APPENDIX: COMMITTEE QUESTIONS

1. **When did Barclays first become aware of the system failure; when were you personally informed of it; and when did you first inform the Financial Conduct Authority?**
    - From 10:10 British Summer Time (BST) on Thursday 20 September reports were received from colleagues unable to access one of our main systems used by staff in branch and our contact centres. These reports were also confirmed by our technology monitoring centre. A team began to investigate the issues immediately.
    - At 10:22 BST the impact of the issue was identified and the incident was escalated to a 'Major Incident' and, as per protocol, a broad technical specialist team was engaged to manage the incident.
    - At 11:14 BST the incident was escalated to a 'Severity-1' issue. This means that the incident was escalated to several senior leaders, including the Barclays UK CEO, BUK Chief Operating Officer (COO), BUK Chief Information Officer (CIO), Group Chief Information Officer (CIO), and Group Chief Operating Officer (COO).
    - We informed the FCA at 11:27 BST and the PRA at 11:30 BST, and followed up via email at 11:36 BST. An official PSD-2 (regulation) email was sent to both regulators at approximately 12:30 BST. A series of phone calls with both the FCA and PRA followed throughout the day to update on progress, with the last session focussed on customer redress.
    - The Group Chief Executive, Jes Staley, was in New York at the time of the incident. He was informed over the telephone by the Group Chief Operating Officer at 12:03 BST / 07:03 Eastern Daylight Time (EDT)/US time.
    - At 12:30 BST the Barclays UK Crisis Leadership Team (CLT) was instigated to manage the ongoing issues. The CLT is a predefined group of senior leaders across the business, chaired in this instance by the BUK Chief Information Officer, with the accountability to manage this type of scenario.
    - Both the Barclays UK and Barclays Group boards were informed and kept updated.
    - The CLT takes inputs from all areas across the business such as Technology, Compliance, Fraud and Front Line customer feedback and communication.

2. **For how long was Barclays aware of the system failure before issuing its first public statement on the incident? What subsequent steps did you take to inform your customers about the incident and its impact on them?**
    - We began updating our public status page from 10:42 BST showing outages for online banking and telephone banking services and then again at 11:25 BST to show Branches as also affected following the Severity-1 escalation.
    - Front line colleagues were informed of the incident via email at 10:32 BST, followed by a mass e-mail to all front line colleagues at 11:03 BST. Managers of branches and contact centres were also notified by text messages sent at 11:30 BST.
    - After understanding the issue, and informing the PRA and FCA (11:30 BST), we issued a statement via our public Twitter handle (@BarclaysUKHelp) at 11:56 BST informing customers of the technical issue.
    - This statement referred customers to our status page which, at the time, informed them of which channels were impacted, and that core Mobile Banking Services were operating as normal. Once channel outages were confirmed, the status page was reflected, as per protocol.

- In total, 94 minutes elapsed from the moment our technical bridge was established (10:22 BST) to our first public interaction, via Twitter (11:56 BST). During this time, our technical and communication teams worked together to ensure messaging was accurate, clear and transparent for our customers.
- The following day, we issued an apology to all customers; whether they were directly impacted or not.

3. What services were unavailable, either wholly or partially, as a result of the failure, and for how many hours in each case?

- For the duration of the incident our ATM, core features on Mobile Banking and card services were available for all of our customers.
- The following services were impacted for our customers:
    - Some branch and telephony colleagues were unable to use the colleague-facing tool to service customers via contact centres and branches.
    - Counter services in branch went into 'offline mode', meaning reduced cash withdrawal limits would have been utilised.
    - Customers were unable to access the Barclays Online Banking website, MyBarclays.
    - Mortgage Brokers and Advisors were unable to make mortgage applications (mortgage completions were unaffected).
- All channels with impacts listed above were impacted from 10:10 BST to 17:55 BST (services will have been coming online from 15:45-17:55 BST, but all services were confirmed as running as normal by 17:55 BST).

4. How many and what proportion of (a) business and (b) personal accounts were affected?

- Business and personal customers trying to access channels that experienced an outage during the period will have been affected. Typically, for Online Banking Services (Business and Retail) during the time of the incident we would have expected 89,000 logins. This represented 1.3% of our daily digital traffic.
- 300 Lending applications were affected (Barclaycard – 'Barclays Partner Finance' (point of sale finance).
- 60,000 customer calls to our Contact Centres were affected and prevented from using our automated voice recognition service.
- Our Smart Investor platform remained fully operational, however, we often see customers access the application through Online Banking. Those trying to access the application in this way may have been impacted.
- 8 mortgage completions required that day were impacted and any potential issues were fully mitigated by colleagues who conducted the processes manually, therefore bypassing the affected systems.

5. In your assessment, has the risk of fraud to customers been raised as a result of this incident? If so, what have you done to highlight this risk to customers?

