Financial Services Authority

FINAL NOTICE

To: **HSBC Life (UK) Limited**

Of: 7th Floor, Norwich House
Nelson Gate, Commercial Road
Southampton
Hampshire
SO15 1GX

Date: 17 July 2009

TAKE NOTICE: The Financial Services Authority of 25 The North Colonnade, Canary Wharf, London E14 5HS ("the FSA") gives you final notice about a requirement to pay a financial penalty.

1. THE PENALTY

1.1. The FSA gave HSBC Life (UK) Limited (HSBC Life or the firm) a Decision Notice on 2 July 2009 which notified the firm that, pursuant to section 206 of the Financial Services and Markets Act 2000 (the Act), the FSA had decided to impose on it a financial penalty of £1.61 million. This penalty is in respect of the firm's breaches of Principle 3 of the FSA's Principles for Businesses which occurred between 1 January 2006 and 28 March 2008 (the Relevant Period).

1.2. The firm confirmed on 12 June 2009 that it will not be referring the matter to the Financial Services and Markets Tribunal.

1.3. Accordingly, for the reasons set out below and having agreed with the firm the facts and matters relied on, the FSA imposes a financial penalty on the firm in the amount of £1.61 million.

1.4. The firm agreed to settle at an early stage of the FSA's investigation. It therefore qualified for a 30% (Stage 1) discount under the FSA's executive settlement procedures. Were it not for this discount, the FSA would have imposed a financial penalty of £2.3 million on HSBC Life.

2. REASONS FOR THE ACTION

2.1. In the Relevant Period, HSBC Life breached Principle 3 by failing to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. HSBC Life did not take reasonable care to establish and maintain effective systems and controls to manage the risks relating to data security, specifically the risk that confidential customer data might be lost or stolen.

2.2. Within particular parts of its business, HSBC Life failed to undertake an adequate assessment of the risks relating to data security, failed to assess whether its existing controls were adequate to manage these risks, and failed to implement adequate and effective procedures, guidance, training and monitoring to address these risks.

2.3. In particular HSBC Life failed to ensure that one of its departments had in place adequate and effective procedures, guidance and resources to ensure that:

(1) customer data sent to third parties on portable electronic media (e.g. CDs, disks and USB devices) was secure in the event that the data was lost or intercepted; and

(2) customer data kept in its offices was at all times secure from the risk of internal fraud or theft.

2.4. HSBC Life's failure to properly assess these risks and to implement robust systems and controls to deal with them increased the risk that its business could be used for purposes connected with financial crime and exposed its customers to the risk of being victims of financial crime.

2.5. The weak controls surrounding data security resulted in practices that placed customer data at risk of loss or theft in that:

(1) HSBC Life's Finance department routinely sent unencrypted CDs containing significant amounts of confidential customer data to third parties by unrecorded delivery; and

(2) notwithstanding that access to the firm's offices was securely restricted, confidential customer data held by the same department was routinely kept in unlocked cabinets. This included unencrypted electronic copies of more than 740,000 "live" policies and over 1 million "non-live" policies.

2.6. These failures contributed in February 2008 to the loss by HSBC Life's Finance department of an unencrypted CD sent through the post by unrecorded delivery. The CD contained confidential data of 180,000 policy holders. Although some technical skill was required to interpret the data, it included names, ages, sex, dates of birth, smoker status, policy numbers, the same details for joint policy holders, premia and sums assured. Although a member of staff was aware that the CD had not arrived on

11 February 2008, its loss was not formally escalated within HSBC Life until over a month later, on 20 March 2008.

2.7. The FSA considers these failings to be particularly serious because:

(1) During the Relevant Period, HSBC Life had over 740,000 customers. This included not only individual customers but also corporate customers where large numbers of individuals participated in corporate life, investment and insurance schemes or policies. All of these individuals are entitled to rely on HSBC Life to take reasonable care to ensure the security of customer data entrusted to it. The failure to have appropriate data security controls had the potential to expose these individuals to the risk of identity theft and financial loss.

(2) The failures occurred following a period of heightened awareness of financial crime issues as a result of government initiatives, increasing media coverage and a FSA campaign about the importance of financial crime within the financial services sector. Further, HSBC Life was aware that data security and the associated risks of fraud and identity theft were increasing problems for the financial services industry but failed to take sufficient steps within the Relevant Period to ensure that all of its data security procedures were adequate and robust enough to prevent customer data being mislaid and potentially released into the public domain.

