Treasury Select Committee:
Inquiry into IT failures in the financial services sector
Submission by Barclays

About Barclays

Barclays is a transatlantic consumer and wholesale bank with global reach, offering products and services across personal, corporate and investment banking, credit cards and wealth management, with a strong presence in our two home markets of the UK and the US. With over 325 years of history and expertise in banking, Barclays operates in over 40 countries and employs approximately 85,000 people. Barclays moves, lends, invests and protects money for customers and clients worldwide.

Barclays welcomes the opportunity to provide written evidence to the Committee on the important topic of IT failures.

Introduction

Recent years have seen significant advances in technology that have delivered enormous benefits in customer convenience, safety and functionality in banking and financial services. Barclays has embraced these changes to offer unprecedented ease of access and availability, increased security, enhanced economic crime detection and prevention, automation of processes to reduce errors and greatly increased speed of processing requests.

Disruptions that affect customers' access to their accounts and their money impacts consumer confidence in the banking sector and, more specifically, individual firms. This issue is, therefore, one of our greatest priorities. Against the backdrop of FCA data that suggests an increase in the number of IT issues, and some instances that have seen customers with no access to banking services for prolonged periods, we share the Committee's concern about this issue.

To meet customer expectations and guard against IT failures that have widespread impact, we have invested heavily in our IT infrastructure. We organise and run our systems to enable our customers to use different channels interchangeably and seamlessly so there are: alternative channels available; systems are duplicated; and there are stand-in processing arrangements in the event of need.

Barclays' multi-channel strategy, not only provides customer choice and convenience, but also 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. We believe this deliberate, multi-channel approach has clear customer benefits over, for instance, a single channel provider, such as via a mobile banking app only, that leaves customers with no alternative in the event of a systems failure.

On 20 September 2018, when Barclays experienced an operational incident in which some of our systems were subject to substantial disruption, and on which we exchanged correspondence with the Chair of the Committee, our customers were still able to use core features on Mobile Banking and could use their cards and our ATM network throughout.

Barclays processes approximately 25,000 technology changes every month to ensure our systems stay ahead of a range of threats, trends, and customer demands. Technology has created a new dimension in competition as firms compete to provide the best features and greatest functionality through innovation in digital products and services for customers. This, in turn, requires ongoing changes to our systems. At the same time, we face an ever present and growing threat from cyber criminals trying to disrupt our systems and we must also respond rapidly to regulatory requirements to comply with changes to regulation and the law. Whilst the vast majority of the thousands of technology changes are completed successfully, very occasionally, they can result in unexpected outcomes which may impact our service delivery.

There is also an increasingly interconnected ecosystem of technology and infrastructure providers on which financial services providers are dependent, including broadband, mobile data networks, and other services.

In this environment, no system can be 100 per cent free from failure.

We regret any instance of service disruption to customers and remain focused on reducing the volume of operational incidents, through continued investment in our resilience and the strengthening of controls relating to technology. Nearly one quarter of Barclays’ global workforce of 85,000 is dedicated to technology and security. Just as we enable our customers to transact 24/7, we seek to ensure around-the-clock security and resilience. Barclays has created a network of Joint Operation Centre’s around the world with state-of-the-art technology and highly trained staff enabling ‘always on’ monitoring, tracking, and handling of technology issues and cyber threats.

We believe our approach is proving successful. Bucking what we understand to be the industry trend, operational incidents caused by technology are becoming less frequent across Barclays year-on-year, with a 15 per cent and 13 per cent reduction in the last two years respectively, which reflects our continued investment in resilience.

Where incidents do occur, we are resolutely focused on minimising any impact on customers. Indeed, it is Barclays’ absolute priority to ensure customers continue to have access to their cash, products, and services through some means.

Customer communication is also key and we look to provide proactive, regular and clear updates to our customers through different channels in order to signpost customers to those services that are unaffected in order to enable them to fulfill their requests.

We also ensure that we are proactive in providing redress for customers that we know have suffered financial detriment, e.g. in fees for missed payments etc., and take a case by case approach to other, more complex requests for compensation.

