Financial Services Authority

FINAL NOTICE

To: Zurich Insurance Plc, UK branch

Of: The Zurich Centre
3000 Parkway
Whiteley
Fareham
PO15 7JZ

Date 19 August 2010

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 Zurich Insurance Plc, UK branch (ZIP UK) a Decision Notice on 11 August 2010 which notified ZIP UK that pursuant to section 206 of the Financial Services and Markets Act 2000 (the Act), the FSA had decided to impose a financial penalty of £2,275,000 on ZIP UK. This penalty is in respect of ZIP UK's breaches of Principle 3 of the FSA's Principles for Businesses and breaches of the rules in the Senior Management Arrangements, Systems and Controls sourcebook at SYSC 3.1.1R and SYSC 3.2.6R. The breaches occurred during the period from 1 August 2007 to 14 August 2009 (the Relevant Period).

1.2. ZIP UK confirmed on 5 August 2010 that it will not be referring the matter to the Upper Tribunal (Tax and Chancery Chamber).

1.3. Accordingly, for the reasons set out below, the FSA imposes a financial penalty on ZIP UK in the amount of £2,275,000.

1.4. ZIP UK 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 £3.25 million on ZIP UK.

2. REASONS FOR THE ACTION

2.1. In the Relevant Period, Zurich UK[1] breached Principle 3 by failing to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

2.2. Zurich UK also breached SYSC 3.1.1R and SYSC 3.2.6R by:

(1) failing to take reasonable care to establish and maintain systems and controls that were appropriate to its business; and

(2) failing to take reasonable care to establish and maintain effective systems and controls to counter the risk that Zurich UK might be used to further financial crime.

2.3. The breaches related to the management of risks associated with the security of customer information in the context of certain outsourcing arrangements.

2.4. The breaches arose in connection with the general insurance business of Zurich UK (Zurich UK (GI)). Zurich UK (GI) outsourced the processing of some of its customer data to Zurich Insurance Company South Africa Limited (ZICSA). Both Zurich UK and ZICSA are members of Zurich Financial Services Group (the Zurich Group) and are subject to relevant common Zurich Group policies, procedures and controls. However, as a result of the intra-group relationship, Zurich UK (GI) relied to an unreasonable extent on ZICSA being in compliance with Zurich Group policies and did not manage the outsourcing arrangement as if it were a third party supplier arrangement.

2.5. Zurich UK (GI) failed to take reasonable care to ensure that it had effective systems and controls to manage the risks relating to the security of confidential customer information arising out of the outsourcing arrangement with ZICSA and the consequential risk that lost or stolen information might be used for the purposes of financial crime.

2.6. Zurich UK (GI)'s failings only came to light following a data loss incident. On 11 August 2008, one of ZICSA's subcontractors lost an unencrypted back-up tape during a routine transfer to a data storage centre. The tape contained certain personal

[1] Prior to 1 January 2009, the substantial part of the general insurance business of Zurich Financial Services Group was carried on in the UK by the UK branch of Zurich Insurance Company Ltd (ZIC UK). This business was transferred to ZIP UK under Part VII of the Act with effect from 1 January 2009. This is described further at paragraphs 4.1 to 4.3 below. In this Notice, we refer to the general insurance business of ZIC UK and ZIP UK as Zurich UK (GI), and we refer to ZIC UK and ZIP UK together as Zurich UK.

information belonging to 46,000 policy holders of Zurich Private Client, Zurich Special Risks and Zurich Business Insurance Direct (each of which is a business line of Zurich UK (GI)), as well as certain personal data of 1,800 third parties. In addition, deficiencies in the management of security procedures involving data tapes in South Africa potentially also affected a further 5,000 UK customers whose personal data was not on the lost back-up tape but was otherwise held in South Africa.

2.7. The data on the unencrypted back-up tape consisted of an extensive range of sensitive insurance information belonging to policyholders. The nature of the personal data held on the lost tape varied between customers but included, among other things, identity details, bank account and credit card details and details of insured assets and the type of security arrangements used to protect them. The loss of this data could have resulted in financial loss to customers and potentially also exposed customers to the risk of other crime such as burglary and theft. It should however be noted that Zurich UK (GI) has seen no evidence to suggest that the lost personal data has been compromised or misused.

2.8. Zurich UK (GI) did not become aware of the data loss incident until a year later when the incident was reported through internal audit (following a Group data privacy audit undertaken at ZICSA). Subsequent internal investigations revealed certain failings in the management of security procedures involving data tapes in South Africa. The investigations also revealed Zurich UK (GI)'s failings in managing the outsourcing arrangement and the associated risks.

