Financial Services Authority

FINAL NOTICE

To: **HSBC Actuaries and Consultants Limited**

Of: 36 Ridgmont Road, St Albans
Hertfordshire
AL1 3AB

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 Actuaries and Consultants Limited (HSBC Actuaries 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 £875,000. 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 31 October 2007 (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 £875,000.

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 £1.25 million on HSBC Actuaries.

2. REASONS FOR THE ACTION

2.1. In the Relevant Period HSBC Actuaries breached Principle 3 by failing to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. HSBC Actuaries 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 customer information might be lost or stolen.

2.2. HSBC Actuaries 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 Actuaries failed to have 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;

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

(3) customer data received from third parties on portable electronic media was properly recorded upon receipt.

2.4. HSBC Actuaries' 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 a purpose 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 staff practices that placed customer data at risk of loss or theft in that:

(4) on a number of occasions, HSBC Actuaries staff sent unencrypted electronic media (such as floppy disks) containing significant amounts of customer data to third parties through the post or by local courier services;

(5) notwithstanding that access to the firm’s offices was securely restricted, in some parts of the business, staff routinely left confidential customer data on open shelves or in cabinets which could not be locked; and

(6) on one occasion, staff did not adequately check if they had received customer data which appeared to have been sent to the firm by a third party.

2.6. In part, these failures contributed in April 2007 to the loss in the ordinary post of an unencrypted floppy disk (and the possible loss of a further copy of the disk within

HSBC Actuaries' offices) containing the names, addresses, dates of birth and National Insurance numbers of 1,917 members of a pension scheme administered by HSBC Actuaries.

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

(1) During the Relevant Period, HSBC Actuaries had approximately 1,000 corporate customers. It administered approximately 1,990 policies and schemes, containing the details of approximately 500,000 active policy/scheme members. These individuals are entitled to rely on HSBC Actuaries to take reasonable care to ensure the security of customer data entrusted to it. The failure to implement 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 Actuaries was aware by October 2006 at the latest 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 its data security procedures were adequate and robust enough to prevent customer data being mislaid and potentially released into the public domain.

(3) HSBC Actuaries failed to respond to problems identified in June 2007 from the data loss incidents in April 2007, namely its lack of appropriate systems and controls, in a timely and appropriate manner. The firm took three months before implementing a procedure in September 2007 requiring staff to encrypt customer data that was being sent by email or placed on a portable storage device for transit.

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

2.9. HSBC Actuaries' 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 incidents HSBC Actuaries reported the matter to the FSA (and kept it fully appraised of the steps which it was implementing in response to those incidents) and wrote to all customers affected by the data losses to offer support at HSBC Actuaries' expense; and

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

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

(1) amended its procedures to include a requirement to encrypt data in order to ensure the secure transmission of confidential data;

(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) engaged with the HSBC Business Information Risk Officer programme, which includes the assessment of ongoing performance against 18 key information risk indicators;

(5) ensured that its Compliance department regularly communicated amendments to its "Business Instruction Manual" (BIM) to staff by email;

(6) restricted further the ability of staff to download data to portable devices;

(7) introduced Data Protection Champions to cascade information from Compliance to employees and to be the first source of contact for day to day data security queries; and

(8) put in place a defined response plan for reporting data loss incidents.

2.11. HSBC Actuaries 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 Actuaries is a wholly owned subsidiary of the HSBC group of companies (HSBC Group). HSBC Actuaries has been authorised by the FSA to perform a number of regulated activities since 1 December 2001.

4.2. HSBC Actuaries specialises in the provision of actuarial, employee benefits and financial planning services with the core nature of its business being the provision of actuarial and pension consultancy to corporate customers. The firm also has a number of individual customers who are participants in its Group Personal Pension policies and Group Stakeholder policies.

4.3. As of 30 April 2008, HSBC Actuaries had approximately 1,000 corporate customers. It administered approximately 1,990 policies and schemes containing the details of approximately 500,000 active policy/scheme members. Customer data was exchanged with third parties (such as pension scheme providers) as required for the administration of policies and schemes.