Whilst there will need to be a certain level of tolerance to operational disruption, firms should be judged on their resilience to minimise the occurrence of disruption, on their efficiency and effectiveness in responding to any incident, the way they communicate with their customers during any disruption, and how they treat and remediate any negatively impacted customers.

Addressing the specific topics raised by the Treasury Select Committee

1. **The extent to which operational incidents are becoming more frequent, and how the prevalence of such incidents may change in future as consumers and firms come to rely more heavily on technology**

The way in which businesses operate and consumers manage their lives is fundamentally changing. Almost all sectors are being impacted by digitisation, with financial services, in particular, being transformed. At Barclays, our customers undertake over six million - and growing - digital banking interactions every day through online and mobile services. This transformation of the financial services sector with services being provided through digital channels has provided significant benefit to consumers. The 'always on' nature of digital banking has massively improved convenience, enabling customers to engage through their preferred channel, at a time of their choosing, without having to visit a physical branch. As banking services are increasingly provided through such digital channels, the issue of bank operational resilience becomes ever more important, as banks seek to ensure they can continue to provide high quality service 24/7, as customers have come to expect.

In a recent study on technology and cyber resilience, the FCA noted that the number of incidents reported had increased by 138 per cent in the past year[1]. This increase may, in part, reflect the shift to digital service provision across the sector. In contrast, 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*), which reflects our continued investment in resilience.

Barclays determines any technological problem primarily through a customer lens. When any of our critical platforms do face difficulties, our systems are designed to ensure that other platforms remain available (we refer to our multi-channel strategy in response to Q3 as both an opportunity for consumer choice as well as a resilience measure), but there are also, often, non-digital alternatives available for use as back-up. An example of this would be during the day of disruption to some of Barclays' systems last September. Whilst eight mortgage completions required that day were impacted, our colleagues conducted the processes manually, bypassing the affected systems, and avoiding any customer disruption.

[1] https://fca.org.uk/publication/research/technology-cyber-resilience-questionnaire-cross-sector-report.pdf

Barclays is focused on continuing to reduce the volume of operational incidents going forward, through the strengthening of controls relating to technology underpinning our business. For example, we have agreed standards and processes in place to manage the risks of operating and maintaining a complex technology estate across the Group. We have also sought to identify and understand our most critical banking services, and the internal processes that exist to support and fulfil any customer requests. We also ensure appropriate levels of resilience are designed and implemented for each service, depending on its criticality, and assign a senior Accountable Executive to each critical banking service responsible for ensuring its resilience and that regular testing is undertaken. While we don't expect the causes of incidents to change in the future, the prevention, response and resolution time will become increasingly important given our customers' reliance on digital services.

2. The common causes of operational incidents in the financial services sector

While there may be a variety of causes of operational incidents, including human error, third party failure, and failure of software and hardware, the most common causes at Barclays relate to technology change management activity. Barclays processes approximately 25,000 technology changes every month (with a peak of 33,000 changes in one month in the last year), which are rigorously managed, and with a 99.8 per cent success rate. When incidents do occur, we seek to resolve them as efficiently as possible to minimise any impact on the customer. Even in the case of the 0.2 per cent of changes that are not executed in the way that we would wish, an even smaller fraction result in any noticeable impact on our customers.

Under the Second Payment Services Directive ('PSD2'), we report all incidents above a certain threshold, which impact any Payment Account (which includes current accounts, savings accounts and credit cards across all customer segments including retail, SME and corporate) to the FCA. In addition, we report externally a subset of these which impact Personal' and 'Business' Current Account holders, to enable customers to make comparisons. On that basis, there were 18 incidents for the second quarter of 2018 and 16 for the third quarter.

While many changes are driven by Barclays' strategic investment to improve our service for customers, over half are required to deliver the changes mandated by regulators and the Government, and to keep our systems up to date and secure for our customers. A number of major technology change programmes have been mandated by Government or regulators, to transform the financial services sector and provide services digitally, for example the Open Banking framework, Cheque Imaging functionality, and UK bank ring-fencing requirements. Barclays fully supports, and indeed is looking to lead, the digitisation of banking services in the UK, but we would note that 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.