2.8. The cumulative impact of the failings represented a material risk to the FSA objective of protecting customers and reducing financial crime.

2.9. HSBC Life's failures therefore merit the imposition of a significant financial penalty. In deciding upon the level of disciplinary sanction, the FSA recognises that:

(1) in response to the data loss incident HSBC Life reported the matter to the FSA, contacted all 180,000 individuals affected by the data loss and strengthened its caller identification procedures; and

(2) the firm subsequently notified the FSA about deficiencies in its controls surrounding data security.

2.10. In addition, HSBC Life has taken significant and proactive steps since the data loss incident to revise its procedures and controls, which have served to mitigate the seriousness of its failings. In particular, the firm has:

(1) provided for compulsory encryption on all electronic data transfers and given clear instructions to its staff on when and how to apply encryption;

(2) enhanced physical security in its offices by installing lockable cabinets in every office;

(3) enhanced data security awareness by revising induction training for new staff and requiring all existing staff to undertake annual data security refresher training;

(4) introduced an Information Security forum as a sub-committee to the formal risk committee structure;

(5) implemented procedures to further restrict the ability to download data to portable devices; and

(6) introduced the dedicated role of Business Information Risk Officer, including assessing ongoing performance against 18 key information risk indicators.

2.11. HSBC Life has also co-operated fully with the FSA in the course of its investigation.

3. RELEVANT STATUTORY AND REGULATORY PROVISIONS

3.1. Under section 206(1) of the Act, if the FSA considers that an authorised person has contravened a requirement imposed by or under the Act, it may impose on him a penalty, in respect of the contravention, of such amount as it considers appropriate.

3.2. Under section 2(2) of the Act the reduction of financial crime is a regulatory objective for the FSA.

3.3. The FSA's Principles for Businesses constitute requirements imposed on authorised persons under the Act.

3.4. Principle 3 of the FSA's Principles for Businesses states that:

"A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems."

4. FACTS AND MATTERS RELIED ON

Background

4.1. HSBC Life (UK) Ltd is a wholly owned subsidiary of the HSBC Group of companies (HSBC Group). HSBC Life has been authorised by the FSA to perform a number of regulated activities since 1 December 2001. HSBC Life is authorised by the FSA to perform investment and insurance activities and is a provider of life and pension products for HSBC Group members, which are sold to individual and corporate customers.

4.2. HSBC Life holds large amounts of financial and personal data about its customers. This is frequently exchanged with third parties, such as reinsurance firms, solicitors and medical record bureaus.

4.3. Throughout the Relevant Period, HSBC Life had over 740,000 customers, which were a mixture of individual and corporate customers. It held data for more than 1 million other individuals as the firm retained data for "non-live" policies, which included inactive policies or single premium policies that had not reached maturity.

4.4. The types of confidential customer data held by HSBC Life and handled by or accessible to its staff variously includes:

(1) full name, title and gender;

(2) date of birth;

(3) full address;

(4) National Insurance number;

(5) associated medical and claim records; and

(6) product and policy information such as: policy numbers, expiry/maturity dates, the amount and frequency of payments made and details of the debited bank account.

4.5. As part of its regular business, HSBC Life's Finance department sent monthly electronic reports of current life policies to reinsurance firms. In most cases, the reports were accessed by the reinsurer via a secure electronic "mailbox" system. These reports contained details of "live" policies administered through particular reinsurers. The policy data included names, ages, sex, dates of birth, smoker status, policy numbers, the same details for joint policy holders, premia and sums assured. However, one reinsurer was unable to utilise this secure system. Accordingly, HSBC Life staff each month copied the reports on to a CD and sent the CD to the reinsurer by post:

(1) the CD typically contained policy data for approximately 260,000 individuals and approximately 1,900 claimants;

(2) throughout the Relevant Period, the data on the CDs was not encrypted and it was posted by unrecorded delivery.

Assessment of data security risk

4.6. Throughout the Relevant Period, HSBC Life failed to undertake an adequate assessment of the risks that customer data in its possession might be lost or intercepted and used for the purposes of financial crime, in particular whether its existing systems and controls were adequate to manage these risks.

