THE LEVESON INQUIRY
WITNESS STATEMENT FOR PART 1

WITNESS STATEMENT OF JONATHAN FRANCIS SHAWCROSS

I, Jonathan Francis Shawcross, Director of Group Security and Fraud, Lloyds Banking Group, 48 Chiswell Street, London, EC1Y 4XX, say as follows:

1. On 21 November 2011, I received a section 21(2), Inquiries Act 2005 notice from the Leveson Inquiry team ("**the Inquiry Notice**"), requiring my response, on behalf of Lloyds Banking Group ("**Lloyds" or "the Bank"**) to a number of questions regarding "blagging".

2. I subsequently tasked members of my team to investigate and report back to me on the questions set out in the Inquiry Notice.

3. In carrying out this task, my team has adopted the following approach:

    a. The team has construed "blagging" as the process by which one person seeks to obtain confidential information from another, through covert means, for example, by pretending to be someone else.

    b. The team has focused its attention on approaches to obtain confidential information where these approaches involve direct contact with a member of the Bank's staff, either in person or over the telephone. The team has not taken into account attempts to obtain confidential information by other means which do not involve personal contact with Bank staff, for example through electronic access via the internet.

    c. The team has also focused its attention on attempts to obtain Lloyds' customers' personal data. Accordingly, the team has not taken into account attempts to obtain other types of confidential information, for example, confidential corporate information relating to how Lloyds conducts its business.

4. My response to each of the questions posed by the Inquiry Notice is set out below. My response should be read in the following context:

    a. Lloyds was established in January 2009, following the merger of Lloyds TSB PLC and Halifax Bank of Scotland PLC (HBOS).

b. Like other large financial institutions, Lloyds is a target for financial crime, including fraud.

c. The Bank holds a large number of records across a number of divisions and functions which relate to the detection and prevention of financial crime. These records span across the different banks (each with differing record-keeping systems) which now form part of Lloyds. Key records include:

   i. records which indicate when security of customer data has been compromised, in circumstances where accounts have been accessed and funds fraudulently withdrawn;

   ii. telephone banking records which indicate when a caller has failed customer verification procedures;

   iii. records of completed 'approaches to staff' forms which have been used within Lloyds from 2008 to record illegitimate approaches made to staff by an external source to acquire customer data ("**Colleague Approach Forms**"); and

   iv. case management systems recording details of internal investigations carried out by the Group Security and Fraud Division.

d. Given the volume of data held across different record-keeping systems and relating to different entities within Lloyds, my response reflects my team's findings based only on the conduct of reasonable enquiries in the time available, and not on an exhaustive search of Lloyds' systems and records in their entirety.

Question 1: Who you are and a brief summary of your career history.

5. I joined Lloyds Banking Group in April 2010 to undertake my current role as Director of the Group Security and Fraud Division. Prior to taking up this employment, I was employed by the Royal Bank of Scotland as COO, Group Functions and before that as Global Director, Security & Fraud. Prior to this, I undertook a variety of roles within RBS and previously NatWest, within their Back Office Operations. These have included roles as Head of Communications; Head of Customer Management – Cash & ATM Operations; Manager, Group Operations Strategy and Manager, Telephone Banking Strategy.

6. As Director of Group Security and Fraud, my responsibilities include ensuring that the customers, colleagues and property of Lloyds Banking Group are adequately protected against preventable loss, theft, fraud,

wider financial crime and unforeseen circumstances. This includes ensuring that the appropriate measures are in place to protect against unauthorised access to customer data.

Question 2: Whether your financial institution is or has been targeted by persons seeking to "blag" confidential data from your organisation? For the purposes of this request please go back at least 10 years.

7. For the following reasons, it is difficult to state with any certainty whether and to what extent Lloyds has been targeted over the last 10 years by persons seeking to "blag" confidential data from our staff members.

8. Lloyds takes the protection of its customer data very seriously. There are a large number of security measures and controls embedded within Lloyds for the purposes of the prevention and detection of financial crime. These security measures and controls help to ensure that customer data is protected against unauthorised access or misuse. Further details of these measures are set out in my response to question 4 below.

