing demand on complaints teams following an incident, firms must be able to quickly scale up their capability. The FCA must ensure that firms are resolving complaints and awarding any compensation quickly and take action where this is not the case. (Paragraph 199)

# Formal minutes

## Tuesday 22 October 2019

Members present:

Catherine McKinnell took the Chair, in accordance with the Resolution of the Committee of 9 September

Rushanara Ali Alison McGovern

Alison Thewliss

Draft Report (*IT Failures in the Financial Services Sector*), proposed by the Chair, brought up and read.

*Ordered*, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 199 read and agreed to.

Summary agreed to.

*Resolved*, That the Report be the Second Report of the Committee to the House.

*Ordered*, That the Chair make the Report to the House.

*Ordered*, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

[Adjourned till Tuesday 29 October at 9.15 a.m.

# Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

### Tuesday 9 July 2019

**Simon Chard**, Financial Services Partner, PwC, **Sarah Isted**, Financial Services Risk and Regulation, PwC, **Marcus Scott**, Chief Operating Officer, TheCityUK — Q1–84

### Wednesday 17 July 2019

**Graham Bastin**, Head of Operational Resilience, Barclays, **Ian Lundberg**, Chief Officer Head of Client Services, Visa, **Anne Boden**, CEO, Starling Bank — Q85–209

### Wednesday 24 July 2019

**Alison Barker**, Director of Specialist Supervision, Financial Conduct Authority, **Lyndon Nelson**, Deputy CEO and Executive Director, Regulatory Operations and Supervisory Risks Specialists, Prudential Regulation Authority, **David Bailey**, Executive Director Financial Market Infrastructure, Bank of England — Q210–309

# Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

OPR numbers are generated by the evidence processing system and so may not be complete.

1 Barclays (OPR0009)

2 Center for Evidence-Based Managment (OPR0003)

3 Cyber Risk Investigation Working Party (under auspices of Institute and Faculty of Actuaries) (OPR0011)

4 Equifax (OPR0006)

5 Financial Conduct Authority, Bank of England and Prudential Regulation Authority (OPR0012)

6 ITRS Group (OPR0001)

7 PwC (OPR0008)

8 RBS (OPR0004)

9 TSB Bank (OPR0010)

10 UK Finance (OPR0005)

11 Visa (OPR0007)

# List of reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website. The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

## Session 2019-20

| | | |
|---|---|---|
| First Special Report | The work of the Financial Conduct Authority: the perimeter of regulation: FCA response to the Committee's Thirty-Fifth Report of Session 2017-19 | HC 132 |

## Session 2017–19

| | | |
|---|---|---|
| First Report | Appointment of Sir Dave Ramsden as Deputy Governor for Markets and Banking at the Bank of England | HC 472 |
| Second Report | Appointment of Professor Silvana Tenreyro to the Bank of England Monetary Policy Committee | HC 471 |
| Third Report | The Solvency II Directive and its impact on the UK Insurance Industry | HC 324 (HC 863) |
| Fourth Report | Transitional arrangements for exiting the European Union | HC 473 (HC 850) |
| Fifth Report | Autumn Budget 2017 | HC 600 (HC 757) |
| Sixth Report | Appointment of Elisabeth Stheeman to the Financial Policy Committee | HC 758 |
| Seventh Report | Student Loans | HC 478 (HC 995) |
| Eighth Report | Appointment of Charles Randell as Chair of the Financial Conduct Authority and the Payment Systems Regulator | HC 838 |
| Ninth Report | Childcare | HC 757 (HC 1196) |
| Tenth Report | Re-appointment of Alex Brazier to the Financial Policy Committee | HC 936 |
| Eleventh Report | Re-appointment of Donald Kohn to the Financial Policy Committee | HC 937 |
| Twelfth Report | Re-appointment of Martin Taylor to the Financial Policy Committee | HC 938 |
| Thirteenth Report | The Motability Scheme | HC 847 |
| Fourteenth Report | Re-appointment for Gertjan Vlieghe to the Monetary Policy Committee | HC 1056 |