4.7. The customer data held within HSBC Life was sufficient for criminals to use as a starting point to fraudulently redeem policies and to commit identity theft and other frauds.

4.8. In July 2007 HSBC Life received an email from its Head Office Compliance department which highlighted the risk to the security of customer data transferred to third parties by disc. It instructed staff to ensure that data security procedures were adequate and robust enough to prevent customer data being mislaid and potentially released into the public domain. Although HSBC Life undertook a review of its processes following receipt of this email, and the CEO asked for confirmation that all areas of the business address any gaps in the process, the Finance department was not included in this activity until a separate internal audit identified the relevant issues in January 2008 (see paragraph 4.29). Procedures were then implemented in March 2008.

Relevant systems and controls

4.9. During the Relevant Period, HSBC Life failed to take reasonable care to ensure that its data security procedures were adequate and robust enough to prevent customers being exposed to the risk of financial crime, especially in respect of the day-to-day working practices that affected data security.

4.10. HSBC Life failed to take care to adequately organise its procedures concerning data security. Its procedures were a complex amalgamation of HSBC Group mandated procedures and its own business-specific instructions. These were available to staff via links on the HSBC intranet. The procedures were inadequate in that:

(1) they covered a very broad range of information handling issues that were mostly focussed on compliance with the Data Protection Act 1998 (DPA) rather than the financial crime risks associated with the loss or theft of customer data (e.g. identity theft);

(2) the procedures concerning data security were inadequately organised and presented. HSBC Life's data security procedures were not contained in a single document but in a wide variety of documents and locations on the intranet. Staff had to find a number of different documents to understand the procedures in full; and

(3) they were conflicting and fragmented which could not have helped staff understand their responsibilities for data security.

4.11. The two key areas where customer data was exposed to the greatest risk of loss or theft were communications security (i.e. security of information sent by HSBC Life to third parties such as reinsurers) and physical security (i.e. security of information kept within HSBC Life's offices).

Communications Security procedures

4.12. During the Relevant Period, HSBC Life failed to have effective procedures in place and provide adequate guidance to staff concerning how to protect customer data being transferred out of the firm.

4.13. Procedures that were available during the Relevant Period were conflicting and lacked sufficient detail. For staff intending to send data externally, there were at least two differing standards of security requirements (password protection or encryption) between concurrent documents. A member of staff following one procedure could be unaware of the conflicting procedures in another document, which could lead to confusion and inconsistent practices being adopted by staff.

4.14. HSBC Life gave no guidance concerning the appropriate level of postal or courier service required for sending computer media such as CDs or discs containing customer data. Although this risk was identified in January 2008, HSBC Life did not implement a formal policy until March 2008.

Physical Security procedures

4.15. During the Relevant Period, although access to HSBC Life's offices was securely restricted to staff and independent contractors, the firm failed to provide adequate resources for staff to comply fully with the firm's procedures concerning the physical security of customer data.

4.16. HSBC Life staff had access to physical security guidance in the form of the "Branch Procedures manual". Although this was a guide aimed at HSBC branch staff rather than tailored to non-branch businesses, it was adopted by HSBC Life.

4.17. The procedures included clear desk policies and specific action points (for example, checking printers and faxes, clearing post and locking away customer data). However, the effectiveness of these procedures in protecting customer data was limited. Until the end of the Relevant Period, staff within the Finance department did not have readily available keys to lock cabinets, so customer data cleared from desks was left unsecured.

Staff training and guidance

4.18. During the Relevant Period, HSBC Life failed to provide adequate training to its staff to ensure that they were sufficiently aware of the risks of financial crime arising from the loss or theft of customer data. Staff were not provided with training which adequately addressed the data security risks arising in the course of their day-to-day duties.

4.19. HSBC Life did provide data protection training to staff during their induction, followed by refresher training every two years. However, this training material:

(1) focused on compliance with the DPA;

(2) did not address working practices in respect of information risk or data security; and

(3) addressed the role of HSBC branch staff, rather than being specifically tailored to HSBC Life departments or specific staff roles.

