LLOYDS
BANKING GROUP

Ron van Kemenade
Group Chief Operating Officer
33 Old Broad Street
London
EC2N 1HZ

Dame Meg Hillier MP
Chair of the Treasury Select Committee
House of Commons
London
SW1A 0AA

28 April 2025

Reply to TSC letter dated 8 April 2025

Dear Dame Meg,

Thank you for your letter regarding the IT disruption that occurred at Lloyds Banking Group on Friday 28 February. We recognise the frustration that any service disruption can have for our customers, and I am sorry for the issues that occurred on that morning.

Although the disruption to our services did not constitute a full outage, we acknowledge the effect this had on some of our customers. On 28 February, around a quarter of customers were unable to successfully logon to our internet banking and mobile application services on their first attempt of trying within a two-hour period. It did not affect all customers or prevent access through alternative channels where transactions could still be carried out. This helped to mitigate the broader impact and financial consequences for our customers. Most customers who were unable to logon at their initial attempt were able to logon at the second or third time of trying during this period.

We have set out answers to the Committee's questions below.

1.Please can you outline the failure that occurred, what caused it and how it affected your customers? In your description, please can you provide a timeline of events, and a description of the failure by channel (i.e. app, web, branch, ATM, cards, etc). Please can you also note when all system failures were rectified?

On 28 February, some customers experienced disruption when attempting to logon to our Lloyds, Halifax, Bank of Scotland and MBNA internet banking and mobile application. A component of our infrastructure, which supports smooth customer authentications and applications, was not functioning optimally. Our online logon system is built to be highly resilient and handle the loss of several components, and we regularly test this. On this occasion the relevant component was functioning slower than normal and so was elongating the logon process for some customers, but because it had not failed, our checks did not pick this up and redirect customer logons to alternative routes within the system which were operating normally.

We did, however, have heightened monitoring of the pattern and speed of logons in place which allowed us to promptly identify that there was an issue, in line with our standard protocol. This meant we could quickly take action to minimise disruption. On this occasion we began to control logon demand so that only 75% of customers were able to logon at the first time of trying. This enabled us to stabilise the service.

Customers who logged on would have seen the message "We know some of our customers are having issues logging on to Online Banking and our app. We're sorry for this and we're working to have everything back to normal." During this disruption, one in four customers may have been prevented from logging on initially. These one in four customers would have had to try two or three times to access their banking services via these two channels. This led to an increased number of customers contacting the personal banking telephone lines, which resulted in longer wait times, which increased from an average of less than three minutes to five minutes 18 seconds. Customers who were transacting through branches, ATMs, making card transactions: including point of sale, chip and pin, contactless and card not present (apart from those requiring two factor application authentication) and direct debits were not impacted.

Timeline of events:

- 7:40am: Support teams began to observe high numbers of logons, but within normal thresholds.
- 7:56am: The team observed issues with our online banking customer authentications and applications service.
- 8:26am: We began to control logon demand, so that only 75% of customers were able to logon to the service at the first time of trying. We did this in order to manage demand and stabilise the service. When applied, controlling logon demand helps ensure that our system remains stable and continues to function effectively for the vast majority of customers.
- 8:27am: We added messaging for all customers which indicated intermittent issues were ongoing. Customers could retry and log on successfully.
- 10:00am: The controlling of logon demand was removed, with service stability confirmed by 10:30am.

2. Please can you provide an outline of how you intend to prevent such a failure happening again?

When such incidents occur, our IT Problem Management process is initiated to identify and resolve the underlying causes of service disruptions. The primary objectives are to prevent recurrence, minimise impact, and improve efficiency by enabling IT teams to respond more swiftly, ultimately enhancing service provision to our customers.

To prevent future service disruptions, we have identified two key initiatives:

- Enhancing our log on infrastructure to make it more resilient with additional capacity and improved ability to remove faulty components;

- Upgrades to our IT monitoring systems to allow us to spot any latency issues as soon as possible and improved logging to enable greater analysis should issues arise again.

3. Please can you provide an overview of how your Board responded to the outage?

The Lloyds Banking Group Board places a high priority on ensuring that our services remain accessible to our 28 million customers. It closely monitors the resilience of our services, the controls in place and their effectiveness. The Board regularly reviews reports on resilience and related management information.

The Board is engaged directly in Lloyds Banking Group's most severe operational incidents. Exercises are held each year to model these types of incidents and the Group's response. For incidents like that of 28 February, the Board, Executive management and regulators are updated on the impact, approach and progress on resolution. Checkpoints during incidents like this regularly consider whether additional support is needed from the Executive and the Board.

