THE LEVESON INQUIRY INTO THE CULTURE, PRACTICES AND ETHICS OF THE PRESS

BARCLAYS BANK PLC

WITNESS STATEMENT OF GARETH JOHN DAVIES

I, **GARETH JOHN DAVIES** of [redacted] will **SAY** as follows:

1. I am employed by Barclays Bank Plc ("Barclays") as Group Head of Information Risk Management and I have held this position since August 1st 2011. My current role involves responsibility for the management of information in its many forms across Barclays. Prior to August 1st 2011, I was Global Head of Risk and Control for the Chief Operating Officer of the Retail and Business Bank arm of Barclays. That role was a combination of direct management and oversight responsibility for all aspects of Risk and Control Management for the Global COO.

2. The facts and matters within this statement are either within my own knowledge in which case they are true or are derived from the information sources within Barclays Bank Plc in which case they are true to the best of my knowledge, information and belief.

3. There is now produced and shown to me and marked "GJD1" a bundle of numbered copy documents. In my statement, I refer to various documents within this bundle.

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.

4. "Blagging" attempts, whereby individuals attempt to elicit confidential information through impersonation, coercion or some other mechanism, are a common occurrence across financial institutions. Like every other bank in the UK, Barclays experiences attempts by unauthorised 3rd parties to access customer information and carry out fraudulent transactions. This is not a new phenomenon. For this reason, we have comprehensive and risk-based identity management controls in place, including secret passcodes and our PINsentry authentication device, to protect our customers' data.

5. The drivers behind these attacks vary and the Bank has observed that the frequency of attempts is often affected by macro-level conditions such as the overall economic climate, increased media publicity, organisational or operational changes etc. "Blaggers" may be attempting to capture information for the purpose of financial gain (e.g. fraud or identity theft), or to gain a competitive advantage (e.g. commercial espionage, recruitment). The former is typically most common. The most frequest "blagging" attacks observed across the Bank pertain to individuals seeking to capture customer data with a view to committing fraud. The purpose of the majority of such fraudulent attempts is for personal financial gain. These attempts may be targeted at customer-facing staff, or indeed at customers themselves. The majority of unauthorised attempts take place within our contact centres and these are normally prevented by the controls that are in place.

6. The Bank participates in numerous industry forums (for example the Information Security Professionals network and I4) to share observed incidents with peer organisations and monitor these against industry trends; to date, the experiences across Barclays appear in-line with those across the financial industry.

7. Barclays is defined as a data controller under European data protection legislation and is consequently required to implement appropriate technical and organisational measures to protect personal information. The security and protection of customer information is also overseen by other regulatory institutions, including financial services regulators (in the UK

this includes the Financial Services Authority). In addition to this, we are subject to the common law duty of confidentiality. Barclays considers the fair and lawful treatment of personal information as key to its business and a prerequisite for the achievement of its strategic aims. We take our legal and regulatory obligations seriously and have developed robust policies, practices and training to ensure the protection of personal information.

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.

8. The problem is well understood within Barclays across a spectrum of attack vectors, including telephony and/or email, online and in person.

9. Physical "blagging" attempts can involve impersonation of customers in branches in order to get access to customer accounts and data, or impersonation of permanent or auxillary staff to gain access to buildings. Online "blaggers" may try to exploit the Barclays brand in phishing attacks aimed at luring customers into divulging sensitive information on fake websites, or may exploit data available on social media sites such as LinkedIn and Facebook to develop more sophisticated attacks.

10. Fraudsters may attempt to elicit organisational data or details of staff for industrial espionage or for recruitment purposes (e.g. staff poaching, head-hunting).

11. In December 2009, the Bank was targeted by reporters from the Sun Newspaper, who attempted to blag details of high-profile customers from contact centre staff. This became the basis of a story purporting to show the ease with which account information could be "blagged" in the telephony authentication process. Immediate steps were taken to enhance our controls and engage with the Information Commissioner's Office ("ICO"). The ICO investigated the incident to ensure customer identification and verification processes were sufficiently robust (see "**GJD1**" documents 1, 2,

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

12. Barclays employs a broad suite of controls to protect confidential data from "blaggers". Physical access controls are in place to prevent unauthorised access to our premises and buildings. Data is secured appropriately across the organisation and a range of policies and controls are in place to thwart any opportunistic "blagging" attempts within the enterprise, these include: security policy; data classification schemes and supporting guidelines to ensure employees handle data appropriately in accordance with its confidentiality; clear desk policy; automated locking of unattended computer screens and a social media policy to ensure employees do not divulge sensitive information when interacting on social networks. Waste paper is secured in confidential waste bins until it is collected for secure destruction. Robust processes are in place to ensure employees are appropriately screened before commencing employment, to weed out individuals with any history of compromising confidential data from the outset. Photo identification badges are carried by all staff and visitors are accompanied at all times and escorted off the premises when their business has concluded.

