LLOYDS
BANKING GROUP

Dame Meg Hillier MP
Chair of the Treasury Committee
House of Commons
Palace of Westminster
London
SW1A OAA

Lloyds Banking Group
33 Old Broad Street
London EC2N 1HZ

Tuesday 24th March 2026

Dear Dame Meg,

Thank you for your letter dated 17 March 2026 to Charlie Nunn requesting details about the incident on 12 March, where some customers were able to see transactions carried out by others in their mobile banking app. As CEO Consumer Relationships, I am replying on behalf of the Group.

Although it was fixed promptly, we are extremely sorry the incident happened and we understand the questions it will have prompted. We have immediately investigated how the incident occurred. We have also notified the Financial Conduct Authority, the Prudential Regulation Authority and the Information Commissioner's Office and will, of course, cooperate fully with them.

We note your request to keep the Committee updated at intervals and will do so. Please find below our responses to the Committee's questions based on our findings to date.

1. Please can you provide the Committee with an overview of the incident, including the channels (e.g. app, internet banking) and brands that were affected by this incident. This should include a timeline of your response:

The incident was caused by an IT update to our mobile banking apps overnight between 11 and 12 March. It affected the Lloyds, Halifax and Bank of Scotland apps but not internet banking. In summary, between 03:28 and 08:08 on 12 March some customers logging in to the apps were able to see some other people's transactions, and potentially have their transactions viewed by other customers. In order to have seen another person's transactions and for theirs to be potentially viewed by other customers, a customer had to access their own list of transactions within small fractions of a second of another person doing the same. The issue related to current account transactions only.

Customer balances were not affected and customers were not able to perform unauthorised actions or move money on anyone else's account.

I have set out more fully the detail of the IT change and how it led to the issue in answer to Question 8. The timeline of the incident and our immediate response on Thursday 12 March was as follows:

- 03:28 – overnight IT change completed, causing the issue (please see Question 8).
- 06:20 – IT investigations and recovery began, following early customer reports.
- 08:08 – the issue was resolved, with no transactions showing incorrectly after this point.
- 08:12 - we began responding to individual customers raising the issue on social media with a message reading "*We're sorry about this. Some customers are having issues viewing balances & transactions in internet banking and in the app. Bear with us as we fix this.*"
- 09:00 – guidance issued to colleagues to help them answer direct enquiries from customers (e.g. by telephone).
- 10:38 - social media response message to individuals updated to "*This morning we incorrectly showed transaction information from some accounts to other customers in Internet Banking and the mobile app. We're sorry this happened. This issue was quickly identified and resolved. We can assure you that nobody had access to your accounts. We're currently reviewing what happened to ensure this cannot occur again. Protecting our customers' personal information and account security remains our priority.*"
- 17:27 - social media response message to individuals updated to "*Earlier today, some customers briefly saw some transactions that weren't theirs. We're really sorry – the issue was fixed quickly and there's no action needed. No one could access anyone else's account. We're reviewing what happened to make sure it doesn't happen again.*"

• Monday 16th March 15:09 - pinned social media message: "*On 12th March, a limited number of customers using our app may have briefly seen transactions that weren't theirs due to an internal IT change. We're very sorry this happened. No action is needed and there was no account security issue. We've identified the affected customers and will contact them to provide further information.*" The message remained pinned until 20 March at 9pm.

We continued to closely monitor the service, and the issue did not recur. We also have ongoing monitoring measures in place.

2. A description of the information that has been incorrectly presented to people other than the correct account holder, including whether it was limited to just information about transactions or whether other personal information, including National Insurance numbers, was released;

3. Whether it is possible to identify those whose information has been incorrectly passed on to others, and if so, how you will communicate with those customers;

4. The number of customers that have been affected by the incident. This should be separated into the number of people who saw other people's information, and the number of people whose information was erroneously provided to others, if possible.

I thought it might be helpful to group these questions together.

Types of information visible

Customers experiencing the issue could have seen different types of information depending on whether they simply clicked into their current account to see their list of transactions (level 1), or whether they additionally clicked on an individual transaction within that list (level 2). At each level, the information that could have been seen by customers affected by the issue was their own transaction information and/or transaction information from one or more other account holders.

At the first level, the transaction list, the information that customers may have been able to see was:

- the amount of money involved with a transaction;
- the date of a transaction; and
- a payment identifier representing the payer, payee or merchant involved. This identifier may have included additional details provided by the sender. This could include National Insurance numbers, for some payments.