2.9. During the Relevant Period, Zurich UK (GI) failed to oversee effectively the outsourcing arrangement and did not have adequate control over the data that was being processed by ZICSA. In particular:

(1) Zurich UK (GI) did not carry out an ongoing assessment of the risks connected with the outsourcing arrangement in that it failed to carry out adequate due diligence on the data security procedures used by both ZICSA and ZICSA's subcontractors during the Relevant Period;

(2) Zurich UK (GI) did not obtain sufficient management information from ZICSA to enable Zurich UK (GI) to identify, measure, manage and control data security and financial crime risks. Routine monitoring was limited to regular service management conference calls dealing with various matters such as service and contract issues and these calls ceased after March 2008;

(3) Zurich UK (GI) considered that it was entitled to rely on ZICSA being in compliance with Zurich Group policies, in particular a policy requiring appropriate security measures, including encryption of confidential data. However, Zurich UK (GI) did not adequately consider whether this reliance on Group policies was sufficient and did not determine for itself whether appropriate data security policies had been adequately implemented by ZICSA;

(4) there was a failure to put in place proper reporting lines between ZICSA and Zurich UK (GI) during the Relevant Period. This resulted in the data loss incident not being reported to Zurich UK (GI) for twelve months. Zurich UK

(GI) did not ensure there was a co-ordinated policy regarding security incident reporting which, in the event of a data loss incident involving UK customer data, would have ensured the direct and timely escalation of matters to Zurich UK (GI); and

(5) there was also a lack of clarity within Zurich UK (GI) in relation to the functional responsibility for providing assurance to management that data security issues were being appropriately identified and managed. Various members of senior management had responsibility for data security issues, but there was no single data security manager with overall responsibility.

2.10. Zurich UK (GI)'s failure to assess properly the risks involved in the data outsourcing arrangement and to implement robust systems and controls to deal with them increased the risk that data belonging to UK customers might not be sufficiently secure and had the potential to expose its customers to the risk of identity theft or other crime.

2.11. Further, the absence of effective monitoring over the outsourcing arrangement resulted in the failure to identify practices within ZICSA and its subcontractors that placed the confidential information of UK customers at greater risk of loss or theft. In particular, back-up tapes containing Zurich UK (GI)'s confidential customer information were transported to and from a storage facility in an unencrypted format, with the risk that the unprotected data might be lost or stolen in transit. In addition, from early 2008, unencrypted UK customer data was stored in a secure third party data storage centre which was not solely used by ZICSA. Unencrypted UK customer data was regularly left in the office of an engineer at that data storage centre. Therefore there was a risk that third parties with access to the data storage centre might have access to Zurich UK (GI)'s unprotected data.

2.12. The cumulative impact of Zurich UK (GI)'s failings represented a material risk to the FSA's objectives of reducing financial crime and protecting customers. The FSA considers these failings to be particularly serious because:

(1) confidential information belonging to approximately 51,000 UK customers and 1,800 UK third parties was handled by ZICSA under the outsourcing arrangement over the course of the Relevant Period;

(2) policy holders are entitled to rely on Zurich UK (GI) to take reasonable care to ensure the security of their data. Zurich UK (GI)'s failure adequately to consider and manage the risks or to implement effective systems and controls to address these risks had the potential to expose policy holders to the risk of identity theft or other crime and financial loss;

(3) the failures occurred following a period of heightened awareness of financial crime issues as a result of government initiatives and increasing media coverage. In particular, the FSA published a report – Countering Financial Risks in Information Security – in November 2004 and a further report – Data Security in Financial Services – in April 2008;

(4) the back-up tape lost in August 2008 included the data of 46,000 policy holders and 1,800 third parties (such as claimants). In addition, deficiencies in the management of security procedures involving data tapes in South Africa potentially also affected a further 5,000 UK customers whose personal data was not on the lost back-up tape but was otherwise held in South Africa.

(5) the lack of timely escalation of the data loss incident from ZICSA to Zurich UK (GI) meant that customers were not informed of the incident for over a year. This increased the risk that their customer data might be used for the purposes of financial crime, as customers whose data was lost in August 2008 were unable to take steps to protect their data until they were notified in October 2009; and

(6) Zurich UK (GI)'s reliance on ZICSA's compliance with Zurich Group policies was impaired by the fact that Zurich UK (GI) did not itself comply with all relevant aspects of the relevant Group policies, in particular the data classification policy, which required confidential information in storage, processing and transit to be protected by the most secure means, including encryption.

2.13. Zurich UK's failings therefore merit the imposition of a significant financial penalty. In deciding on the level of disciplinary sanction, the FSA recognises that there are circumstances which serve to mitigate the seriousness of Zurich UK (GI)'s failings:

(1) the data loss incident first came to the attention of ZIP UK's senior management on 14 August 2009 and they reported the incident to the FSA in timely fashion on 21 August 2009. Other relevant regulators were also informed. Affected customers and third parties were notified of the data loss incident by ZIP UK in October 2009. Customers were offered a range of measures to minimise the risk of identity theft, all of which ZIP UK offered to pay for;

(2) ZIP UK initially informed the Information Commissioner's Office of the data loss incident on 2 October 2009 and subsequently made a formal notification to them on 11 December 2009. ZIP UK subsequently agreed to sign an undertaking, in respect of its breach of the Data Protection Act 1998, which was published on 24 March 2010;

(3) ZIP UK promptly instructed external advisers to conduct an investigation into the circumstances surrounding the data loss incident and related issues. The FSA was involved in scoping the terms of reference for the investigation and was kept updated throughout the investigation. The FSA was able to rely upon the investigation work carried out by the external advisers in its own investigation and in reaching the conclusions set out in this Notice. A firm's willingness to volunteer the results of its own investigation is welcomed by the FSA and is something the FSA may take into account when deciding what action to take. The FSA considers that the effectiveness and openness of the firm's own investigation in this matter has significantly reduced the level of disciplinary sanction that otherwise would been imposed on ZIP UK;