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

(1) names, addresses, date of birth and marital status;

(2) National Insurance numbers, employee numbers, policy numbers, fund choice, contribution level, pension benefits; and

(3) salaries and copies of application forms with details of health status.

Assessment of data security risk

4.5. Until the April 2007 data loss incident, HSBC Actuaries 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.

4.6. The customer data held by HSBC Actuaries was sufficient for criminals to use as a starting point to commit identity theft and other frauds.

4.7. In October 2006, HSBC Actuaries identified and recorded a risk relating to data security under the heading *"Lost post within office"*. The risk was allocated a C rating by the firm ("A" being the highest risk rating). The risk was subsequently reviewed in March 2007 and the risk entry was not altered. There was no identification of the risk posed by sending personal data to third parties either via email attachments or by portable storage devices. It was only after the April 2007 data loss incidents, that the risk was amended in July 2007 to also include "lost post or information within office or in transit" and the exposure enhanced to state "*disks sent externally to be password protected and sent by recorded delivery*".

4.8. In March 2007, HSBC Group issued an analysis report of the FSA's Final Notice on the *Nationwide* case. This analysis included a recommendation that customer data on portable media (such as USB devices, CDs and DVDs) should be encrypted.

4.9. HSBC Actuaries' response to this recommendation was insufficient: the firm took no action at the time to review its existing systems and controls to determine whether it adequately mitigated the risks raised by the *Nationwide* case. Whereas all laptops in use by the firm were secure (i.e. encrypted) in the event of theft or loss, the firm did not address the other identifiable risks, such as a lack of encryption or other protection of customer data in emails, CDs or other portable storage devices.

4.10. In July 2007, following the April 2007 data loss incidents (see paragraph 4.36 below), HSBC Actuaries received an email from its Head Office Compliance department, which highlighted the risk to the security of customer data when being transferred to third parties by disk. HSBC Insurance Compliance instructed HSBC Actuaries to ensure that data security procedures were adequate and robust enough to prevent customer data being mislaid and potentially released into the public domain. However, HSBC Actuaries did not introduce encryption until September 2007.

Relevant systems and controls

4.11. During the Relevant Period, HSBC Actuaries 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. Its procedures in relation to data security focused on compliance with the Data Protection Act (DPA) rather than the financial crime risks associated with identity theft. The firm's written procedures were fragmented and not readily accessible to staff and failed to give adequate guidance on how staff should handle or transfer customer data securely.

4.12. The primary source of procedures and guidance available to HSBC Actuaries' staff was its BIM, which collated the firm's main business procedures into a central document.

4.13. Staff were expected to be familiar with the BIM as it was required reading for new joiners to the firm. The BIM contained HSBC Actuaries' "House Rules", which were provided to all staff members. The "House Rules" did not contain sufficient procedures or guidance in relation to data security, although they referred to a separate HSBC publication called "*Information Technology - Security Guidelines"* that was available separately "if required". These Guidelines included some guidance on physical security, computer crime and encryption key management. Although these Guidelines were available on the intranet, the existence and content of the guidelines were not generally known.

4.14. 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 Actuaries to third parties such as pension scheme providers) and physical security (i.e. security of information kept within HSBC Actuaries' offices).

Communications security procedures

4.15. During the Relevant Period, HSBC Actuaries 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.

4.16. Prior to September 2007, the BIM contained only high level policies for the transfer of electronic data to third parties. The procedures in the BIM stated that staff "*must ensure that confidential information cannot readily be accessed, opened or browsed without detection by unauthorised individuals*". These procedures regarding communications security were inadequate in that:

(1) HSBC Actuaries did not require staff to encrypt customer data sent externally by the firm either by email or by portable storage devices; and

(2) if staff had wanted to encrypt an email, CD, disk or other portable storage device, HSBC Actuaries did not have the mechanism in place (i.e. an encryption system) to enable staff to do so.

4.17. The lack of procedures concerning this aspect of securing customer data is especially serious in that approximately 120 staff members, amounting to a quarter of the firm's staff, were able to bulk download material, including customer data, from their personal computers to portable devices such as floppy disks, CDs or USB devices.