Barclays performs regular analysis of the root causes of any operational incidents caused by technology. Following any significant service disruption, Barclays follows its formal 'Incident Management' process, including completion of a 'Post Incident Review', to ensure that the cause is fully understood and to identify potential enhancements and service protection measures. Barclays remains focussed on operating a robust process and on strengthening our technology and operational controls.

3. The extent to which there exist "single points of failure" and/or other sources of concentration risk in the financial services sector

We define single points of failure as parts of underlying technology systems, which, if they were to fail, could prevent our systems from working as they should. They can, therefore, impact the resilience level of critical banking services and the internal processes that support them.

We have reviewed all of our critical banking services, and the internal processes that support them, to identify any single points of failure and we continue to use information gathered in reviews of any incidents to identify and address them. We have worked hard over the last few years to remove critical single points of failure from our banking services.

We also operate a multi-channel strategy to provide our customers with the opportunity to engage through their channel of choice but also to offer an alternative option should their preferred channel be encountering problems. For instance, if customers are experiencing an issue with our Barclays Mobile Banking app, they can use Barclays Internet Banking or one of our call centres.

There is also a level of "stand-in" capability available should there be an operational issue, for example, with systems that support our ATM (cash machines) and Point of Sale services. "Stand-in" processing is performed by a card scheme (e.g. VISA Europe, Mastercard) to ensure that cardholders can continue to transact in the event of a service disruption or outage.

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. To maintain high levels of resilience in this environment, Barclays operates a robust third party management framework to oversee the management of associated supplier related risks, including the identification of single points of failure – see Q7.

4. The incidence of multiple old legacy systems and the nature of their connectivity, and the impact of retrofitting web based/mobile systems to legacy systems

Barclays strives to develop a technology estate of modern systems with high levels of resilience and service provision for our customers. We are constantly evaluating all of our systems from the perspective of how effectively they are able to serve our customer needs. This is an organic and continuous process involving significant, and increasing investment, in both upgrading our existing technology estate, and in decommissioning elements that are no longer strategic to our banking services. These actions continue to create a more resilient, simplified, strategic technology estate, ensuring Barclays is well positioned to serve our customers and clients.

Barclays operates, manages, and maintains a number of core strategic technology platforms that underpin the banking services to our customers and clients. These platforms use a variety of technologies and are appropriately secured using strong controls to protect our customer and client information and transactions. As part of our regular control processes, Barclays ensures that the software we operate is maintained to the latest level of security, via a regime of regular updates.

While a system running a service will inevitably age, this does not necessarily mean that it poses greater risk. As explained in Q2, it is the process of changing systems that causes most operational incidents, so risk may actually exist in the upgrading of older systems or implementing changes to connect them to new systems, but rarely solely by virtue of systems being ‘mature’. We cannot comment on whether outdated systems may potentially be more of a risk for other organisations.

5. The risks associated with integrating banks/systems, following takeovers and mergers, for example

We recognise that the integration of different technology systems could pose a challenge from a technology change perspective. However, in the experience of major change that Barclays does have, we have largely succeeded in integrating any new systems into our core platforms and channels without major operational incidents or service disruption for customers.

Barclays also has experience in managing resilience and mitigating risks of significant structural reform in the context of UK bank ring-fencing requirements. On 1 April 2018, we successfully completed our separation - one of our most complex and largest change initiatives – to become the first UK ring-fenced bank, ahead of the regulatory deadline. Over seven major migration events, we safely transferred over 600,000 customers and clients, and 1.1bn associated ledger accounts to our ring-fenced entity. 132 technology applications were in scope with 1.6m letters issued to our personal and business customers. There was no significant and unexpected impact to our banking services during this period as planned maintenance periods were communicated well in advance to our customers and the industry.

6. The quality of relevant technical documentation

Strong governance frameworks are vital to ensure high levels of operational resilience, with technical documentation playing a key role in any framework.

Barclays has a defined framework for managing operational risks including resilience, as well as agreed processes to manage the technology environment from an incident, problem and change management perspective. These processes are designed to manage the risks of operating and maintaining a technology estate across the group.

We also maintain and regularly enhance a number of crisis ‘playbooks‘, and each of our scenarios has an associated playbook which is expanded through ‘wargaming’ to specify the roles and actions required in a crisis.