For this incident the root cause and areas for improvement were discussed at the "IT and Cyber Advisory Forum" chaired and attended by designated Non-Executive Directors (NEDs), being a Board sub-committee that focuses specifically on Technology matters, including IT Service Performance as a standing agenda item.

4. Please can you provide an estimate of the number of customers affected by your most recent outage (including as a proportion of your total customers), including an estimate of the number of vulnerable customers affected?

During the disruption to service around 1.3 million logons were affected. This number represented around circa 700,000 unique customers who had to try logging on more than once (representing around 2.5% of our 28 million customer base). There were approximately five million successful logons (79%) during the same period.

Lloyds Banking Group serves 28 million customers, and approximately two million people (around 7%) have a vulnerability – or a need for additional support – which they have given us permission to record. It is not possible to breakdown how many vulnerable customers were affected through the logon data collected.

However, any vulnerable customers affected who called our telephone service following the disruption would have had their call prioritised. We prioritise calls from vulnerable customers who have a registered support need, or use a word associated with vulnerability. At the time of the incident, we spoke to around 1,300 vulnerable customers over the phone and their average wait time was seven seconds, in comparison to the average customer waiting five minutes 18 seconds during this time.

5. Can you explain how Lloyds Banking Group is managing customer complaints following this incident, including whether you are being proactive in contacting customers who may have suffered, or whether you are entirely relying on complaints being reported to you?

During any IT event that impacts our customers, we advise them that we will ensure that they will not be left out of pocket and we will cover any charges they incur such as late payment fees.

Where we believe harm has been caused to our customers we look to proactively identify and compensate for any distress and inconvenience. Where customers have experienced a disruption to service, such as this incident where some customers tried to logon two or three times to their internet banking, we would rely on complaints being reported to us for consideration of the impact of the disruption to these two channels during this time.

6. Please can you provide your estimate of the amount of compensation Lloyds Banking Group expects to pay out, given the potential costs your customers faced, and your expected timeline on the provision of that compensation?

For the issue on the 28 February we received 714 customer complaints, with an average compensation payment of c.£22 per customer. The overall aggregated amount paid to customers was c.£16k. Complaint themes were mostly relating to a customer's inability to make online payments or to approve card transactions in the app. Of the 714 complaints received, 157 (22%) were classified as vulnerable.

7. Please can you provide the Committee with how your customer services response times changed over the period of the failure and in the period directly after, and the resources you have put in place to meet customer queries over the period and in the period directly after?

During the incident we had approximately 9,500 additional calls, 2,000 mobile messages from customers and 800 social media messages. The normal average wait time for customers to speak with a colleague is less than three minutes, and during the incident it increased to five minutes and 18 seconds. Our branches saw more visitors, and Fraud Telephony remained stable.

We had strong resourcing plans in place on the day to cope with any additional demand and to ensure we could speak to our customers. We adjusted schedules, and overtime was offered to maximise the number of colleagues available to answer our customers.

8. Please can you provide the Committee with an overview of your expected increase in fraudulent transactions over this period, how you have mitigated the risk of such transactions, and how you are helping customers who may have suffered due to fraud over the period?

Our data shows that there was no increase in fraud through the internet and mobile banking channels during the affected period and no increase in fraud reporting. Our fraud detection controls remained in place throughout this event and continued to protect our customers during

and after the outage event. There has also been no evidence that fraudulent activity has increased since the event – however we remain vigilant.

9. This IT failure occurred towards the very end of the month. Are there key times, within an average month, when systems are more likely to fail?

Over the past two years, our review of IT-related events shows no discernible pattern tied to specific times of the month. These events have been relatively evenly distributed across the month, with no concentration in any particular time of the month. We have not identified, and would not expect, a greater likelihood of such incidents occurring at specific points in the month. Furthermore, the event in question was not associated with our system performing at peak levels or was driven by coinciding with a day where high levels of payments were being made.

Friday 28 February was recognised in advance as a "peak day" for payments, because it was payday for many customers. During forecasted peak events, we conduct live monitoring of the status and health of our systems - it was this monitoring which picked up the issue quickly. Any unexpected system behaviour is promptly addressed, and we have pre-set emergency controls in place to ensure a swift response to any issues.

I hope you find these responses helpful. Please let me know if there is any further detail I can provide to assist you or the Committee.

Yours sincerely,

Ron van Kemenade
Group Chief Operating Officer