Financial Services Authority

FINAL NOTICE

To: **HSBC Insurance Brokers Limited**

Of: Bishops Court
27-33 Artillery Lane
London
E1 7LP

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 Insurance Brokers Limited (HSBC Insurance Brokers 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 £700,000. 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 30 April 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 £700,000.

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 million on HSBC Insurance Brokers.

2. REASONS FOR THE ACTION

2.1. During the Relevant Period, HSBC Insurance Brokers breached Principle 3 by failing to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. The firm 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. HSBC Insurance Brokers failed to undertake an adequate assessment of the risks relating to data security and 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 Insurance Brokers 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, floppy disks and USB devices) was secure in the event that the data was lost or intercepted;

(2) customer data sent to third parties in hard copy form was sent securely;

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

(4) an appropriate due diligence process was followed prior to contracting services to third parties such as waste disposal firms.

2.4. HSBC Insurance Brokers' failure properly to 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 the firm:

(1) sent unencrypted electronic media (such as CDs) containing significant amounts of confidential customer data to third parties through the post or by local courier services;

(2) notwithstanding that access to the firm's offices was securely restricted, routinely kept customer data on open shelving or in cabinets which were unable to be locked; and

(3) entered into contracts with third parties such as confidential waste disposal firms without explicitly ensuring that appropriate data security arrangements were in place.

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

(1) during the Relevant Period HSBC Insurance Brokers had over 65,000 customers, most of whom were companies in the UK. It handled customer data relating to the individuals associated with a number of personal and group insurance policies the firm arranged for its customers. These individuals are entitled to rely on the firm 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; and

(2) the failures occurred following a period of heightened awareness of financial crime issues as a result of government initiatives, increasing media coverage and an FSA campaign about the importance of financial crime within the financial services sector. Further, HSBC Insurance Brokers 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 within its businesses were adequate and robust enough to prevent customer data being mislaid and potentially released into the public domain.

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

2.8. HSBC Insurance Brokers' failures therefore merit the imposition of a significant financial penalty. In deciding upon the level of disciplinary sanction, the FSA recognises that HSBC Insurance Brokers did not lose any data as a result of the deficiencies in its data security controls and that HSBC notified the FSA about those deficiencies.

2.9. In addition, the FSA also recognises that the firm has taken significant and proactive steps to revise its procedures and controls, which have served to mitigate the seriousness of its failings. In particular, HSBC Insurance Brokers:

(1) issued consolidated procedures and guidance on data security risk to its staff, including on the use of encryption;

(2) further enhanced physical security by providing locks on the cabinets within its offices;

(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; and

(5) restricted further the ability to download data to portable devices.

2.10. HSBC Insurance Brokers 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 Insurance Brokers is a wholly owned subsidiary of the HSBC group of companies (HSBC Group). The firm has been authorised by the FSA to perform a number of regulated activities since 14 January 2005. In particular, it has been authorised to arrange, assist in the administration of, and deal as agent in, non-investment insurance contracts for commercial and retail customers.

4.2. HSBC Insurance Brokers promotes itself as a large international insurance broking and risk management firm with services primarily aimed at corporate clients. The firm operates from ten UK offices and two overseas branches.

4.3. In the Relevant Period, HSBC Insurance Brokers had between 64,600 and 69,307 customers, 93% of which are classed as commercial (corporate) customers by the firm.

4.4. HSBC Insurance Brokers' staff have access to and handle customer data to the extent that it is required for the purpose of providing insurance broking services (principally for commercial customers in respect of property and casualty, motor and other general insurance business) and the administration of insurance business (including claims handling).

4.5. The types of confidential customer data held by HSBC Insurance Brokers and handled by or made accessible to its staff includes information that may be contained in proposal forms or in information required to process a claim, such as:

(1) names, addresses and dates of birth;

(2) bank account numbers, sort codes and signatures (on customer cheques);

(3) debit and credit card payment details, including card security codes (sufficient for 'card-not-present' transactions); and

(4) personal details concerning family, lifestyle and social circumstances, education and training details, employment details, physical or mental health or condition and criminal offences (including alleged offences).

4.6. During the Relevant Period HSBC Insurance Brokers sent customer data by email, on disc and in hard copy form on an ad hoc basis to intermediaries and loss and claim adjusters and more regularly to insurers and reinsurers, for example:

(1) annually at renewal of insurance policies; and

(2) in respect of the placing of new policies and when claims arose.