This technical documentation is reviewed annually and we perform regular test exercises to minimise service disruptions.

7. The impact of outsourcing on operational resilience

As is the case at most large financial services firms, Barclays utilises third party suppliers to provide specific or specialist services. However, Barclays invests significant time and resource to minimise any impact outsourcing may have on Barclays’ operational resilience and our ability to serve our customers.

Barclays has a robust supplier control programme that ensures assurance activities regarding supplier operated controls are carried out in a manner that is commensurate with the level of risk associated with the service being received from the supplier. Such assurance activities may involve supplier self-attestation questionnaires, supplier manager assurance reviews, on-site reviews by our Global Supplier Assurance team, on-site reviews by Barclays’ internal auditing teams, or a combination of these approaches.

To manage the operational resilience of suppliers themselves, Barclays uses a consistent framework for resilience across our supplier network. Prior to contracting, Barclays carries out an assessment of the inherent risk associated with the service being received from the supplier. Depending on the nature of the service being delivered, suppliers are contractually obligated to manage risk in the supplier chain, e.g. ensure timely availability of IT applications and infrastructure, facilities, and people to ensure that service continuity plans are appropriately tested. Each supplier is also assigned a resilience rating, which would take into account their criticality to the provision of our banking services.

Also, to manage any supplier risk to our operational resilience, Barclays has been reducing the complexity of our supplier estate. During the last two years, Barclays has reduced the number of suppliers across the group by over 65 per cent. In addition, we have been centralising and standardising the management of our critical suppliers which are now managed within our procurement function by dedicated supplier management professionals.

A contributory element of Barclays' reduction in operational incidents is also our investment in people, which has included insourcing key staff from third parties.

8. The ways in which consumers typically lose out as a result of operational incidents, including inconvenience and vulnerability to fraud

As a result of operational incidents, customers may lose out by not being able to complete their banking transactions, including potential disruptions to the payments that they seek to make.

Barclays has invested significant effort in recent years to improve our proactive processes and policies to mitigate and minimise any potential negative customer impact of a service disruption. Some examples include:

- Clear and timely communications with customers, for example through the use of SMS or via in-app messaging, to make customers aware of the issue and what we're doing to fix it. We may also offer the customer an alternative channel to service (e.g. online, telephony or branch, assuming those channels were operational).
- The automatic refunding of any fees or interest that have been incurred as a result of the incident, and/or product pricing re-set correctly on accounts.
- Case by case resolution of consequential loss to consumers.
- We extend branch opening hours on the day of any major service disruption, when it is required.
- The use of back-up 'Stand-in' processing systems whilst primary systems are unavailable, to enable the majority of card payments still to be approved, and service maintained.
- Ability to process transactions manually – e.g. mortgages, high value, and salary payments.

Barclays' customers are protected by a number of controls including our own designed and operated fraud prevention and detection systems, plus the wider industry controls operated specifically by global Card Scheme providers (e*.g. VISA Europe, Mastercard*).

Barclays' internal analysis suggests that these efforts are positively benefitting customers. Complaint volumes from operational incidents caused by technology have reduced by 10 per cent - these volumes relate directly to the initial incident (and include incidents caused by third parties) but exclude any additional complaints relating to queue times or secondary impact. Additionally, social media comments relating to operational incidents caused by technology (whether an accurate or fair report of disruption or not) have reduced by 30 per cent.

While customers' exposure to fraud is not increased directly as a result of any service disruption, there is a risk that opportunist fraudsters seek to take advantage of the situation to defraud customers. Barclays and the industry as a whole are making significant efforts to raise awareness of fraud across the industry to minimize this as much as possible.

9. Examples of best practice with respect to firms' responses to and handling of operational incidents, including approaches to communicating with customers, identifying and addressing the causes of incidents, and handling customer complaints and compensation

Barclays seeks to ensure best practice across all aspects of operational resilience, from identifying and handling incidents to communication with customers.