(4) in addition, ZIP UK commissioned a comprehensive review of its information security procedures and overall control environment with advice and assurance in relation to electronic customer data being provided by a leading firm of accountants and has invested a significant amount of time and resource to remedial action. ZIP UK has, since the data loss incident, made certain necessary changes to relevant systems and controls, policies and procedures and strengthened its governance in relation to information security. These steps (further details of which are set out at paragraphs 6.9 and 6.10 below) have served to mitigate the seriousness of its failings; and

(5) since the discovery of its failings, ZIP UK and its senior management have fully cooperated with the FSA's investigation. The FSA recognises that ZIP UK and its senior management have demonstrated a willingness to treat this matter with the utmost seriousness and a commitment to take the necessary steps to seek to ensure the ongoing security of customer data.

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. The definition of authorised person includes an EEA firm qualifying for authorisation under Schedule 3 of the Act (an incoming EEA authorised firm), by virtue of section 31 of the Act.

3.3. Under section 2(2) of the Act, the protection of consumers and the reduction of financial crime are regulatory objectives for the FSA.

3.4. The FSA's Principles for Businesses constitute requirements imposed on authorised persons under the Act. For an incoming EEA firm, the Principles apply in so far as responsibility for the matter in question is not reserved by an EU instrument to the firm's Home State Regulator (PRIN 3.1.1R).

3.5. 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".

3.6. The rule in the Senior Management Arrangements, Systems and Controls sourcebook of the FSA's Handbook, SYSC 3.1.1R provides:

"*A firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business*".

The areas to be covered by these systems and controls are set out in SYSC 3.2.

3.7. SYSC 3.2.6R provides:

"A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the

regulatory system and for countering the risk that the firm might be used to further financial crime".

3.8. Responsibility for breaches of Principle 3, SYSC 3.1.1R and SYSC 3.2.6R in relation to systems and controls to counter the risk that a firm might be used to further financial crime (in this case in relation to data security and outsourcing arrangements) are not reserved to a firm's Home State Regulator and are matters within the FSA's competence for an incoming EEA firm.

3.9. Relevant guidance is set out at Annex A (attached).

4. FACTS AND MATTERS RELIED ON

Background

4.1. The Zurich Group is a global provider of general and life insurance. It substantially conducts its general insurance business in the UK (the Relevant Business) through a branch company.

4.2. Until 31 December 2008, the Relevant Business was carried on by ZIC UK, the UK branch of Zurich Insurance Company Ltd, a Swiss company. ZIC UK had permission under Part IV of the Act to carry out contracts of insurance.

4.3. On 1 January 2009, the Relevant Business was transferred to ZIP UK, the UK branch of Zurich Insurance Plc, an Irish company, by way of a transfer under Part VII of the Act. The Relevant Business has been carried on by ZIP UK (which is an incoming EEA authorised firm) since that time.

4.4. In July 2002, ZIC UK outsourced its arrangement for the processing of certain of its data to another Zurich Group company, ZICSA. Over time, the data included confidential UK customer information gathered from the following lines of business: Zurich Private Client, Zurich Special Risks and Zurich Business Insurance Direct. A written outsourcing agreement was entered into with ZICSA in May 2004 which contained provisions with regard to the protection of Zurich UK (GI)'s customer data and to allow Zurich UK (GI) to monitor the outsourcing arrangement. For example, the outsourcing agreement included various warranties that ZICSA had appropriate protection for Zurich UK (GI)'s customer data in place and that it would comply with Zurich UK (GI)'s data security policies and with UK data protection legislation.

4.5. The written outsourcing agreement also gave Zurich UK (GI) the ability to monitor the outsourcing arrangement, for example by giving Zurich UK (GI) the right to inspect ZICSA's procedures or to request a report as to the technical and organisational measures used to protect personal data. ZICSA also agreed that it would monitor and report security violations to Zurich UK (GI) in line with agreed IT security standards.

4.6. ZICSA agreed that it would not subcontract the services to be provided under the agreement (other than to certain specified subcontractors) without the prior written consent of Zurich UK (GI).

4.7. The outsourcing arrangement involved ZICSA holding and processing data for the relevant business lines on a system that had been developed for Zurich UK (GI). The data was backed up fully on a daily basis – the routine was to write a copy of all data to electronic disk which was then copied to back-up tapes for off-site storage. Back-up tapes were regularly returned to ZICSA to be reused.

4.8. Until 2008, the data centre in which Zurich UK (GI)'s customer data was held and processed was at ZICSA's offices. Unencrypted back-up tapes of the data were routinely transported between the data centre and a storage facility. ZICSA engaged a subcontractor to collect and deliver the back-up tapes and to provide the storage facility for those back-up tapes (without Zurich UK (GI)'s written consent). That subcontractor itself subcontracted the collection and delivery of the back-up tapes to a third party contractor (unknown to ZICSA and without Zurich UK (GI)'s consent).

4.9. In early 2008, Zurich UK (GI)'s customer data was transferred to a data centre owned and managed by a third party. Another subcontractor was used by ZICSA to provide data centre services, including backing up data, tape administration, supervision of activities within the data centre and management of the collection and delivery of back-up tapes. Unencrypted back-up tapes continued to be transported routinely between the third party data centre and the storage facility.