4.7. During the Relevant Period HSBC Insurance Brokers' staff handled customer data concerning:

(1) approximately 7,000 transactions per month; and

(2) approximately 1,800 insurance claims per month.

Assessment of data security risk

4.8. Throughout the Relevant Period, HSBC Insurance Brokers 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.

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

4.10. Until May 2007, HSBC Insurance Brokers did not carry out a specific assessment of the data security risks in respect of its customer data.

4.11. From May 2007, HSBC Insurance Brokers performed a regular data security risk assessment in respect of customer data with reference to breaches of the Data Protection Act 1998 (DPA). Whilst this risk assessment identified some of the risks associated with the physical security of customer data (e.g. the risk of confidential waste not being shredded), it failed to correctly identify other physical security risks such as documents not being secured in offices and failed to identify risks associated with the communication or transfer of customer data.

4.12. In February and March 2006, HSBC Insurance Brokers' compliance department (Compliance) carried out a Data Protection review at the firm with reference to the DPA. The subsequent report dated March 2006 identified the type of personal data held and the way in which personal data was held and processed, but did not assess the associated financial crime risks. Whilst the report focused on the DPA, the following recommended actions were relevant to mitigating the risks to customer data security:

(1) computer based 'data protection principles' training should be rolled out to all staff; and

(2) data protection issues should be incorporated into all divisional and central management manuals to ensure that staff are aware of their obligations with regard to the processing and handling of personal data.

4.13. This review was repeated in October 2007 and the subsequent report repeated these recommendations, reflecting that HSBC Insurance Brokers had not yet implemented the recommended changes, although progress had been made to address the identified needs in the intervening 20 months. The recommended training and procedures were implemented during the last quarter of 2007.

4.14. HSBC Insurance Brokers failed to act in an appropriate and timely manner to a clear recommendation from Compliance and later took inadequate action when revising its procedures in November 2007 and March 2008.

4.15. In July 2007 HSBC Insurance Brokers 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 disc and instructed staff to ensure that data security procedures are adequate and robust enough to prevent customer data being mislaid and potentially released into the public domain. The firm did not take sufficient action in response to this instruction and later took inadequate action when revising its procedures in November 2007 and March 2008.

Relevant systems and controls

4.16. During the Relevant Period, HSBC Insurance Brokers failed to take sufficient 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. Rather the procedures in relation to data security focused on compliance with the DPA.

4.17. 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 the firm to third parties) and physical security (i.e. security of information kept within the firm's offices). In addition customer data was placed at risk when handled by a small number of third parties (which included couriers and waste disposal firms), where contracts were entered into with those entities without appropriate due diligence checks.

4.18. Further, the procedures that were in place did not provide HSBC Insurance Brokers' staff with readily accessible guidance concerning customer data security as, in order to understand the relevant policies and requirements in full, staff would have had to refer to several documents. The firm's staff procedures were contained primarily in its Core Procedures Manual (CPM) which was superseded in November 2007 by its Business Instruction Manual (BIM). These procedures were supplemented by various HSBC Group standards and policy documents.

4.19. In July 2007 HSBC Insurance Brokers recognised that the CPM was not sufficiently comprehensive and the BIM was introduced in November 2007 with a view to expand, update and standardise procedures across the firm. The BIM was later revised in March 2008.

Communications security procedures

4.20. During the Relevant Period, HSBC Insurance Brokers failed to have effective procedures in place and provide adequate guidance to staff concerning how to protect electronic and hard-copy customer data being transferred out of the firm:

(6) HSBC Insurance Brokers did not require its staff to encrypt customer data sent outside the firm by electronic media such as email or on discs until February 2008.

(7) The firm's procedures did not address the circumstances in which customer data sent to third parties should be sent by secure post or courier rather than by normal post.

4.21. In March 2008, more detailed procedures were issued to staff concerning the secure transfer of customer data, whether internally or externally. However, these procedures were ambiguously worded and required further explanation to understand the prescribed working practices.

Physical security procedures

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

4.23. Until March 2008, HSBC Insurance Brokers only had high level policies concerning the physical security of customer data, which required that information must be kept and stored securely and should not be freely accessible to unauthorised persons. The firm failed to set out procedures and give proper guidance to its staff concerning the working practices that should be followed to achieve these standards, such as a requirement to store customer files in locked cabinets.