13. In branches '2-factor authentication mechanisms' are employed to prevent "blaggers" from impersonating customers. Before getting account access, every customer must use his/her bank card in combination with a unique banking PIN to validate his/her identity via the Barclays PINSentry device. Contact centre staff follow strict scripts with a range of authentication questions to verify customer identities and refer any suspicious calls to dedicated fraud teams. Barclays Capital also has a dedicated 24x7 social engineering hotline to which employees can refer any suspicious calls and an online chat channel for reporting "blagging" incidents.

Technical controls are in place to monitor sensitive data leaving the organisation perimeter via email and incident management processes are embedded to ensure a cohesive response to "blagging" attempts. The Bank leverages the services of online brand monitoring services to keep track of its online presence and identify fraudulent websites set up for phishing purposes in order to close them down to protect its customers.

14. A range of training materials are in place across the Bank to ensure employees are fully aware of the issue and understand the associated risks. A number of awareness campaigns have also been run to heighten awareness and embed a culture of data security. These include:

14.1 "Faking It": a campaign run between December 2009 and April 2011 across all UK-based contact centres to highlight the risk of blagging and ensure agents refer suspicious calls on. The campaign has seen a 123% rise in the number of referred calls, indicating awareness of the issue has been significantly heightened. The approach was shared with industry groups to support a broader response to the issue and we are currently exploring opportunities to extend the campaign to offshore contact centres (see "**GJD1**" documents 4, 5, 6).

14.2 "Think Privacy": endorsed by the Information Commissioners Office and extended into an industry-wide consortium, this campaign focused specifically on protecting sensitive information through changing employee behaviours and ensuring a better level of awareness of data privacy requirements (see "**GJD1**" documents 7, 8, 9, 10, 11).

14.3 "The Risk": an award-winning campaign which includes messages on how employees should modify behaviour in order to reduce the threat of social engineering. The initiative focused on a broad range of general information risk issues and included messages to ensure employees do not share sensitive data inappropriately (see "**GJD1**" documents 12 and 13).

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.

15. All Barclays employees are required to adhere to various Company-mandated employment policies. These policies include employee conduct regarding confidential information, be it customer or Company confidential data, and employee interaction with the media.

16. Where Barclays becomes aware of a potential breach of these (or any of its) employment policies we fully investigate the issues involved to determine whether a formal disciplinary process is warranted. If appropriate, a full disciplinary process is then completed, during which the employee's version of events is sought, and is tested against the evidence. Thereafter, a decision on a disciplinary sanction (if at all) is made and communicated to the employee. Where an employee is caught disclosing confidential information to the media the investigation and disciplinary processes are completed.

17. The Barclays United Kingdom Employee Relations teams ("the Teams") reviewed their employee case records to consider whether any employee in the last ten years had been

disciplined for disclosing confidential information to the media ("the Review"). The Teams encountered several issues in completing the Review:

17.1 Across Barclays individual business units operate bespoke Records Retention Policies, in order to comply with the employer duty in the Data Protection Act 1988, to hold personal information for no longer than is necessary. Under these policies Barclays generally only holds information on its (ex) employees for three years post termination of employment.

17.2 Several business units use a central system to store staff employment records. However, this system does not itemise the type of disciplinary action (including dismissal) an employee may be subject to. The system records only basic information, such as employee name and staff number. Specifically, it does not code disciplinary action (including dismissal) by type (e.g. dismissal for disclosing confidential information).

17.3 The Teams called on corporate knowledge of cases caught by the Review.

18. There is one case that involved disclosure of information to the media. In 2009 an employee was dismissed for disclosing confidential information to the Sun Newspaper ("the Sun").

19. At a meeting in October 2009 a 'current state assessment' was given by a Team member. This update included a synopsis of emerging tax fraud 'scams',

20. An employee who attended the meeting later contacted the Sun to tell them about the 'scam' and details thereof. This disclosure was unsolicited. Barclays became aware of the disclosure when the Sun contacted our Media Relations Team asking questions about the fraud

21. An internal investigation was conducted, in which the employee admitted emailing and then speaking with the Sun about the fraud [redacted] The employee was then suspended from work. A formal disciplinary hearing followed. At this hearing the employee admitted that in his telephone call with the Sun he disclosed that he worked for Barclays and the name of the [redacted] Team Member giving the update. The employee also confirmed that his motivation for contacting the Sun was to highlight his perception that HMRC were not doing anything about the fraud losses as the amounts at hand were not substantial enough.

22. The employee's response was considered, before a decision to immediately dismiss him was taken. The dismissal was based on the employee's breach of Barclays policies on disclosure of confidential information and speaking with the media [redacted]

23. The contents of this statement are true to the best of my knowledge and belief.

Signed [redacted]

Dated 1 December 2011