



Information Commissioner's Office

Press Release

Date: 24 February 2010

Mortgage company accidentally discloses over 15,000 account details

The Information Commissioner's Office (ICO) has found Redstone Mortgages Ltd in breach of the Data Protection Act (DPA) after personal information relating to 15,333 mortgage accounts was emailed to a member of the public by mistake.

The information, which included personal data relating to individuals' arrears or possession proceedings, was sent to Redstone's head office and several other recipients as part of a monthly analysis report. It was not encrypted or password protected and was initially intended for a consultant using a private email address. Instead, the information was sent to a member of the public who had a similar email address.

David Lautier, Chief Executive Officer for Redstone Mortgages, has now signed an [Undertaking](#) to ensure that all reports containing personal information will be suitably password protected before being emailed externally. The Undertaking also requires Redstone Mortgages to implement other security measures as it deems appropriate to ensure that personal data is protected against unauthorised access.

Sally-anne Poole, Head of Enforcement & Investigations, said: "It is essential that the right procedure is followed and care is taken when sending out emails of this nature. If personal information falls into the wrong hands, individuals could experience considerable distress. It appears that this method of sending out reports containing personal information has been common practice within the company for a while. I am pleased that Redstone Mortgages has agreed to take remedial steps to safeguard personal information and prevent a similar incident 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 data controller shall, as from 19 February 2010 and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

- All reports containing personal data, the loss of which could cause damage or distress, shall be protected by means of a password consisting of at least eight characters, including upper and lower case letters and at least one non-text character, which will be separately transmitted and regularly changed before being transmitted electronically outside the data controller's internal computer network;
- All other emails containing personal data, the loss of which could cause damage or distress, shall be protected in the same manner as in (1) above or shall be redacted so that the identity of the data subject is not readily discernable by any third party;
- The above provisions shall be incorporated into all contracts between the data controller and any data processor acting on its behalf, and appropriate steps taken to ensure compliance;
- The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

2. The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

3. The ICO is an independent body with 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.

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