| | | |
|---|---|---|
| Fifteenth Report | Women in finance | HC 477<br>(HC 1567) |
| Sixteenth Report | Appointment of Bradley Fried as Chair of Court, Bank of England | HC 1319 |
| Seventeenth Report | Appointment of Professor Jonathan Haskel to the Monetary Policy Committee | HC 1318 |
| Eighteenth Report | Appointment of Andy King to the Budget Responsibility Committee of the OBR | HC 1340 |
| Nineteenth Report | Household finances: income, saving and debt | HC 565<br>(HC 1627) |
| Twentieth Report | Appointment of Jill May to the Prudential Regulation Committee | HC 1511 |
| Twenty-first Report | Appointment of Professor Julia Black to the Prudential Regulation Committee | HC 1512 |
| Twenty-second Report | Crypto-assets | HC 910<br>(HC 1845) |
| Twenty-third Report | Re-appointment of Sir Jon Cunliffe as Deputy Governor for Financial Stability at the Bank of England | HC 1626 |
| Twenty-fourth Report | SME Finance | HC 1626<br>(HC 1873) |
| Twenty-fifth Report | The UK's economic relationship with the European Union: The Government's and Bank of England's Withdrawal Agreement analyses | HC 805 |
| Twenty-sixth Report | Budget 2018 | HC 1819 |
| Twenty-seventh Report | Appointment of Kathryn Cearns as Chair of the Office of Tax Simplifications | HC 1606<br>(HC 2111) |
| Twenty-eighth Report | Economic Crime - Anti-money laundering supervision and sanctions implementation | HC 2012 |
| Twenty-ninth Report | Consumers' access to financial services | HC 2010<br>(HC 2187)<br>(HC 2530<br>(HC 2535) |
| Thirtieth Report | Re-appointment of Michael Saunders to the Monetary Policy Committee | HC 1642<br>(HC 2423) |
| Thirty-first Report | Re-appointment of Dr Ben Broadbent as Deputy Governor for Monetary Policy at the Bank of England | HC 2294 |
| Thirty-second Report | The appointment of Dame Colette Bowe to the Financial Policy Committee | HC 2235 |
| Thirty-third Report | The re-appointment of Professor Anil Kashyap to the Financial Policy Committee | HC 2237 |
| Thirty-fourth Report | Disputing tax | HC 1914 |
| Thirty-fifth Report | The work of the Financial Conduct Authority: the perimeter of regulation | HC 2594 |

| | | |
|---|---|---|
| First Special Report | Transitional arrangements for exiting the European Union: Government Response to the Treasury Committee's Fourth Report | HC 850 |
| Second Special Report | The Solvency II Directive and its impact on the UK Insurance Industry: Bank of England Response to the Committee's Third Report of session 2017–19 | HC 863 |
| Third Special Report | Autumn Budget 2017: Government and Office for Budget Responsibility responses to the Treasury Committee's Fifth Report | HC 757 |
| Fourth Special Report | Student Loans: Government and Office for National Statistics responses to the Committee's Seventh Report | HC 995 |
| Fifth Special Report | Childcare: Government Response to the Committee's Ninth Report | HC 1196 |
| Sixth Special Report | Women in finance: Government Response to the Committee's Fifteenth Report | HC 1567 |
| Seventh Special Report | Household finances: income, saving and debt: Government Response to the Committee's Nineteenth Report | HC 1627 |
| Eighth Special Report | Government and Financial Conduct Authority Responses to the Committee's Twenty-Second Report: Crypto-assets | HC 1627 |
| Ninth Special Report | Government and Financial Conduct Authority Responses to the Committee's Twenty-Fourth Report: SME Finance | HC 1873 |
| Tenth Special Report | Government Response to the Twenty-Sixth Report: Budget 2018 | HC 2111 |
| Eleventh Special Report | Government Response to the Committee's Twenty-Eighth Report: Economic Crime - Anti-money laundering supervision and sanctions implementation | HC 2187 |
| Twelfth Special Report | Consumers' Access to Financial Services: Financial Conduct Authority response to the Committee's Twenty-Ninth Report | HC 2423 |
| Thirteenth Special Report | Consumers' Access to Financial Services: Government Response to the Committee's Twenty-Ninth Report | HC 2530 |
| Fourteenth Special Report | Consumers' Access to Financial Services: Payment Systems Regulator and Bank of England responses to the Committee's Twenty-Ninth Report | HC 2535 |
| Fifteenth Special Report | The work of the Financial Conduct Authority: the perimeter of regulation: Government Response to the Committee's Thirty-fifth Repor | HC 2674 |