4.20. This generic data protection training was supplemented by some detailed step-by-step task-specific instructions, such as instructions for preparing reinsurance policy reports. However, the instructions did not address data security or alternative methods of completing the task (for example, in the event of system incompatibility or errors).

4.21. Throughout the Relevant Period, staff received email reminders of various procedures in the form of "Local Diary Cards". These were designed to act as aide-memoirs for best practice and contained links to related procedures on the intranet. Whilst a small number of these reminders related to data security risks (such as adhering to clear

desk policies and the need to display security passes), the effectiveness of the system was diluted by there being in excess of 150 different reminders in regular circulation, whilst action points, such as "*ensure all staff are aware of the procedure to follow if fraud is suspected*" were directed at managers.

Monitoring and review of adequacy of controls

4.22. During the Relevant Period, HSBC Life failed to carry out adequate monitoring and paid insufficient attention to the risks associated with lost or stolen customer data.

4.23. The monitoring of data security was inadequate to detect and deter all instances of poor working practices. Although monitoring was performed in accordance with risk-based principles, the framework of defined risks did not adequately cover data security and associated financial crime risks.

4.24. HSBC Life's Compliance department (Compliance) was responsible for monitoring data protection. Compliance team members attended regular meetings where data protection matters were discussed, along with other agenda items such as regulatory risks. These meetings included discussions on relevant regulatory matters including FSA Final Notices to other firms.

4.25. Compliance "Data Protection" reviews focussed on compliance with the DPA, rather than financial crime risks and the "Financial Crime" module looked predominantly at money laundering and fraud. Neither topic included consideration of internal risks, such as physical data security in HSBC Life's offices. The review of practices for sending data to third parties was not included until January 2008.

4.26. In addition, technical specialists such as IT Security administrators, were not involved in planning of, or involved in, subsequent reviews. This reduced HSBC Life's ability to detect weak practices and procedures or to identify technical risks such as weak password technology or encryption applications.

4.27. Prior to the Relevant Period, Compliance decided that data protection reviews should be treated thematically across the whole of HSBC Life and that it only needed to be addressed every two years. This was based on the belief that underlying data protection issues were relatively constant. This decision underlined the lack of understanding of financial crime risks, including those posed by changing technology.

4.28. In January 2008, Compliance undertook a data protection review across HSBC Life. Using a risk-based approach, the reviewers did not examine the Finance department that was sending CDs to reinsurers by post. The data loss which occurred later that month originated from the same department (see paragraph 4.34 below). The Finance department had previously been reported internally by Compliance in April 2007 for a Data Protection breach. Although a manual corrective process was put in place at the time, the breach was "*due to a lack of awareness*".

4.29. During the January review, Compliance identified a process of customer data being transferred externally without adequate risk or security assessment. The reviewer graded it as low risk, due to management plans to implement a revised policy. The risk to customer data was not addressed until a policy was implemented in March

2008. An HSBC Group Audit in February 2008 identified the issue of customer data being sent that was not secured as high risk.

Practices adopted by staff

4.30. In the absence of clear procedures, guidance and adequate training and monitoring, HSBC Life staff in the Finance Department adopted working practices that put customer data at risk.

4.31. Although there was a general awareness of the existence and location of HSBC Life's business procedures, the structure and content of available information (as described in paragraph 4.10 above) made it difficult for staff to find answers easily on the intranet.

4.32. The Finance department had established the practice of sending unencrypted data to at least one third party on an unencrypted CD by unrecorded delivery (as described in paragraph 4.5 above). This was a major risk to customer data security.

4.33. Although HSBC Life staff had access to detailed clear desk procedures and lockable cabinets were provided, and notwithstanding that access to HSBC Life's offices was securely restricted, Finance staff routinely left the cabinets storing customer data unlocked, due to a lack of available keys. The customer data left unsecured in this manner included unencrypted electronic copies of more than 740,000 "live" policies and over 1 million "non-live" policies in HSBC's "LifePen" system. This issue demonstrated a lack of staff and management awareness and diligence over simple financial crime precautions.

Data loss incident

4.34. In January 2008, a second reinsurance firm became unable to access the monthly policy data sent to it by HSBC Life electronically via its usual secure mailbox. On 31 January 2008, HSBC Life provided the data on CD by post, following the existing practice which it had adopted for the first reinsurer (see paragraph 4.5 above).