4.18. HSBC Actuaries was notified of the data loss incident by the pension scheme provider in mid June 2007. Following notification, HSBC Actuaries failed to take immediate effective action by failing to recognise the immediate need for encryption to be introduced. Staff were told in August 2007 that if bulk personal data was being sent by disk or email it must be encrypted/password protected. At that stage, it was not possible for staff to encrypt bulk personal data. The firm took three months from notification of the data loss incidents to begin to implement a procedure enabling staff to encrypt data that was being sent by email or placed on a portable storage device for transit.

Physical security procedures

4.19. During the Relevant Period, although access to HSBC Actuaries' offices was securely restricted to staff and independent contractors, the firm failed to clearly set out all procedures and give proper guidance to its staff concerning the working practices that should be followed regarding the physical security of customer data.

4.20. Staff members were instructed in the BIM that they should follow the "clear desk" principle to ensure that confidential information could not easily be seen by others. Practical guidance on how this principle should be followed was not provided to staff, e.g. it was not specified whether confidential information needed to be removed from desks each evenings and kept in locked cabinets overnight.

Staff training and guidance

4.21. During the Relevant Period, HSBC Actuaries 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.

4.22. Throughout the Relevant Period, training for data protection was limited to 20 minutes during the firm's one day staff induction course. This training focussed on staff compliance with the DPA rather than on data security issues. Temporary staff were not provided with any formal training, other than ad hoc guidance from management, during the Relevant Period.

4.23. From September 2007, staff attending the induction course were also provided with a booklet entitled "*Your Personal Guide to Data Protection and Confidentiality*". This document did not make any reference to the need to encrypt electronic media containing customer data which was being sent externally by post or email.

4.24. From July 2007, the induction training material included reference to the April 2007 data loss incidents. However, the risks relating to data security and financial crime were not mentioned within this training material.

4.25. Whilst HSBC Actuaries' policy required data protection refresher training at least every two years, the firm did not provide refresher training until October 2007 (when an online learning programme was introduced). In the meantime, ad hoc guidance for individual queries was available from the Compliance department.

Monitoring and review of adequacy of controls

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

4.27. Compliance had a monitoring programme in place during the Relevant Period that included data protection. However, its focus was on inadvertent disclosure and compliance with the DPA rather than on data security risk and financial crime.

4.28. In February 2008, Compliance undertook a themed audit on data protection and data security issues. Prior to undertaking the audit, Compliance sent questionnaires to its various business practices asking about procedures in place within each practice, such as the type of personal data held, physical access to business areas and training given to staff. The audit revealed that further action was still required by the firm in some limited areas.

Incident reporting

4.29. During the Relevant Period, the firm failed to have effective procedures in place and provide specific guidance as to what to do in the event of data being lost or stolen (e.g. if a laptop went missing or if personal data did not arrive at its location). Whilst staff members were expected to report data loss to their line manager, there was no defined response plan in place for reporting such incidents until April 2008.

4.30. The firm was not aware that two disks containing personal customer data were potentially missing from April 2007 until they were notified by the pension scheme

provider on 14 June 2007. Compliance was informed of the data loss on 25 June 2007.

4.31 Prior to February 2008, aside from the April 2007 data loss incident, no data security breaches were reported by staff during the Relevant Period. However, since February 2008, HSBC Actuaries' staff have reported seven incidents at its St Albans and Bristol offices where correspondence was posted to incorrect addresses or material was included in the wrong envelope.

Practices adopted by staff

4.32 In the absence of clear procedures, guidance and adequate training and monitoring, HSBC Actuaries staff adopted working practices that put customer data at risk during the Relevant Period. For example:

(1) in the absence of controls, unencrypted customer data was transferred to third parties;

(2) staff were able to download customer data without appropriate security in place; and

(3) staff did not always store confidential data in lockable cabinets, which were not available in all parts of the firm throughout the Relevant Period.

4.33 HSBC Actuaries was unable to determine on exactly how many occasions electronic customer data was transferred unencrypted to third parties but estimates that it happened on up to six occasions prior to the data loss incidents in April 2007.