1) *Response to and handling of operational incidents*

Barclays agrees that speed of response is imperative and has put in place infrastructure and processes which enable us to identify and respond to incidents swiftly, to resolve the incident, minimise impact on customers and identify and fix root causes. Examples include:

- Barclays has controls in place to highlight when the risks of incidents are increasing. Using these controls, we can act promptly to prevent an issue occurring.
- All colleagues have the ability to raise incidents and are familiar with the process for doing so.
- As well as our own detection systems, Barclays monitors social media channels to identify potential service issues early on, and to understand customer impact.
- All incidents raised are categorised by the scale and depth of their impact.
- Incident management teams are available in individual business units to manage medium scale incidents and, as centres of excellence, they have access to all the technical, operational and customer subject matter experts required to handle this.
- For larger scale incidents, our Joint Operations Centres co-ordinate our response and can escalate to a full Crisis Management Team when appropriate. This framework is regularly tested with both internal and external sector-wide exercises and covers both internal incidents (*caused by Barclays or Barclays' third parties*) and external incidents (*not caused by us but which impact Barclays' customers*).

2) *Communicating with customers*

Barclays has delivered a step change in communication with our customers in the last few years. We acknowledge, and appreciate, that poor communication regarding operational incidents and service disruption can be very frustrating to consumers. For this reason, we take customer communication very seriously and are constantly reviewing and improving the way we communicate with our customers. Barclays strives to provide customers with transparency, visibility and control across all of our banking services, including in the event of an operational incident. Whilst the approach will vary depending upon the incident, common methods of communication include:

- Proactively communicating to colleagues engaging with customers across Barclays regarding issues (and potential issues) to equip them with the latest information to advise customers.
- Providing general updates via our social media pages, our website, service status page (see Annex) and automated voice systems, and more specifically, if cohorts of impacted

customers are identified, via phone and SMS (this often means we can inform and update the customer before they need to contact us).

  - Our social media teams are linked with our incident management colleagues and resourced to support customers and proactively communicate updates via these channels.

- Our customer communications are intended to:
  - Reassure customers that we are aware of and working on the issue.
  - Guide them towards alternatives (e.g. alternative channels).
  - Provide them with details of where they can obtain up-to-date information (e.g. via our website, service status page, call centre).
  - Reassure customers regarding any impacts on them (e.g. removal of any Barclays fees they incur as a result).
- Barclays has also introduced a Service Status Page on our website to provide the latest view of planned maintenance, and service availability, across our platforms and segments.

3) Handling customer complaints and compensation

Barclays seeks to manage any operational incidents so as to avoid, to the maximum extent possible, any impact being felt by the customer. However, in the event that customers are negatively impacted, we seek to resolve matters as efficiently and fairly as possible, to ensure the customer is satisfied:

- For impacts which we can independently determine (e.g. customers incurring a Barclays fee as a result of the incident), we will proactively manage this (e.g., removing fees without any action needed from customers).
- Where we cannot determine the impact (e.g. a missed payment opportunity with a third party) we look to respond swiftly and fairly, with all of our front-line colleagues empowered to deal with such complaints at the first point of contact (including being able to compensate a customer based on costs, distress, and inconvenience incurred).

10. What should be learned from the operational incidents witnessed in recent years

The increase in operational incidents across all sectors of the economy in recent years has provided key take-aways for all parties to learn from, react and enhance their own resilience capability.

As part of Barclays' formal 'Lessons Learned' and 'Post Incident Review' processes, Barclays monitors both internal operational incidents and what happens externally across the UK financial services sector. Additionally, Barclays regularly uses scenario planning to further improve our activities and plans in the event of an incident or crisis.

Key Barclays' learnings from recent incidents across the sector include the following, which have now been built into our resilience strategy:

- **Prevention is Key** – Barclays continues to invest in resilience for our most critical systems, and testing the resilience capability to prove that it works.

- **Customer communication is crucial -** Social media platforms enable customers to share knowledge of any operational incident very quickly, and voice their dissatisfaction very easily (albeit not always accurately or fairly). On the one hand, this provides an opportunity for banks to more quickly understand when an incident has occurred. On the other, it highlights the need for effective communication with customers to keep them appropriately and accurately informed.
- **Banks must prepare for incidents** – practising for operational incidents in a training scenario enables Barclays to more effectively respond in a 'live' environment. Barclays uses an award winning "Near Miss Exercising Model" to test our effectiveness and readiness.