- All our fraud systems were operational during the outage and we have seen no increase in fraud during the incident, or subsequently.
- Given the low level of risk assessed, and our understanding of experience other firms have encountered, we decided not to proactively engage with customers on this topic as we believe that proactive outreach could have actually increased the risk of fraud.

6. **What arrangements have you put in place to compensate customers who have lost out as a result of the failure? How in particular, do you intend to deal with consequential loss claims from business customers?**
    - Our first priority was to raise awareness of the issue with our customers and to apologise. Messages were posted across all our channels, in branch, telephony and digital as well as on social media. We also sent out over 15 million apologies via 'in app' notifications and SMS messages.
    - We have since been supporting customers who suffered any issues as a result of the incident and have already started making some redress payments to customers by way of compensation.
    - In addition, a group of our customers rely on an SMS service to trigger reminders to transfer funds into their accounts to avoid late payment charges. As there is a potential that these customers may not have been able to make the necessary transfers we have proactively not applied late payment charges to all impacted accounts.
    - Regarding business customers and consequential loss claims, our priority is to support any of them that were impacted. We will compensate on a case-by-case basis, whether by means of refunds or gestures of good will.
        - To provide a sense of scale, our business banking customers were unable to draw down on a total of 139 loans, but these were all subsequently completed. In one instance, we have identified a client who incurred contractual penalties as a result of late payment. In this case we will, of course, look to refund the client in question.

7. **What was the cause of the service failure? Are you completely confident that the causes have been addressed, and that your services are now working as they should?**
    - The cause of the issue was a rare interaction between two software systems, causing a corruption in the messaging being sent between our cheque imaging technology platform and our other key financial servicing systems.
    - We have identified that this was introduced during a change that was implemented the previous day and had run successfully in production and our test environments. The corrupt messages adversely affected our critical central messaging infrastructure, which communicates to a large number of our applications and services.
    - The corrupt messages (that caused the failure) were removed from the environment, and a full recycle of service restarts commenced from 15:45BST with all services confirmed as restored by 17:55BST.
    - We are confident that we have remediated the corrupted messages by making configuration changes, the systems are currently in a Business as Usual (BAU) state and are being fully monitored. We are however, working with our vendors to fully understand why the incompatibility issue between these systems arose in our production environments, post rigorous testing.

8. **What controls were in place to mitigate against such a failure, and why did these controls fail to prevent the failure?**
    - This was an extremely rare compatibility issue between two software systems. The changes were rigorously tested through one of our test environments and they did not exhibit the corruption behaviour demonstrated during the incident. The corruption only

occurred on a very small percentage of messages that were processed on the day, none of which occurred when running our tests. The full testing process for this change is currently under review with our specialists and we are reviewing both our testing plans and our test environment to see if we can build extra resilience into the process.

- We have invested heavily in the resilience of our platforms and on some of our core applications, for example, we now have four separate copies of our mission critical data (known as '4x redundancy'). In addition, we operate a testing schedule to ensure we understand this arrangement will work, when needed. However, due to the unique nature of the incident, corrupt messages were sent across all four copies, causing the outages experienced. More common problems would have been dealt with effectively and with zero impact to customers, for example hardware or application failures.
- In addition, we have been building diversity between our customer channels in order to not impact all channels at the same time. This approach supported us during the incident with mobile and online being on separate technology 'stacks' for their core features such as login, balance views, transaction views, and payments.

9. What steps will you be taking to ensure such similar system failures do not happen again?

- Barclays introduces thousands of software changes every day.
- This incident was a result of two software systems having a rare incompatibility issue which was not evident in our test environments, or from the vendors involved.
- The incompatibility was introduced due to change which had followed all of our process protocols and controls. These include:
    - Robust design, build and test phases for every change.
    - A large volume of tests to ensure all changes work as expected (for example: Security Testing, Functional Testing, System Integration Testing, User Acceptance Testing and Regression Testing).
    - Each change has 'Back-Out' plans created to ensure that we can revert back to previous versions, should the change be unsuccessful.
    - Live-proving plans are also made to ensure a smooth transition into customer rollout.
    - Each change is also given a risk rating and then taken through Change Advisory Boards to review and approve– this particular change was given a 'moderate' rating.
- We continue to operate these controls with rigour and are reviewing them for any further enhancements.
- We make thousands of software changes on an ongoing basis, and with a rigorous system of controls, see very few problems that have any impact on customers. Unfortunately, very occasionally, despite the controls, there is a customer impact which we need to put right.
- We are now going through a thorough analysis of what went wrong with both software vendors to drive a clear understanding of what caused the compatibility issue and how we can ensure this will not affect our customers and colleagues again.

10. What discussions have you had with the Financial Conduct Authority regarding the incident?

- We briefed the FCA as soon as we had a clear view of the incident. We kept our regulators closely involved with developments and had calls on both the Thursday and Friday to run through the issue, impacts, and our actions.