Data loss incident

4.10. On 11 August 2008, an unencrypted back-up tape containing UK customer data was lost by the third party subcontractor (referred to in paragraph 4.8 above) during the collection and delivery process between the third party data centre and the storage facility:

(1) the back-up tape included certain personal information of 46,000 policy holders of Zurich Private Client, Zurich Special Risks and Zurich Business Insurance Direct and 1,800 third parties (such as claimants);

(2) the data on the unencrypted back-up tape consisted of an extensive range of sensitive insurance information belonging to policyholders. The nature of the personal data held on the lost tape varied between customers but included, among other things, identity details, bank account and credit card details and details of insured assets and the type of security arrangements used to protect them; and

(3) the back-up tape was unencrypted and meaningful data could be obtained from the tape by a sufficiently determined individual with an appropriate level of technical expertise and knowledge in the use of specific software and hardware.

4.11. Zurich UK (GI)'s lack of oversight of ZICSA may have contributed to the data loss incident. If Zurich UK (GI) had made appropriate enquiries of ZICSA and had understood the security measures in place to protect its customer data, it could have made recommendations to improve security, which might have prevented the back-up tape being lost.

4.12. In addition, if Zurich UK (GI) had itself implemented Zurich Group's data classification policy (which required confidential information in storage, processing and transit to be protected by the most secure means, including encryption) and had ensured that this had also been implemented by ZICSA, the lost customer data would have been better protected.

4.13. Issues relating to the outsourcing arrangement, including the failings identified in paragraph 2.9 above, only came to light following the data loss incident. These failings are set out in more detail below.

Oversight of the outsourcing arrangement

4.14. In order to ensure that it had taken reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems in relation to data security, Zurich UK (GI) should have carried out during the Relevant Period an ongoing assessment of the risks connected to the outsourcing arrangement with ZICSA.

4.15. In order to undertake such an assessment, Zurich UK (GI) should have ensured that it carried out sufficient due diligence during the Relevant Period on both ZICSA and ZICSA's subcontractors who were involved in the collection and delivery process to ensure that they had adequate systems and controls in place to ensure the security of Zurich UK (GI)'s confidential customer data.

4.16. Zurich UK (GI) should have regularly considered during the Relevant Period whether it required any further information to enable it to assess whether the relevant security measures of ZICSA and its subcontractors remained appropriate to protect the UK customer data they were handling. Zurich UK (GI) did not request any further information during the Relevant Period to update such an assessment (for example Zurich UK (GI) did not obtain updated information about ZICSA's subcontractors).

4.17. In order to ensure it was taking reasonable care to organise and control the processing of its UK customers' confidential data responsibly and effectively, Zurich UK (GI) should also have properly supervised and monitored its outsourcing arrangement with ZICSA. However, Zurich UK (GI) undertook only limited supervision or monitoring of ZICSA, consisting principally of service management conference calls. These calls dealt with a number of different matters such as service and contract issues, but did not normally cover data protection or data security issues. These calls ceased after March 2008, when a relevant member of staff at Zurich UK (GI) changed role.

4.18. Zurich UK (GI) did not obtain sufficient management information from ZICSA to enable Zurich UK (GI) to identify, measure, manage and control data security and financial crime risks. Zurich UK (GI) did not request such management information and none was provided. Zurich UK (GI) did not request a report as to the technical and organisational measures in place to protect its customers' data (notwithstanding that the outsourcing agreement between them gave Zurich UK (GI) the right to do so).

4.19. Zurich UK (GI) did not assess regularly the resources of ZICSA to ensure that its customer's confidential information was secure. During the Relevant Period, Zurich UK (GI) did not undertake sufficient due diligence to inform such an assessment and

obtained only limited information about the subcontractors used by ZICSA (see below at paragraph 4.28).

4.20. Zurich UK (GI) relied instead on ZICSA's compliance with Zurich Group policies (including policies on encryption and reporting security incidents). However, Zurich UK (GI) did not adequately assess whether ZICSA was complying with those policies or whether ZICSA had sufficient compliance resource to ensure Group policies were effectively implemented.

4.21. Zurich UK (GI) could have had more oversight over the outsourcing arrangement by ensuring that adequate reporting procedures were in place so as to ensure that any UK related issues arising from an audit of ZICSA were promptly brought to the attention of relevant persons in Zurich UK (GI). However Zurich UK (GI) failed to do so.

Management responsibility, clear reporting lines and staff awareness

4.22. In order to ensure it was taking reasonable care to organise and control its affairs responsibly and effectively, Zurich UK (GI) also should have ensured that there were clear management responsibilities and clear reporting lines in place in relation to data security and financial crime issues.

4.23. There was a lack of clarity within Zurich UK (GI) as regards the functional responsibility for providing assurance to management that compliance risks relating to data security were being appropriately identified and managed. This was, at least in part, because data privacy and protection and data security issues were split between the Compliance and Group IT functions (including Group IT Risk). The Compliance function within Zurich UK (GI) was responsible for overseeing financial crime prevention and compliance with data privacy and protection. However Group IT was responsible for data security. The Compliance function did not consider it was responsible for providing assurance with respect to the data security aspects of data privacy and protection.