We are increasing our investment against each of the areas above on a year-on-year basis.

11. The ability of the regulators to ensure firms are adequately guarding against service disruptions

and

12. Whether the regulators have the relevant skills to hold appropriate parties to account in the event of significant operational incidents

Barclays has a close, proactive and continuous engagement with our UK financial supervisors that includes, amongst other things, discussions on technology and operational resilience. Barclays also engages in relevant industry groups, some of which are led by the UK Authorities, e.g. the Cross-Market Operational Resiliency Group. Barclays UK actively participates in industry groups focusing on cyber and resilience, and proactively responds to industry exercises such as the 'Dear Chairman' letters.

It is important to recognise 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. Regulators should ensure they have a comprehensive understanding of the evolving financial services landscape, the new risks it may pose to consumers and any impacts on service provision and competition.

13. Approaches to operational resilience in different jurisdictions

Barclays applies a consistent global approach to operational resilience and associated activities, including a standard process for assessing risk and impact across all jurisdictions. Where jurisdictions across the world take different approaches to operational resilience, Barclays seeks to incorporate any regional regulations into our global approach to ensure our Group Resilience Policy is suitable across all jurisdictions.

14. The opportunities and risks presented by the application of new technology in the financial services sector with respect to operational resilience

Banking services are increasingly provided digitally, such as online or through mobile, and new technologies are enabling services to be provided in new and innovative ways. For example, the new Open Banking framework in the UK uses API technology to enable customers to share their data with third party providers. Barclays believes strongly that technological innovation in the provision of digital financial services has the potential to transform how consumers manage their finances and provide significant consumer benefit.

However, the development of new services based on technology also creates the potential for new operational risks, whether that be the change management process required to implement any new systems, or managing the operational resilience risk of third parties who may be involved in the new system e.g. third parties in delivering Open Banking services.

When the potential operational resilience risks can be managed effectively, Barclays believes that development of new technology based services will have an overwhelmingly positive impact on the consumers of financial services products and services, and the sector as a whole.

That being said, as referenced in our response to Q12, the financial services landscape is being transformed by technology and the entry of large technology firms into the sector. To ensure maximum protection for consumers, all financial services legislation and regulation should be technology and business model neutral. That is to say any new and emerging entrants offering financial services akin to traditional banks should be subject to the same regulatory rules and requirements as traditional banks, regardless of their primary business or home sector. Ultimately, policymakers should ensure equality of regulation, supervision, market access and obligations arising from participation in the financial services market, i.e. ‘same activity, same risk, same regulation’.