At the second level of viewing, where customers clicked on individual transactions, they will have been able to see additional information. The data they may have seen would vary depending on the nature of the transaction viewed, so could potentially have included:

- the sort code and account number of a person being sent a payment (and equivalents for payments abroad);
- the sort code and account number of an account from which a payment originated for transfers between Lloyds Banking Group accounts held in the same name;
- National Insurance numbers or vehicle registration numbers where these were used as a payment reference (e.g. by government bodies);
- text entered in a "reference" field.

In some cases, the transaction information visible may have related to individuals who are not Lloyds Banking Group customers, for example in an instance where a payment was made from a Lloyds Banking Group customer account to an account holder at another bank.

As set out above, although this information should not have been visible, customers' account balances were not affected, and customers were not able to perform unauthorised actions or move money on anyone else's account. Customers who experienced the issue would have been able to view others' data momentarily, and the information that was visible would not be sufficient on its own for someone to carry out fraud against an individual's bank account. Our assessment is that it is also very unlikely the information potentially viewed could be used to carry out fraudulent activity more widely. We are providing this reassurance to customers.

We have sophisticated fraud detection capabilities and monitoring in place at all times. We have not identified any evidence of fraud occurring as a result of this incident but will continue to monitor closely. If customers are concerned about any transactions they can contact our helpline 24/7 on 0345 300 0000 or message us via the app.

Numbers of customers

Of our 21.5m mobile banking users, 1.67m logged into our mobile banking apps while the incident was ongoing. Not all customers logging in experienced the issue. We have identified all but a small number of Lloyds Banking Group customers whose transactions could have been viewed by other customers in error. In addition we have assessed how many customers viewed individual current account transactions.

We assess that a maximum of 447,936 customers who viewed their transaction list during the affected time period may have been presented with other people's transactions or may have had some of their transactions presented on another customer's transaction list (described as level 1 above). We assess that a maximum of 114,182 customers clicked through to view the detail behind individual current account transactions during that time and may have been presented with information about individual payments (described as level 2 above).

Since the incident, we have alerted our customers via social media and from today all Lloyds Banking Group customers who may have viewed other people's transactions or had their transactions incorrectly seen by others will be alerted in their app.

5. What steps you are taking to encourage those who may have taken copies of data to which they were not entitled to delete it:

Following the incident we have alerted our customers via social media, and from today our customers who may have viewed other people's transactions, or had their transactions incorrectly seen by others, will see an alert when they log in to their app.

As part of this communication, we are making it clear that if our customers recorded or shared any information relating to another individual – for example by taking screenshots, posting online, or writing it down – it should be deleted. There is currently no evidence of misuse or malicious activity as a result of the incident through our fraud and cyber monitoring processes.

6. The amount of compensation that Lloyds Banking Group has so far paid related to this incident and to how many people, and whether Lloyds Banking Group will be proactive in providing compensation to those who may at present not know they have been a victim of this data breach:

Based on our assessment of this incident, we have not identified evidence that customers have suffered financial loss, and no customer has reported a financial loss arising from the incident at this stage. Accordingly, we have not made compensation payments on this basis. However, we would of course address any claims for financial loss and associated compensation promptly.

Separately, it is our existing practice that we may make goodwill payments for distress and inconvenience in individual cases, for example where there has been a direct impact on an individual. We have made goodwill payments totalling just over £139,000 to around 3,625 customers as of 23 March. Our customer service teams are continuing to respond to enquiries. We are supporting customers in line with our responsibilities under the Financial Conduct Authority's rules.

7. When Lloyds Banking Group first informed the Financial Conduct Authority and the Information Commissioner about this breach:

We contacted the Financial Conduct Authority, the Prudential Regulation Authority and the Information Commissioner's Office on the morning of the incident, 12 March. We then continued to provide updates to the FCA and PRA as part of our active incident management processes. We submitted formal notification to the Information Commissioner's Office within 72 hours, in line with statutory timelines.

8. Your initial explanation of the reason for this failure of data protection:

The incident was caused by an IT change made overnight between 11 and 12 March which introduced a software defect. As set out above, the defect meant that when a customer requested to view their current account

transactions, their transaction data was potentially visible to other customers who were simultaneously - within small fractions of a second - requesting access to their own transactions. We have established that the defect was in the design of the code used to update the Application Programme Interface (API) used by the app. We are reviewing why this individual defect was not detected by our design, quality assurance and testing processes.

Our priority now is to complete our full analysis, continue to engage with our customers, and ensure that we address our responsibilities towards them in full. We will also seek to learn any lessons and update our processes as a result of this incident.

I hope this provides the Committee with an understanding of the incident that occurred, our immediate assessment of its cause and number of customers involved, and the steps that we are now taking to support them. We will update the Committee further at the intervals requested.

If you have any further questions, then please let us know.

Yours sincerely,

Jasjyot Singh OBE
CEO, Consumer Relationships
For and on behalf of
Lloyds Banking Group