

Press Release

For immediate release

26 August 2010

Yorkshire Building Society takes action after customers' details are stolen

The Information Commissioner's Office (ICO) has found Yorkshire Building Society (YBS) in breach of the Data Protection Act after an unencrypted laptop belonging to the former Chelsea Building Society (CBS), which had recently merged with YBS, was stolen from its Cheltenham premises. The laptop contained a substantial part of the CBS customer database.

The laptop was recovered within 48 hours after YBS appointed private investigators, and forensic investigations revealed that none of the data had been accessed during that time, although there had been several attempts to do so.

The laptop was being used by a CBS employee who had been working from home and had given it, on request, to a manager who returned it to CBS's former head office in Cheltenham. It was later discovered that the manager had written down the passwords to the computer and left these in a bag with the laptop under a desk overnight.

Iain Cornish, Chief Executive of Yorkshire Building Society has [agreed to take a series of remedial steps](#) to ensure that such a data security breach does not happen again. This will include ensuring that all portable devices including laptops are encrypted (a measure that is already in place at

YBS), that all staff are made aware of the company's policies for the storage and use of personal data and that staff will only have access to the type and amount of personal data that is necessary for their work.

Mick Gorrill, Head of Enforcement at the ICO, said: "It is extremely concerning that an unencrypted laptop containing large amounts of personal data was left unsecured overnight, together with details of its passwords. What's more, the fact that the employee did not require all the information to carry out the task in hand created an unnecessary risk which could easily have been avoided; employees should only have access to information that is absolutely vital to work which is being carried out. I am pleased that the Yorkshire Building Society took such prompt and effective action and am satisfied that steps are now in place to prevent this happening again."

A full copy of the Undertaking can be viewed here:

http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx

ENDS

If you need more information, please contact the ICO press office on 020 7025 7580 or visit the website at: www.ico.gov.uk

Notes to Editors

1. The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
2. The ICO has specific responsibilities set out in the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.
3. For more information about the Information Commissioner's Office subscribe to our e-newsletter at www.ico.gov.uk. Alternatively, you can find us on Twitter at www.twitter.com/ICOnews.
4. Anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
 - Processed for limited purposes
 - Adequate, relevant and not excessive
 - Accurate and up to date
 - Not kept for longer than is necessary
 - Processed in line with your rights
 - Secure
 - Not transferred to other countries without adequate protection
5. The Data Protection Act (1998) does not cover the acts of interception of communications or 'hacking' of personal information. The interception of communications falls under the Regulation of Investigatory Powers Act (2000) which is regulated by the Interception of Communications Commissioner.
6. The ICO has legal powers to ensure that organisations comply with the requirements of the Data Protection Act. In using its regulatory powers, the ICO considers the nature and severity of the breach which has occurred. Dependent on circumstances, the powers the ICO has at its disposal include:
- serving information notices requiring organisations to provide the ICO with specified information within a certain time period;
 - serving enforcement notices requiring organisations to take specified steps in order to ensure they comply with the law;
 - issuing monetary penalties of up to £500,000 for serious breaches of the Data Protection Act;
 - conducting audits to assess whether organisations are processing personal data in accordance with good practice;
 - reporting to Parliament on data protection issues of concern;
 - prosecuting those who commit criminal offences under the Act. The ICO prosecutes individuals and organisations for specific breaches of the Act such as the illegal trading of personal data and non-notification.