Data loss incidents

4.34 In April 2007, there were two separate customer data loss incidents. Both incidents related to a computer floppy disk in transit between HSBC Actuaries and the provider of a pension scheme provider administered by HSBC Actuaries. Each disk contained customer data relating to the same 1,917 pension scheme members:

(1) The first floppy disk had been sent by the pension scheme provider to HSBC Actuaries. The disk contained a schedule of the surnames, first initials, National Insurance numbers and dates of birth of the pension scheme members. Contrary to normal practice, HSBC Actuaries was instructed by the pension scheme provider to add the members' addresses to the schedule and return it so that the provider could send annual Additional Voluntary Contribution benefit statements directly to members' home addresses. Having done so, HSBC Actuaries returned the floppy disk by ordinary post (i.e. unrecorded delivery) to the pension scheme provider. The disk was not encrypted (or password protected). Although HSBC Actuaries' staff became aware of the potential loss of the disk on 14 June 2007, Compliance were not

notified promptly and did not become aware of the incident until 25 June 2007. The disk was never recovered.

(2) The same month, HSBC Actuaries received a letter from the pension scheme provider which listed a second floppy disk as one of its enclosures. HSBC Actuaries staff did not notice when they received the letter whether a disk was in fact, enclosed. Accordingly, once the disk was identified as potentially missing in June 2007, HSBC Actuaries did not know whether it had been lost in transit or at its offices, or whether it had actually been sent. This second disc (which was password protected but not encrypted) was also never recovered.

4.35 HSBC Actuaries reported these incidents to the FSA on 17 July 2007.

4.36 Whilst there is no evidence that the data was compromised, data included on the disks contained sufficient information to expose the pension scheme members to the risk of identity theft. The pension scheme members were informed by letter of the data loss, and were offered the benefits of an Experian monitoring service at the firm's expense.

5. PRINCIPLE BREACH

5.1. By reason of the facts and matters set out above, the FSA considers that HSBC Actuaries has contravened Principle 3 of the FSA's Principles for Businesses, namely that HSBC Actuaries 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 data security training needed by its staff;

(4) the monitoring of staff; and

(5) guidance for staff in event of data being lost or stolen.

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 Actuaries 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 HSBC Actuaries is of a particularly serious nature (see paragraphs 2.1 – 2.8 above). For a period of almost two years HSBC Actuaries did not 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 losses 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 Actuaries.

Conduct following the breach

6.11. When HSBC Actuaries reported the loss of customer data to the FSA, the FSA requested that HSBC Actuaries conduct a formal assessment of the incident. In response to this request HSBC Group carried out a review of HSBC Actuaries' procedures.

6.12. In August 2007, the resulting internal audit report identified that the root cause of the data loss incident was HSBC Actuaries' lack of relevant processes, procedures and training. The August 2007 report made a number of recommendations. However, a follow up review performed in November 2007 noted with particular concern that the issues raised by Group audit in August 2007 had not yet been fully implemented. Subsequently HSBC Actuaries:

(1) revised induction training for new staff to enhance data security awareness;

(2) required all existing staff to undertake data protection refresher training every two years. By November 2007 all HSBC Actuaries' staff had either completed on-line data protection training or had attended refresher training on data protection. Refresher training is now required every year;

(3) introduced data security training for temporary staff;

(4) restricted further the ability of staff members to download data to portable devices;

(5) amended the data protection chapter of the BIM to include a requirement to encrypt data and a chart demonstrating steps to ensure secure transmission of confidential data;

(6) ensured that its Compliance department regularly communicated amendments to the BIM to staff by email;

(7) introduced Data Protection Champions in January 2008, with at least one in each practice. The purpose of this role was to cascade information from Compliance to employees and to be the first source of contact for day to day compliance queries;

(8) enhanced physical security by greater security of premises and incorporating lockable cabinets in every office;

(9) engaged with the HSBC Business Information Risk Officer (BIRO) programme;

(10) wrote to all customers affected by the data losses to offer support through Experian at HACL's expense; and

(11) put in place a defined response plan for reporting any future data loss incidents.

6.13. Throughout the FSA's investigation, HSBC Actuaries 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 Actuaries 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 Actuaries 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 Actuaries 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 Actuaries 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 Actuaries 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