DATA PROTECTION ACT 1998

UNDERTAKING

[redacted]

16/8/10

Data Controller: Yorkshire Building Society

Yorkshire House
Yorkshire Drive
Bradford
BD5 8LJ

I, Iain Cornish, Chief Executive of Yorkshire Building Society (the "Society"), for and on behalf of the Society, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Yorkshire Building Society is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the "Act"), in respect of the processing of personal data carried out by the Society and is referred to in this Undertaking as the "data controller". Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the "Commissioner") was provided by the data controller with a report of the theft of an unencrypted laptop containing a substantial part of the customer database of the former Chelsea Building Society, which had just merged with the data controller. The laptop was used for marketing analysis by an employee working occasionally from home, and had been returned to Thirlestaine Hall (Chelsea's former head office) by that employee's manager, who required access to this work. Contrary to policies and procedures, the manager had written down the passwords and, when his work was concluded, left these and the laptop in its bag under his desk overnight.

3. The laptop was stolen from Thirlestaine Hall the following morning. Following the appointment of private investigators, it was recovered a couple of days later and investigations by independent computer forensic experts revealed that the data had not been accessed successfully, although several attempts had been made to do so. It was noted that the data controller took immediate and appropriate remedial action following the incident, including the commissioning of an independent investigation. The Commissioner also noted, however, that the employee had not required access to all the data held on the laptop in order to complete the analysis work.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provisions are the Third and Seventh Data Protection Principles, which are set out in Schedule 1, Part I to the Act.

5. Following consideration of the remedial action that has been taken

by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking 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 Third and Seventh Data Protection Principles in Part I of Schedule 1 to the Act, and in particular that:

(1) All portable and mobile devices including laptops and other portable media used to store and transmit personal data, the loss of which could cause damage or distress to individuals, are encrypted using encryption software which meets the current standard or equivalent;

(2) All staff are made aware of the data controller's policies for the storage and use of personal data and are appropriately trained how to follow those policies;

(3) Compliance with the data controller's policies on data protection and IT security issues is appropriately and regularly monitored;

(4) Staff shall only have access to the type and amount of personal data that is necessary for their work;

(5) The data controller shall implement such other measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction and/or damage, and that it is not excessive for the purpose(s) for which it is being processed.

Dated 16 August 2010

Signed [redacted]
pp Iain Cornish
Chief Executive
Yorkshire Building Society
(signed in his absence but with his authority by Robin Churchouse, Finance Director)

Signed [redacted]
Mick Gorrill
Head of Enforcement
For and on behalf of the Information Commissioner