4.35. At the time the existing practice was to put the data into an electronic document, which was password protected and copied on to a CD. HSBC Life posted the CD to the second reinsurer by unrecorded delivery. The CD contained details of 369,000 policies, putting at risk the personal information of 180,000 individuals. The data included names, ages, sex, dates of birth, smoker status, policy numbers, the same details for joint policy holders, premia and sums assured.

4.36. The fact that the CD had not arrived at the second reinsurer was identified by HSBC's Global Service Centre on 11 February 2008, who contacted HSBC Life and requested another copy to be sent. This second copy was also unencrypted, but was this time sent by recorded delivery and arrived successfully.

4.37. Although the individual concerned discussed the incident with a colleague internally and was advised to escalate the matter, a formal alert that a data loss incident had occurred was not escalated within HSBC Life until over a month later on 20 March 2008.

4.38. The incident identified the following serious failings within the Finance department of HSBC Life:

(1) unrecorded and ill-defined practices that are not captured by internal reviews;

(2) minimal staff awareness of best practice concerning data security;

(3) poor understanding of electronic data protection techniques;

(4) no audit trails for bulk data dispatch and delivery; and

(5) slow data loss reporting.

4.39. Whilst there is no evidence that the lost data was compromised, the password protection applied to the data was very weak and could be easily circumvented. Although the data would have required some technical skill to interpret and did not include individuals' bank account details, it did, however, include sufficient information to potentially pass HSBC Life caller identification checks and thus expose the policy holders to the risk of policy take-over fraud and identity theft.

5. PRINCIPLE BREACH

5.1. By reason of the facts and matters set out above, the FSA considers that HSBC Life has contravened Principle 3 of the FSA's Principles for Businesses, namely that HSBC Life failed to take reasonable care to establish and monitor appropriate staff procedures concerning:

(1) the secure communication of customer data;

(2) the physical security of customer data in its offices;

(3) the level of training needed by its staff; and

(4) the monitoring of staff.

6. FACTORS RELEVANT TO DETERMINING THE ACTION

Relevant guidance on sanction

6.1. The FSA has considered the disciplinary and other options available to it and has concluded that a financial penalty is the appropriate sanction in the circumstances of this particular case. The principal purpose of a financial penalty is to promote high standards of regulatory conduct. It seeks to do this by deterring firms who have breached regulatory requirements from committing further contraventions, helping to deter other firms from committing contraventions and demonstrating generally to firms the benefit of compliant behaviour.

6.2. In determining the financial penalty proposed, the FSA has had regard to guidance contained in the Decisions Procedure and Penalties manual (DEPP) which came into force as part of the FSA's Handbook of Rules and Guidance (the FSA Handbook) on 28 August 2007. The FSA has also had regard to guidance contained in the

Enforcement Manual (ENF) which formed part of the FSA Handbook during the majority of the Relevant Period.

6.3. DEPP 6.5 sets out some of the factors that may be of particular relevance in determining the appropriate level of a financial penalty. Chapter 13 of ENF contains the equivalent guidance that was in effect during the Relevant Period. DEPP 6.5.1 G and ENF 13.3.4 G both state that the criteria listed in DEPP 6.5 and ENF 13.3 respectively are not exhaustive and all relevant circumstances of the case will be taken into consideration. In determining whether a financial penalty is appropriate and the amount, the FSA is required therefore to consider all the relevant circumstances of the case.

Deterrence

6.4. Deterrence is an important factor when setting financial penalties, particularly in cases where the FSA considers that Enforcement action taken in respect of similar breaches in the past has failed to improve industry standards. The FSA considers that the financial penalty imposed will promote high standards of regulatory conduct within HSBC Life and deter it from committing further breaches. The FSA also considers that the financial penalty will help deter other firms from committing similar breaches as well as demonstrating generally the benefits of a compliant business.

The nature, seriousness and impact of the breach in question

6.5. The FSA has had regard to the seriousness of the breaches, including the nature of the requirements breached, the number and duration of the breaches and whether the breaches revealed serious or systemic weakness of the management systems or internal controls.