4.24. In November 2007, when the CPM was replaced by the BIM, HSBC Insurance Brokers issued further high level policies concerning the need to store customer data securely but only applied these policies to "sensitive" customer data as defined by the DPA (such as data relating to health, lifestyle and criminal convictions) and not to other customer data such as name, address, bank account number, transaction details, employment records and date of birth. This distinction failed to take account of the potential for non-sensitive personal data to be used to further financial crime and resulted in inadequate security procedures being implemented for all customer data. In any event, staff were still not given adequate practical guidance about how they should store customer data securely (for example no reference was made to placing files in locked cabinets).

4.25. HSBC Insurance Brokers refined its procedures in March 2008 to require all customer data to be stored securely and customer data defined as 'sensitive' to be kept in locked cabinets. In any event, by the end of the Relevant Period, lockable cabinets had yet to be introduced into all of the firms UK offices.

4.26. HSBC Insurance Brokers' procedures in respect of physical security were also inadequate in that no clear desk policy was implemented until 1 February 2007.

4.27. The clear desk policy was ineffective from 1 February to 30 April 2008 in that, whilst HSBC Insurance Brokers' staff were initially instructed to implement a clear desk policy in respect of all paperwork:

(1) written procedures set out the requirement for staff to lock away 'sensitive' customer data that had been cleared from desks, but other personal customer data that could be used for the purpose of financial crime was not captured by this requirement;

(2) there was inadequate practical guidance as to where to store non-sensitive customer data; and

(3) whilst the firm restricted access to its offices to staff and independent contractors, those offices that did not have lockable cabinets for the purpose of securing sensitive data only had open shelving and unlockable cabinets as alternative storage.

4.28. HSBC Insurance Brokers did not have any procedures in place in respect of the disposal of confidential waste until November 2007. From November 2007 the firm required that confidential waste be disposed of 'carefully', that it must be shredded and be 'destroyed in accordance with procedures'. However, the firm's procedures did not set out any associated working practices which staff were to follow.

Contracts with third parties

4.29. Until November 2007, HSBC Insurance Brokers failed to set out procedures and give proper guidance to its staff concerning the working practices that should be followed to ensure appropriate data security arrangements were in place when entering into contracts with third parties (such as confidential waste disposal firms, IT vendors and a claims management firm). The firm's procedures did not address the need for due diligence checks before entering into the contract and for a clause requiring the party to whom data has been outsourced to comply with data protection legislation. In addition the firm's procedures did not explain the role of the central purchasing function in overseeing the appointment of third parties.

4.30. From November 2007 HSBC Insurance Brokers required that the appointment of third parties to process customer data on its behalf be subject to an outsourcing agreement or other agreed terms and these should be routed to the central purchasing function.

Staff training and guidance

4.31. Until February 2008, HSBC Insurance Brokers 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.

4.32. From March 2006, it was HSBC Insurance Brokers' policy that data privacy, protection and security training was mandatory for new recruits and for all staff every two years. However, for the majority of the Relevant Period, new staff were only given instructions concerning data protection generally as part of a 30 minute training session addressing compliance generally. This took place during a one day induction course which was typically delivered to new staff within a month of starting employment. From April 2006 new staff were also given a written summary of the DPA's Eight Principles.

4.33. This induction training did not address customer data security until February 2008. HSBC Insurance Brokers introduced more comprehensive induction training in February 2008 which covered data security, for example with specific reference to the clear desk policy. Further, until February 2008 the firm failed to provide data protection induction training to temporary staff or require them to sign a confidentiality agreement.

4.34. The need for ongoing refresher training for staff concerning data security had been identified in March 2006 during an HSBC Insurance Brokers compliance review. In response the firm arranged data protection training for human resources staff in respect of the security of staff data. HSBC Insurance Brokers took 20 months (to November 2007) to fully develop and roll out on-line ongoing training for staff in respect of customer data security.

Monitoring and review of adequacy of controls

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

4.36. In addition to day–to-day supervision of staff by line management, Compliance monitored staff practices in respect of customer data security, for example by scheduled monitoring visits to offices and by undertaking spot checks (such as checking adherence to the clear desk policy). Compliance also undertook themed reviews, such as in respect of complaints and money laundering. No themed review was undertaken in respect of data security before 2008. Line management and Compliance assessed staff conduct against the requirements of the CPM and BIM staff procedures manuals in place at the time.