4.24. There were no effective direct reporting lines in place between ZICSA and Zurich UK (GI) in relation to data security issues. Zurich UK (GI) relied on ZICSA to report security incidents to it through Zurich Group escalation policies. However there was a lack of co-ordination between the relevant Zurich Group policies, with several incident reporting procedures which were not wholly consistent in application. For example, there was no consistent approach to assessing the level of risk to be assigned to a data loss incident for reporting purposes. Zurich UK (GI) did not consider adequately whether these policies were sufficient to ensure that ZICSA would bring all material data loss incidents involving UK confidential customer data to the attention of Zurich UK (GI) directly and in a timely manner.

4.25. Training and awareness regarding data security and obligations to customers is part of Zurich UK (GI)'s training requirements. Zurich UK (GI) has a UK data protection policy and a Group Risk Policy (which covers information security procedures and guidance) and, among other things, issues regular reminders to staff on data protection and information security good practice. However, Zurich UK (GI) did not ensure its relevant staff were trained appropriately to understand and manage the relevant data security and financial crime risks arising from the outsourcing arrangement.

4.26. Relevant staff within Zurich UK (GI) had limited awareness of the outsourcing arrangement and the processing of UK customer data in South Africa, for example:

(1) there was limited awareness within certain relevant functions of Zurich UK (GI) that UK customer data was being processed in South Africa;

(2) certain relevant individuals lacked awareness in relation to procedures which could have facilitated the escalation of the data loss incident; and

(3) staff within Zurich UK (GI) had limited awareness of the relevance of the outsourcing arrangement to data security and financial crime issues, in particular:

(a) a pilot data protection health check was conducted by Zurich UK (GI) on one of the relevant business lines in December 2007. A third party data protection expert was engaged for this purpose. The health check consisted of responses to a questionnaire which included a question relating to offshore processing. However the response did not identify the processing arrangement in South Africa; and

(b) three financial crime self-assessments were completed by the same relevant business line (two in 2008 and one in April 2009). The responses did not identify that UK customer data was held in South Africa by ZICSA (although this may have been because there were no questions specifically asking about outsourcing arrangements).

4.27. Zurich UK (GI) did not ensure that internal audit was aware UK customer data was being processed by another Group company in South Africa. Zurich UK (GI) also failed to ensure that adequate reporting procedures were in place so as to ensure that any UK related issues arising from an audit of ZICSA were promptly brought to the attention of relevant persons in Zurich UK (GI).

Risk of loss or theft of customer data

4.28. As a result of the lack of ongoing due diligence and monitoring, Zurich UK (GI) had no effective oversight over the processing of its confidential customer data in South Africa. In particular, it had no oversight of the subcontracting arrangements between ZICSA and third parties who were involved in the collection and delivery of back-up tapes containing Zurich UK (GI)'s customer data. ZICSA conducted due diligence on all of its outsourcing partners at inception and regularly reviewed service delivery. However, ZICSA did not carry out further due diligence checks during the course of the relevant contracts and Zurich UK (GI) did not ensure that ZICSA had conducted adequate due diligence on its subcontractors. For example:

(1) ZICSA subcontracted the collection and delivery of back-up tapes to a company without seeking the written consent of Zurich UK (GI) (which was required by the outsourcing agreement); and

(2) both Zurich UK (GI) and ZICSA were unaware that the same subcontractor had further subcontracted responsibility for the collection and delivery of back-up tapes to another company.

4.29. Further, unknown to Zurich UK (GI), the outsourcing arrangement resulted in practices that placed UK customer data at risk of loss or theft in that:

(1) unencrypted UK customer data was stored on back-up tapes and routinely transported between the data centre and a storage facility. Therefore there was a risk that unprotected data might be lost or stolen in transit;

(2) unencrypted UK customer data was kept in a data centre in South Africa. The data centre to which the data was transferred in early 2008 was owned and managed by a third party and not solely used by ZICSA. Therefore there was a risk that third parties with access to the data storage centre might have access to Zurich UK (GI)'s unprotected data; and.

(3) unencrypted UK customer data was regularly left in the office of an engineer at the third party data centre, contrary to the policy of the subcontractor responsible for performing the backup process. Therefore there was an increased risk that unauthorised third parties might have access to the data.

4.30. These practices increased the risk that customer data would be lost or stolen and be used to facilitate identity theft or other crime. There had been an earlier incident (in June 2007) in which a back-up tape was misplaced in ZICSA's data centre and further failings were highlighted by a tape audit at the third party data centre in August 2008.

Lack of escalation

4.31. The data loss incident, which occurred on 11 August 2008, did not come to Zurich UK (GI)'s attention until a year later on 14 August 2009.