9. Whilst the Bank holds a large number of records relating to attempts made to breach the Bank's systems and controls and to access customers' personal data, it is difficult to ascertain from those records whether, and to what extent, these attempts were made for the purposes of financial crime (for example, to appropriate money from a customer's account) or for some other purpose, such as to inform a media article.

10. The Bank records which I describe in paragraphs 4(c)(i) to 4(c)(iv) above help to show where an unsuccessful attempt was made to access customer data. However the Bank would not necessarily know the underlying reason for the attempt to access the data. Where the attempt was successful, the Bank might be able to deduce the purpose of the attempt – for example if funds were misappropriated from a customer's account, the Bank could deduce that the purpose behind the attempt to access customer data was fraud. However, where the attempt was unsuccessful, the Bank would not be able to determine whether the attempt was for a fraudulent purpose or for some other[1] purpose. Neither would the Bank necessarily know whether the attempt to access the account was made through "blagging" or by some other means.

11. However, from the enquiries carried out by my team, I believe that Lloyds has been the subject of at least one "blagging" approach. I have described this approach in paragraphs 19 to 20 below.

[1] For example, an account holder might attempt to access his or her account but might fail the customer authentication process for some reason (e.g. he or she forgets his password).

Question 3: If so, please give an indication of the scale of the problem, the types and sophistication of "blagging" attempts that are made, the types of data that are sought, who by, who for and any other particulars that will assist the Inquiry to assess the nature and scale of the problem.

12. In order to assist me with the response to this question, my team have reviewed:
    a. a summary of the Staff Approach Forms described in paragraph 4(c)(iii) above;
    b. a key case management system within the systems described in paragraph 4(c)(iv) above.

Staff Approach Forms

13. The Colleague Approach Forms began to be used in 2008, and were rolled out within Lloyds Banking Group as it expanded. These forms are required to be filled in by any member of staff who has been the subject of an apparently illegitimate approach (typically involving face to face contact), for customer information. The forms require full detailed descriptions of the individual making the approach, the nature of the approach (including what information was asked for and whether any inducement was offered or threats made) and a full description of events.

14. My team has reviewed a summary of the Staff Approach Forms as part of gathering our response to your notice. Since 2008, there have been 57 incidents of illegitimate approaches to staff for customer information recorded in the Colleague Approach Forms. Of those, an inducement of money was recorded to have been offered in 21 incidents. In the remaining 36 cases, either small gifts (such as a pint of beer) were offered or the records did not detail any inducements (this could be because the conversation was terminated before an inducement was offered – staff are encouraged to terminate any such inappropriate conversations as soon as possible – or because the information was omitted, for whatever reason, by the member of staff filling in the form). In all 57 instances it is not possible to conclude whether approaches to staff are made by or on behalf of the media, or in fact, by those looking to perpetrate fraud.

Case Management Systems

15. Historically, different constituent parts of Lloyds Banking Group operated differing case management systems and records (which recorded information in a varying manner), with differing record retention periods. My team has reviewed one of the major case management systems used to record Group Security and Fraud investigations relating to a large part of the Bank. The records span across a period of 8 years (the period for which such records are retained according to internal

requirements). In respect of that system, three different types of cases are recorded:

a. significant cases requiring the direct intervention and leadership of the Group Security and Fraud function;

b. lower priority cases which are investigated in other areas of the bank with guidance and support from Group Security and Fraud; and

c. intelligence reports which as they stand do not contain enough information to instigate an investigation but which the team consider noteworthy for future reference.

16. A key word using relevant words such as 'press' and 'media' revealed only one potentially relevant incident described in paragraph 19 to 20 below.

17. A number of disparate systems are also used to record Group Security and Fraud investigations in other parts of the Bank. Given the limited time available and my teams' and my view that these systems are not likely to hold relevant information – we consider over 90% of unauthorised approaches to our banking staff for confidential customer data would be for reasons of financial crime (and the small remaining number of cases for reasons connected to personal or family disputes) – the most effective method for my team to consider such records was to hold a discussion with those colleagues who were involved in the investigations recorded in those systems. The team could not recall any examples of the types of incidents under discussion.