4.37. This monitoring of staff was flawed in that the procedures in the CPM or BIM against which they were assessed did not provide adequate and effective instructions concerning day-to-day working practices that addressed customer data security against which staff could be assessed. This is reflected in the failure by line management to adequately identify and address issues concerning data security.

Practices adopted by staff

4.38. In the absence of clear procedures, guidance and adequate training and monitoring, HSBC Insurance Brokers staff adopted working practices that put customer data at risk. For example, staff:

(1) sent unencrypted electronic media containing customer data (including proposal forms) to third parties by email, by post or via local courier services;

(2) kept customer data in open cabinets without doors and, due to limited storage, often left files on desks (albeit that this was within secured premises); and

(3) on occasion, engaged third parties who handled the firm's customer data without consulting the central purchasing function prior to finalising contracts. However, its contracts were reviewed by its own internal legal team.

4.39. During the Relevant Period, using the established incident reporting procedure, two incidents were reported to Compliance which highlighted established staff practices that placed customer data at risk. In both of these incidents (set out below), the risks to customer data had not been recognised by the staff that were responsible for the transfer and disposal of customer data:

Protection of hard copy customer data in transit

4.40. In August 2006 Compliance investigated an incident in which an accounts envelope that should have been contained within a security bag had gone missing in transit between the firm and an insurer. The security bag contained customer data including hard copy customer policy schedules, cheques and credit card and debit card payment details (including the cards' security codes). The bag should have been secured by a security PIN to show that the bag had not been tampered with in transit. Whilst investigating the loss of the envelope (which was later found to have been sent to the incorrect office and was retrieved), Compliance identified lapses in data security. It had been staff's practice to not use the security PIN and, further, some security bags had tears in them and so could not be secured. This lack of attention to simple security measures reflected the absence of clear instructions in HSBC Insurance Brokers' written procedures and poor levels of staff awareness of communications security risks. Steps were taken to address the relevant security measures that should have been in place; however these were not addressed in the firm's written procedures until March 2008 and then without clear instructions concerning what working practices should be followed.

Disposal of hard copy customer data

4.41. In December 2006 Compliance investigated an incident identified by senior management at HSBC Insurance Brokers' head office. In the absence of written procedures concerning confidential waste disposal, head office staff were found to have routinely disposed of customer data such as bank account details as waste paper for recycling rather than disposing of it securely. This risk to customer data was compounded by the customer data being left in open sacks in the head office's reception area awaiting collection. Immediate steps were taken for customer data to be disposed of as confidential waste. However, the risk to customer data not being treated as confidential waste was not addressed in HSBC Insurance Brokers' written procedures until November 2007 and then without clear instructions concerning what working practices should be followed.

5. PRINCIPLE BREACH

5.1. By reason of the facts and matters set out above, the FSA considers that HSBC Insurance Brokers has contravened Principle 3 of the FSA's Principles for Businesses, namely that HSBC Insurance Brokers 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;

(4) the monitoring of staff; and

(5) the contracting of services to third parties.

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 Insurance Brokers 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. Although HSBC Insurance Brokers has never lost any data, the FSA considers that the failure to implement adequate and effective procedures across the firm is of a particularly serious nature (see paragraphs 2.1 – 2.6 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 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.

6.8. In addition, the FSA considers it particularly serious that the failures by the firm continued even after its compliance staff highlighted the deficiencies in its training and procedures in March 2006. Give the nature of the customer data handled by its staff, although HSBC Insurance Brokers undertook some steps to improve its training and procedures following the March 2006 report, it should have acted more promptly than the 20 months it took to fully implement those procedures and training.

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 Insurance Brokers.

Conduct following the breach

6.11. In response to the broad scope review of data protection by HSBC Group Audit and the recommended fundamental changes to staff procedures, HSBC Insurance Brokers has revised its procedures and controls which has served to mitigate the seriousness of its failings. In particular, the firm:

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

(2) introduced refresher training on an annual basis, rather than every two years;

(3) introduced training for temporary staff;

(4) introduced a dedicated section on information risk on its staff intranet which consolidates all pertinent information, procedures and guidance on information risk, including links to relevant sections of other Group intranets, which includes detailed guidance on the use of encryption.

(5) restricted further the ability to download data to portable devices;

(6) further enhanced physical security by providing locks on the cabinets within its offices; and

(7) engaged with the HSBC Business Information Risk Officer programme.

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

Other action taken by the FSA

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

7. DECISION MAKERS

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 Insurance Brokers 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 Insurance Brokers 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 Insurance Brokers 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 you 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