4.32. Zurich UK (GI) failed to ensure that adequate policies and procedures were in place to allow for the appropriate escalation and reporting of data security incidents. Various factors appear to have contributed to this failure to escalate the incident appropriately to Zurich UK (GI), for example:

(1) the lack of monitoring of the outsourcing arrangement, in particular the fact that data security issues were not normally discussed on the regular service management conference calls held between ZICSA and Zurich UK (GI) and the fact that these calls were not held after March 2008;

(2) the failure to ensure that there were clear management responsibilities and clear reporting lines in relation to data security and financial crime issues;

(3) Zurich UK (GI) relied on ZICSA complying with relevant Group policies which might have facilitated escalation (for example, loss event reporting procedures and audit reporting procedures). However these policies were not fully followed or fully implemented by ZICSA;

(4) Zurich UK (GI) did not adequately consider whether the relevant Group policies were adequate and effective having regard to Zurich UK (GI)'s own regulatory obligations. For example, Zurich UK (GI) did not adequately consider whether Group policies would ensure that data security incidents would be reported by ZICSA directly and in a timely manner to Zurich UK (GI); and

(5) Zurich UK (GI) did not ensure that internal audit in South Africa were aware that UK customer data was held and processed by ZICSA. Zurich UK (GI) also failed to ensure that adequate reporting procedures were in place so as to ensure that any UK related issues arising from an audit of ZICSA were promptly brought to the attention of relevant persons in Zurich UK (GI).

4.33. These failings contributed to the lack of escalation to Zurich UK (GI) until August 2009, a year after the data loss incident had occurred. Customers were not informed of the incident until October 2009. The delay in escalation of the incident to Zurich UK (GI) meant that customers were unable to take any action to protect their data until after that time (for example by registering with CIFAS).

5. BREACHES OF PRINCIPLE 3, SYSC 3.1.1R AND SYSC 3.2.6R

5.1. Zurich UK had an obligation under Principle 3 to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

5.2. Zurich UK also had obligations under the rules in the Senior Management Arrangements, Systems and Controls sourcebook of the FSA's Handbook:

(1) under SYSC 3.1.1R, to take reasonable care to establish and maintain such systems and controls as are appropriate to its business; and

(2) under SYSC 3.2.6R, to take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that Zurich UK (GI) might be used to further financial crime.

5.3. However, by reason of the facts above, Zurich UK (GI) failed to comply with these obligations in relation to managing the risks associated with the security of customer information in the context of the outsourcing arrangement with ZICSA in that:

(1) Zurich UK (GI) relied to an unreasonable extent on ZICSA being in compliance with Zurich Group polices, as a result of the intra-group relationship;

(2) Zurich UK (GI) did not manage the outsourcing arrangement as if it were a third party supplier arrangement;

(3) Zurich UK (GI) failed to ensure that it had effective systems and controls in place to manage the risks associated with its outsourcing arrangement (specifically the relevant data security and associated financial crime risks);

(4) Zurich UK (GI) failed to monitor effectively the outsourcing arrangement with ZICSA;

(5) Zurich UK (GI) failed to identify practices within ZICSA and its subcontractors that placed UK customer data at greater risk of loss or theft, in particular:

(a) Zurich UK (GI) did not adequately consider the risks arising from the transportation of unencrypted data in South Africa; and

(b) Zurich UK (GI) did not consider or assess whether the IT controls and physical security in place in South Africa were adequate to protect UK customer data; and

(6) Zurich UK (GI) failed to ensure that adequate policies and procedures were in place to allow for the appropriate escalation to it of relevant data security incidents.

5.4. As a result, Zurich UK (GI) was not aware that its UK customer data was being processed in South Africa in circumstances where the arrangements were not fully compliant with UK data protection legislation, including relevant recommendations and guidelines about encryption of data.

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 at the beginning 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 ZIP UK 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

6.5. Zurich UK (GI)'s failure to properly assess the 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. The failings identified above may have contributed to the loss of the unencrypted back-up tape in August 2008. The FSA accepts that the circumstances of the incident suggest that the back-up tape was lost rather than stolen. Zurich UK (GI)'s failings did contribute to the delay in escalation of the data loss incident from ZICSA to Zurich UK (GI).

6.6. The cumulative impact of the failings represented a material risk to the FSA's objectives of reducing financial crime and protecting customers. Therefore the FSA considers these failings merit the imposition of a significant financial penalty, in particular because:

(1) policy holders are entitled to rely on Zurich UK (GI) to take reasonable care to ensure the security of their data. The failure adequately to consider and manage the risks or to implement effective systems and controls to address these risks had the potential to expose policy holders to the risk of identity theft or other crime and financial loss;

(2) the failures occurred following a period of heightened awareness of financial crime issues as a result of government initiatives and increasing media coverage. In particular the FSA produced a report on Data Security in Financial Services, which was published in April 2008 (four months before the data loss incident). The report stated that it is not appropriate for customer data to be taken offsite on laptops or other portable devices which are not encrypted. The report highlighted that enforcement action may be taken against firms that fail to encrypt data offsite. Data privacy had also been identified by the Zurich Group and Zurich UK (GI) as a key risk to the business in 2008;

(3) the failings continued for a period of over two years. Although the FSA restricted its investigation to the Relevant Period, it has seen no evidence in

the course of its investigation to suggest that Zurich UK's oversight of ZICSA was substantially different prior to the Relevant Period;

(4) the lost back-up tape included the personal data of 46,000 policy holders of Zurich Private Client, Zurich Special Risks and Zurich Business Insurance Direct and 1,800 third parties (such as claimants). In addition, deficiencies in the management of security procedures involving data tapes in South Africa potentially also affected a further 5,000 UK customers whose personal data was not on the lost back-up tape but whose data was otherwise held in South Africa;