2006 criminal investigation

18. From the reviews described above, there is only one incident which my team has been able to identify as being (apparently) an attempt to "blag" confidential data from our staff, as follows.

19. In 2006, during a high profile police criminal investigation, our organisation became aware of a number of calls made to a range of the Bank's branches in different geographic locations, within a short period of time, by someone claiming to be a member of staff. The staff members who took the calls all recalled being told a similar story, namely that the caller worked in another part of the organisation and that their IT systems were down and they urgently needed some customer information to complete a task[2]. Additionally, calls were also made to the Bank's telephone banking centre by someone claiming to be an actual customer. The caller initially failed to pass the required security checks, although the caller ultimately gained access to account

[2] A subsequent internal investigation failed to reveal any IT faults in the relevant department, or that there were any outstanding tasks on the customer's account.

information. In all cases the caller appeared to be seeking information about a suspect.

20. An internal investigation was undertaken. The investigation records indicate that the Bank was unable to trace the caller and that we did not identify any wrongdoing by internal staff. Given the level of public interest at the time in the police case, it was assumed that the caller was a member of the press.

Question 4: What measures does your organisation presently take in order to prevent "blaggers" from obtaining confidential data?

21. A critical component of Lloyds operational risk framework is the protection of the Bank's information. Another key aspect of Lloyds' operational risk framework is the detection and prevention of financial crime generally, including fraud.

22. There are a number of systems and controls embedded in the organisation, which implement Lloyds' operational risk framework in respect of financial crime and information security. The Bank considers the systems and controls appropriate for the size and business of our organisation, and have implemented these to meet the expectations of our customers and to comply with legal and regulatory requirements.

23. Of these systems and controls, the main ones which help to prevent "blaggers" from obtaining confidential information are the Bank's Customer Verification Procedures. These measures vary depending upon how the customer chooses to interact with the bank (for example, signatures are used heavily in branch transactions but are clearly not appropriate for Telephone or Online Banking) and vary according to the level of risk (e.g. additional checks may be initiated for financial transactions). In Telephone Banking, account access is normally obtained through providing 2 out of 6 digits of a Personal Security Number (PSN) into an automated system. If these digits are correctly entered the caller can obtain basic balance & transactional data and can make payments. If the caller does not know the PSN or if there is no PSN associated with the account, the caller must speak to a bank colleague and answer questions regarding the account and its usage.

24. Additionally, staff are obliged to keep customer data confidential and are expected to escalate attempts to breach security – for example, staff are required to complete and return a Colleague Approach Form when they are subject to an unauthorised physical approach for customer data.

25. Finally, unauthorised disclosure of information by Lloyds Banking Group Staff constitutes a breach of group policies and procedures which may result in disciplinary action, up to and including dismissal.

Question 5: Have any of your staff (i.e. your staff whether casual or permanent) in the last 10 years been caught and/or disciplined for disclosing confidential data to third parties? If so, please provide particulars. This request is particularly directed at third parties who directly, or indirectly, have sought to corrupt your staff in order to obtain confidential data for any manifestation of the media.

26. The Group Security and Fraud investigations team carry out investigations in the event of suspected wrongdoing by members of staff. This would include investigations into the unauthorised provision of customer data.

27. My team have conducted a number of investigations in connection with the unauthorised provision of customer data over the last 10 years (such cases are typically escalated to my investigations team where fraud appears to have been committed) and have reviewed the relevant case management systems recording details of these cases. My team inform me that to the best of their knowledge and belief, there are no recorded instances of staff being disciplined because they were the subject of a "blagging" attempt by or on behalf of the media.

Statement of Truth

To the best of my knowledge and belief, the facts stated in this witness statement are true.

DATED the 2nd day of December 2011

SIGNED:

Jonathan Shawcross
Director, Group Security and Fraud
Lloyds Banking Group