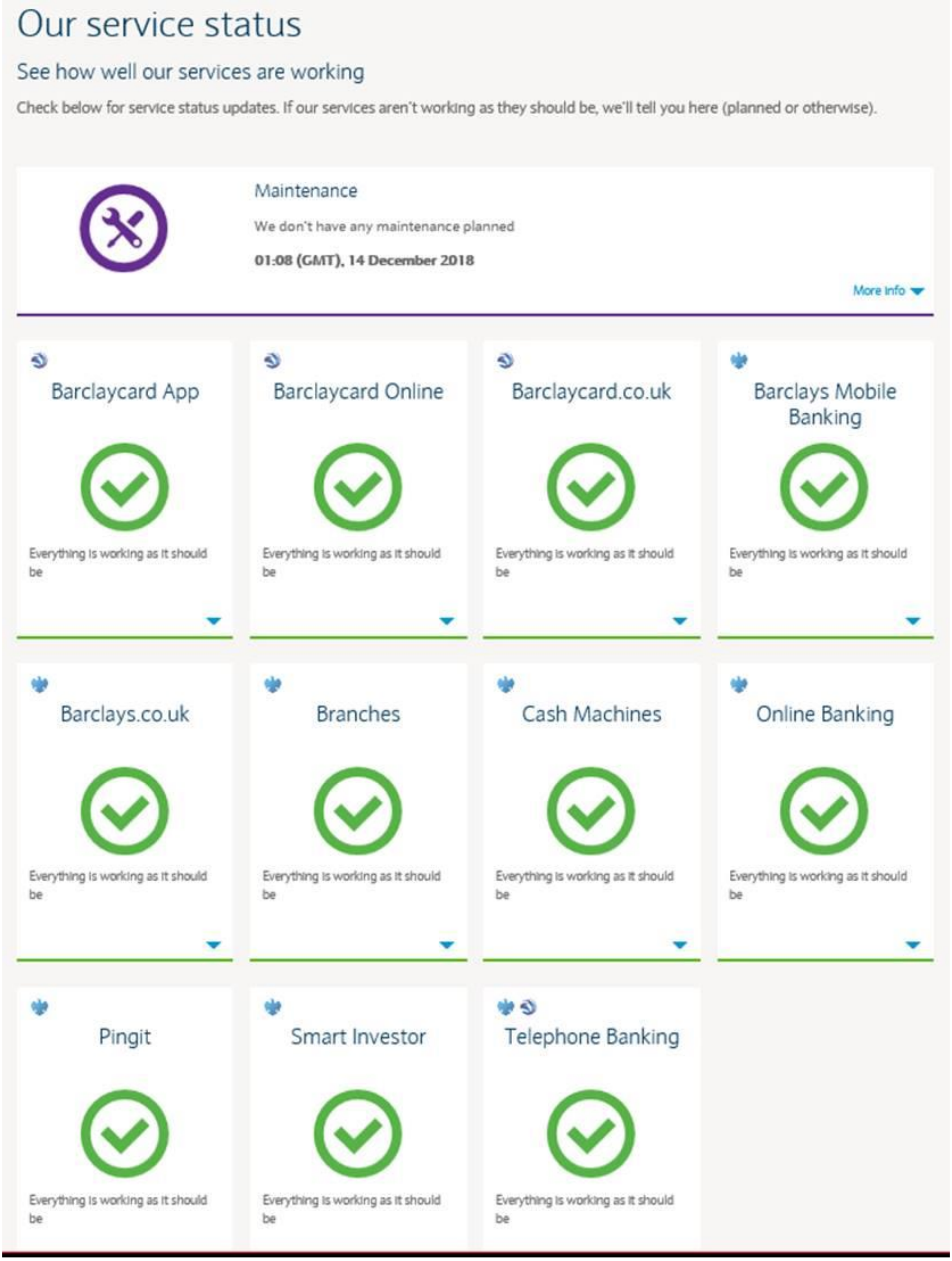
15. What should be considered an appropriate level of tolerance for operational disruptions

Barclays takes operational resilience of our business, and the continued service provision to our customers, extremely seriously. We make enormous efforts to ensure our services remain available to customers and look to minimise any service disruption to the maximum extent possible. For example, Barclays duplicates our key systems, four times in some cases, and segregates them, in an effort to maintain service provision in some channels, in the event that others experience problems.

However, despite Barclays’ considerable efforts, occasional, operational incidents do occur. It is important to recognise that no system is ever 100 per cent resilient, and any incidents are unforeseen and unexpected. Barclays takes all action possible to reduce the risk of incidents and mitigate their impact in the event that they do occur.

There will need to be a certain level of tolerance to operational disruptions, on the basis that a perfectly resilient system simply does not exist, nor is it likely to. Instead firms should be judged on their resilience to minimise the occurrence of disruption, their efficiency and effectiveness in responding to any incident, their communication with customers during any periods of disruption, and remediation of any negatively impacted customers.

Annex: Barclays' Service Status Page



Our service status

See how well our services are working

Check below for service status updates. If our services aren't working as they should be, we'll tell you here (planned or otherwise).

Maintenance

We don't have any maintenance planned

01:08 (GMT), 14 December 2018

Barclaycard App

Everything is working as it should be

Barclaycard Online

Everything is working as it should be

Barclaycard.co.uk

Everything is working as it should be

Barclays Mobile Banking

Everything is working as it should be

Barclays.co.uk

Everything is working as it should be

Branches

Everything is working as it should be

Cash Machines

Everything is working as it should be

Online Banking

Everything is working as it should be

Pingit

Everything is working as it should be

Smart Investor

Everything is working as it should be

Telephone Banking

Everything is working as it should be