(5) the data on the unencrypted back-up tape consisted of an extensive range of sensitive insurance information belonging to policyholders. The nature of the personal data held on the lost tape varied between customers but included, among other things, identity details, bank account and credit card details and details of insured assets and the type of security arrangements used to protect them;

(6) the back-up tape was unencrypted and meaningful data could be obtained from the tape by a sufficiently determined individual with an appropriate level of technical expertise and knowledge in the use of specific software and hardware;

(7) the lack of timely escalation of the data loss incident from ZICSA to Zurich UK (GI) meant that customers were not informed of the incident until over a year later. This increased the risk that their customer data might be used for the purposes of financial crime, as the customers were unable to take steps to protect their data until October 2009; and

(8) Zurich UK (GI)'s reliance on ZICSA's compliance with Group policies was impaired by the fact that Zurich UK did not itself comply with all relevant aspects of the relevant Group policies, in particular the data classification policy, which required confidential information in storage, processing and transit to be protected by the most secure means, including encryption.

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

6.7. The FSA has had regard to the size, financial resources and other circumstances of ZIP UK.

Conduct following the breaches

6.8. In deciding on the level of disciplinary sanction, the FSA recognises that:

(1) ZIP UK promptly reported the incident to the FSA on 21 August 2009 and has co-operated fully with the FSA in the course of its investigation. Other relevant regulators were also informed;

(2) ZIP UK instructed external advisers to conduct an investigation into the circumstances surrounding the data loss incident and related issues. The FSA

was involved in scoping the terms of reference for the investigation and was kept updated throughout the investigation. The FSA was able to rely upon the investigation work carried out by the external advisers in its own investigation and in reaching the conclusions set out in this Notice;

(3) customers whose details were contained on the missing back-up tape were notified of the data loss incident by ZIP UK in October 2009. Further customers, who were potentially affected by deficiencies in the management of security procedures involving data tapes in South Africa, were also notified. Customers were offered a range of measures to minimise the risk of identity theft, including identity theft protection cover and expenses cover and the option of protective CIFAS registration, all of which ZIP UK offered to pay for; and

(4) ZIP UK initially informed the Information Commissioner's Office of the data loss incident on 2 October 2009 and subsequently made a formal notification to them on 11 December 2009. ZIP UK subsequently agreed to sign an undertaking in respect of its breach of the Data Protection Act.

6.9. In addition, ZIP UK has taken steps since the data loss incident to revise its procedures and controls, which have served to mitigate the seriousness of its failings:

(1) ZIP UK commissioned a comprehensive review of its information security procedures and overall control environment with advice and assurance in relation to electronic customer data being provided by a leading firm of accountants and has invested a significant amount of time and resource to remedial action;

(2) ZIP UK has taken steps to review and strengthen certain of its data security controls, including:

(a) extending the role of the UK representative for the Group IT Risk function to have specific accountability to proactively assess all IT risks impacting the UK, regardless of where they originate within the Zurich Group;

(b) further strengthening Group IT Risk reporting procedures including the mandatory requirement for a "high" severity rating for all customer data incidents, triggering enhanced escalation processes;

(c) providing enhanced robust mandatory data security training to all ZIP UK (GI) staff; and

(d) ensuring that all incidents notified to the ZIP UK Helpdesk involving ZIP UK customer data must be reported to the ZIP UK Financial Crime Unit and thereafter to ZIP UK Compliance;

(3) a multi-disciplinary third party working group has been established at ZIP UK to, among other things, strengthen where it considers appropriate the contractual obligations for data security and review monitoring processes for

new and historic contracts. This includes intra-group and third party outsourcing contracts;

(4) ZIP UK is appointing a dedicated Information Security Officer, who will have primary responsibility for co-ordinating and aligning the activities of its assurance functions in this area and provide assurance that the appropriate systems and controls are in place;

(5) ZIP UK has moved the hosting of its UK data from South Africa to Switzerland as part of a process to consolidate the hosting of its UK customer personal data processing applications within a central secure facility which is regularly reviewed by external auditors; and

(6) since October 2009, all newly created ZIP UK data back-up tapes that move between offices or storage locations have been encrypted and any movement of historic back-up tapes is subject to stringent security procedures.

6.10. The actions taken by ZIP UK form part of a Zurich Group initiative to achieve best practice data security controls to protect customer data on a global level through five key programs: improving data security with suppliers; protecting data from theft or loss; staffing and vetting; monitoring access to customer data; and governance and organisational alignment.

Other action taken by the FSA

6.11. The FSA has had regard to previous cases involving breaches of system and control requirements that threaten the FSA's financial crime objective. ZIP UK 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 ZIP UK 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 ZIP UK to the FSA by no later than 2 September 2010, 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 3 September 2010, the FSA may recover the outstanding amount as a debt owed by ZIP UK 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 ZIP UK 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 at the FSA (direct line: 020 7066 4244 /fax: 020 7066 4245).

