MORRISON | FOERSTER

Legal Updates & News

Bulletins

FSA Imposes Biggest Ever Fine on HSBC in the UK for Data Breaches

July 2009
by Ann Bevitt, Anthony Nagle

FSA Imposes Biggest Ever Fine on HSBC in the UK for Data Breaches

Fine

The UK Financial Services Authority (FSA) announced that it has fined HSBC almost £3.2 million in respect of data security breaches by three of the banks' units. HSBC Life UK Limited was fined £1,610,000, HSBC Actuaries and Consultants Limited was fined £875,000 and HSBC Insurance Brokers Limited was fined £700,000. The three firms are wholly owned subsidiaries of the HSBC Group of companies.

This is the largest fine ever imposed by the UK's financial regulator for data breach violations. The fine would have been higher but it was discounted by 30% because HSBC agreed to settle early during the FSA's investigation.

The FSA imposed the fine pursuant to section 206 of the Financial Services and Markets Act 2000 (the Act) in respect of breaches of Principle 3 of the FSA's Principles for Businesses. 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."*

Background

According to the FSA, during the investigation into the firms' data security systems and controls, the FSA found that large amounts of unencrypted customer data had been sent in the post or by courier. Confidential customer information was also routinely left on open shelving and unlocked cabinets and could have been lost or stolen. The FSA said that all three firms had failed to put in place adequate procedures to manage their financial crime risks. The FSA also established that staff were not given the necessary training in respect of identifying and managing the data security risks.

FSA Enforcement Director Margaret Cole stated, 'These breaches are very disappointing. All three firms failed their customers by being careless with personal details which could have ended up in the hands of criminals. It is also worrying that increasing awareness around the importance of keeping personal information safe and the dangers of fraud did not prompt the firms to do more to protect their customers' details. Fraud, particularly identity theft, is a major concern to everyone and firms must ensure that their data security systems and controls are constantly reviewed and updated to tackle this growing threat. In areas where we have previously warned firms of the need to improve, people can expect to see fines increase to deter others and change behaviour in the industry.'

The FSA stated that the firms have since taken remedial actions to address the concerns raised, including contacting the customers concerned, improving staff training, and requiring that all electronic data in transit is encrypted.

Lessons Learnt

In the detailed information and analysis of the individual breaches set out in the 'Final Notice' issued by the FSA to each of the three HSBC firms pursuant section 390 of the Act, there are clear lessons to be learned and steps which can be taken which will help firms remain compliant. The list below is not an exhaustive list.

Firms should:

1) take reasonable care to organise and control their affairs responsibly and effectively, with adequate risk management systems;

2) take reasonable care to establish and maintain effective systems and controls to manage the risks relating to data security, specifically the risk that customer information might be lost or stolen;

3) undertake adequate assessments of the risks relating to data security, assess whether existing controls are adequate to manage these risks, and implement adequate and effective procedures, guidance, training and monitoring of staff to address these risks;

4) need to have in place adequate and effective procedures, guidance and resources to ensure that:

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

(ii) customer data sent to third parties in hard copy form is sent securely;

(iii) notwithstanding that access to a firm’s offices may be securely restricted, customer data kept in its offices must at all times be kept secure from the risk of internal fraud or theft; and

(iv) customer data received from third parties on portable electronic media is properly recorded upon receipt; and

5) properly assess the risks and implement robust systems and controls to deal with them so that a firm's business could not be used for a purpose connected with financial crime and exposes its customers to the risk of being victims of financial crime.

For more information and assistance on how firms can comply in practice with the above steps and other relevant data protection requirements under the UK's data protection regime, please contact Ann Bevitt or Anthony Nagle.