6.6. The FSA considers that the failure to implement adequate and effective procedures across the firm, although particularly in the Finance department, is of a particularly serious nature (see paragraphs 2.1 to 2.7 above). For a period of more than two years the firm failed to take adequate care to consider the risks to customer data security. Reducing the extent to which it is possible for a firm to be used for a purpose connected with financial crime is one of the FSA's four statutory objectives. The FSA requires firms to undertake a risk-based assessment of financial crime risk and where necessary to implement controls to mitigate the risk.

6.7. The FSA considers that the fact that the control failures resulted in the loss of customer data is an aggravating feature of this case, but this is not the sole reason for imposing a penalty. The defects in the procedures alone are a cause of significant concern and routinely exposed customers to the risk of financial crime.

6.8. The FSA considers it particularly serious that the failures by the firm arose during a period of heightened awareness of financial crime issues. The profile of financial crime and customer data security has increased significantly in recent years and the FSA has issued several publications drawing public attention to these risks since November 2004. There have also been numerous high profile articles in the national and trade press, FSA speeches and papers as well as guidance from government and industry organisations.

6.9. Accordingly, the FSA considers the firm's failure during the Relevant Period to address the risks identified (with reference to both the publicly available information concerning the risk of data loss and the actual data loss at HSBC Actuaries) in a timely and appropriate way to be a serious failure.

The size, financial resources and other circumstances of the person on whom the penalty is to be imposed

6.10. The FSA has had regard to the size, financial resources and other circumstances of HSBC Life.

Conduct following the breach

6.11. The FSA considers the firm's failure to address the risks identified (with reference to the publicly available information concerning the risk of data loss) in a timely and appropriate way to be a serious failure.

6.12. In response to the data loss and the broad scope review of data protection by HSBC Group Audit, HSBC Life revised its procedures and controls which has served to mitigate the seriousness of its failings. These changes have included:

(1) contacting all 180,000 individuals affected by the data loss and revising caller identification procedures to account for the lost data;

(2) requiring all staff to complete two programmes of mandatory information risk training, with refresher training mandatory on an annual basis.

(3) revising induction training for new staff to enhance the Information Security message. Any staff member who has joined HSBC Life prior to the programme is required to complete the refresher training identified above;

(4) providing appropriate software and enforcing compulsory encryption on all electronic data transfers and providing clear instructions on when and how to apply encryption;

(5) implementing procedures to further restrict the ability to download data to portable devices and providing keys to staff for all lockable cabinets;

(6) introducing the dedicated role of Business Information Risk Officer, including assessing ongoing performance against 18 key information risk indicators; and

(7) introducing an Information Security forum as a sub-committee to the formal risk committee structure.

6.13. Throughout the FSA's investigation, HSBC Life has co-operated fully and worked with the FSA to facilitate an early settlement of this matter.

Other action taken by the FSA

6.14. The FSA has had regard to previous cases involving breaches of system and control requirements that threaten the FSA's financial crime objective. HSBC Life has not been the subject of FSA enforcement action previously.

7. DECISION MAKER

7.1. The decision which gave rise to the obligation to give this Final Notice was made by the Settlement Decision Makers on behalf of the FSA.

8. IMPORTANT

8.1. This Final Notice is given to HSBC Life in accordance with section 390 of the Act.

Manner of and time for Payment

8.2. The financial penalty must be paid in full by HSBC Life to the FSA by no later than 31 July 2009, 14 days from the date of the Final Notice.

If the financial penalty is not paid

8.3. If all or any of the financial penalty is outstanding on 1 August 2009, the FSA may recover the outstanding amount as a debt owed by HSBC Life and due to the FSA.

Publicity

8.4. Sections 391(4), 391(6) and 391(7) of the Act apply to the publication of information about the matter to which this notice relates. Under those provisions, the FSA must publish such information about the matter to which this notice relates as the FSA considers appropriate. The information may be published in such manner as the FSA considers appropriate. However, the FSA may not publish information if such publication would, in the opinion of the FSA, be unfair to HSBC Life or prejudicial to the interests of consumers.

8.5. The FSA intends to publish such information about the matter to which this Final Notice relates as it considers appropriate.

FSA contacts

8.6. For more information concerning this matter generally, you should contact Mark Lewis (direct line: 020 7066 4244 / fax: 020 7066 4245) of the Enforcement Division of the FSA.

……

William Amos
Head of Department
FSA Enforcement Division