William Amos
Head of Department
FSA Enforcement Division

ANNEX A

1. RELEVANT GUIDANCE

1.1. The guidance in SYSC Chapter 3 (Systems and Controls) applied to Zurich UK (GI) throughout the Relevant Period. The relevant provisions are as follows:

(1) a firm's reporting lines should be clear and appropriate having regard to the nature, scale and complexity of its business. These reporting lines, together with clear management responsibilities, should be communicated as appropriate within the firm (3.2.2);

(2) where functions are delegated:

(a) appropriate safeguards should be put in place (3.2.3(1));

(b) a firm should assess whether the recipient is suitable to carry out the delegated function or task, taking into account the degree of responsibility involved (3.2.3(2));

(c) there should be arrangements to supervise delegation, and to monitor the discharge of delegates' functions or tasks (3.2.3(4)); and

(d) if cause for concern arises through supervision and monitoring or otherwise, there should be appropriate follow-up action at an appropriate level of seniority within the firm (3.2.3(5));

(3) the guidance relevant to delegation within the firm is also relevant to external delegation ('outsourcing'). A firm cannot contract out its regulatory obligations. For example, under Principle 3, a firm should take reasonable care to supervise the discharge of outsourced functions by its contractor (3.2.4(1));

(4) a firm should take steps to obtain sufficient information from its contractor to enable it to assess the impact of outsourcing on its systems and controls (3.2.4(2));

(5) a firm's arrangements should allow its governing body to have the information it needs in relation to identifying, measuring, managing and controlling risks of regulatory concern (including risks relating to the fair treatment of its customers, to the protection of consumers and to the use of the financial system in connection with financial crime). The relevance, reliability and timeliness of that information are relevant (3.2.11); and

(6) a firm's systems and controls should enable it to satisfy itself of the suitability of anyone who acts for it (3.2.13).

1.2. The guidance in SYSC Chapter 13 (Operational risk: systems and controls for insurers) applied to ZIC UK throughout the Relevant Period, until 31 December 2008[2]. The relevant provisions are as follows:

(1) a firm should establish and maintain appropriate systems and controls for the management of operational risks that can arise from employees (13.6.2). A list of factors to be considered is set out at 13.6.2, including noting that these factors should be considered in relation to employees of a third party supplier who are involved in performing an outsourcing arrangement. As necessary a firm should review and consider the adequacy of the staffing arrangements and policies of a service provider (13.6.2(7));

(2) a firm should establish and maintain appropriate systems and controls for managing operational risks that can arise from inadequacies or failures in its processes and systems (including as appropriate the systems and processes of third party suppliers) (13.7.1);

(3) a firm should establish and maintain appropriate systems and controls to manage its information security risks – having regard to, for example, confidentiality and keeping information accessible to authorised persons or systems only (13.7.7);

(4) a firm should ensure the adequacy of the systems and controls used to protect the processing and security of its information, and should have regard to established security standards such as ISO17799 (Information Security Management) (13.7.8);

(5) a firm should understand the effect of any differences in processes and systems at each of its locations, particularly if they are in different countries. A firm should have regard to, for example, the timeliness of information flows to and from its headquarters (13.7.9);

(6) a firm cannot contract out its regulatory obligations and should take reasonable care to supervise the discharge of outsourced functions. It is noted that outsourcing may affect a firm's exposure to operational risk through significant changes to, and reduced control over, people, processes and systems used in outsourced activities (13.9.1);

(7) firms should take particular care to manage material outsourcing arrangements (involving services of such importance that weakness or failure of the services would cast serious doubt on the firm's continuing satisfaction with the threshold principles or compliance with the principles) (13.9.2);

(8) a firm should not assume that because a service provider is an intra-group entity there will necessarily be a reduction in operational risk (13.9.3);

(9) before entering into an outsourcing arrangement a firm should analyse how the arrangement will fit with its organisation and reporting structure; business

[2] Prior to 1 January 2007, this guidance was found at SYSC Chapter 3A.

strategy; overall risk profile; and ability to meet its regulatory obligations (13.9.4(1));

(10) before entering into an outsourcing arrangement a firm should consider whether the agreements establishing the arrangement will allow it to monitor and control its operational risk exposure relating to the outsourcing (13.9.4(2));

(11) before entering into an outsourcing arrangement, a firm should conduct appropriate due diligence of the service provider's financial stability and expertise (13.9.4(3));

(12) in negotiating its contract with a service provider, a firm should have regard to reporting or notification requirements it may wish to impose on the service provider (13.9.5(1));

(13) in negotiating its contract with a service provider, a firm should have regard to the adequacy of any guarantees and indemnities (13.9.5(4));

(14) in negotiating its contract with a service provider, a firm should have regard to the extent to which the service provider must comply with the firm's policies and procedures (covering, for example, information security) (13.9.5(5));

(15) in implementing a relationship management framework, and drafting the service level agreement with the service provider, a firm should have regard to the evaluation of performance through service delivery reports and periodic self certification or independent review by internal or external auditors (13.9.6(2));

(16) in implementing a relationship management framework, and drafting the service level agreement with the service provider, a firm should have regard to remedial action and the escalation processes for dealing with inadequate performance (13.9.6(3)); and

(17) in some circumstances a firm may find it beneficial to use externally validated reports commissioned by the service provider, to seek comfort as to the adequacy and effectiveness of its systems and controls. The use of such reports does not absolve the firm of its responsibility to maintain other oversight (13.9.7).